UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

FELIPE CAYE BATALHA BOEIRA

Proof of Location as a Security Mechanism for Vehicular Ad Hoc Networks

Thesis presented in partial fulfillment
of the requirements for the degree of
Master of Computer Science

Advisor: Prof. Dr. Marinho Pilla Barcellos
Coadvisor: Prof. Dr. Edison Pignaton de Freitas

Porto Alegre
March 2018

CIP — CATALOGING-IN-PUBLICATION

Boeira, Felipe Caye Batalha

Proof of Location as a Security Mechanism for Vehicular Ad Hoc Networks / Felipe Caye Batalha Boeira. – Porto Alegre: PPGC da UFRGS, 2018.

67 f.: il.

Thesis (Master) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR–RS, 2018. Advisor: Marinho Pilla Barcellos; Coadvisor: Edison Pignaton de Freitas.

1. VANET. 2. Security. 3. Platoon. 4. Trust. 5. Proof of location. I. Barcellos, Marinho Pilla. II. Freitas, Edison Pignaton de. III. Título.

'I know of no time in human history where ignorance was better than knowledge.'

— NEIL DEGRASSE TYSON

AGRADECIMENTOS

À família. Agradeço aos meus pais e à minha irmã por todo suporte, dedicação e amor que desenvolveram quem sou. Obrigado, principalmente, por sempre apoiarem minhas decisões. Agradeço à Luciana pela parceria, à Ilse por todo carinho, ao Dirceu por despertar meu fascínio pela computação e aos demais familiares que participaram desta jornada.

Aos amigos. Por todos momentos bons que passamos. Agradeço à Danielle por sempre me incentivar a buscar meus sonhos. Ao Giuliano, pela presença e amizade. À Karol e ao Jerônimo, pelo companheirismo.

Aos professores. Agradeço ao Leonardo e ao Fernando pelo auxílio na minha formação e no desenvolvimento da minha carreira. Ao Alexey e Mikael, obrigado por todo suporte e hospitalidade, assim como pelas discussões fundamentais para o avanço desta pesquisa.

Aos orientadores. Por acreditarem no meu trabalho e dedicação. Por me guiarem no desenvolvimento de ciência, não romance. Obrigado por toda transmissão de conhecimento e por propiciar meu progresso durante estes anos de atividade.

ABSTRACT

In vehicular communication, nodes periodically share Cooperative Awareness Messages (CAMs) in order to convey information such as identity, velocity, acceleration and position. The positioning of nodes in a vehicular network is a key factor that directly affects how applications operate, being the formation of platoons a major case. In vehicular platooning, a group of vehicles travels closely together and leverages information shared through CAMs to operate lateral and longitudinal control algorithms. While the standardised cryptographic mechanisms counteract threats such as identity hijacking and packet tampering, an internal member who holds valid credentials may still be able to lie about the data it transmits in CAMs. In current Vehicular ad hoc Network (VANET) models, each vehicle is responsible for determining and informing its own position, generally using a Global Navigation Satellite System (GNSS) such as the Global Positioning System (GPS). This allows malicious actors to lie about their position and therefore cause unwanted effects in vehicular applications. The dependence of VANET applications on correct node localization introduces the need for position assurance mechanisms. In this dissertation, we first identify the risks associated with falsifying the position in vehicular platooning. Through simulations using the Veins framework, we show that collisions at high speed on a platoon may be caused by nodes that collude in falsification attacks. Given that truthful positioning is essential to proper behavior of VANET applications, we investigate proof-of-location schemes proposed in the literature. Then, a proof-of-location mechanism tailored for VANETs is designed using roadside units, with the capability of using different proof frequencies according to detection accuracy and overhead requirements. Through simulations using the studied attacks in this work, we show that the mechanism can counteract Sybil and message falsification attacks.

Keywords: VANET. security. platoon. trust. proof of location.

Prova de Localização como um Mecanismo de Segurança para Redes Veiculares

RESUMO

O desenvolvimento de redes veiculares possibilita o surgimento de sistemas inteligentes de transporte que podem aumentar a segurança nas vias, aperfeiçoar o controle de tráfego e fornecer entretenimento aos passageiros. O avanço e padronização de tecnologias de comunicação inter-veicular permitem que veículos compartilhem informações de forma colaborativa de maneira a viabilizar o estabelecimento de sistemas de transporte inteligentes cooperativos (C-ITS, Cooperative Intelligent Transportation Systems). Na comunicação veicular, cada nó compartilha periodicamente uma mensagem que contém informações sobre seu estado como posição, velocidade e aceleração. Estas mensagens são denominadas Cooperative Awareness Messages (CAMs) e podem ser utilizadas por veículos vizinhos para a operação de aplicações, sendo a formação de comboios um exemplo. Em um comboio veicular, um grupo de veículos viaja com distância reduzida entre cada membro através da operação de um controlador que utiliza informações compartilhadas por CAMs. O posicionamento compartilhado através de CAMs por cada veículo é crucial para a operação dos controladores de nós vizinhos, dado que este será utilizado para a condução do veículo. Embora os controles criptográficos padronizados para troca de mensagens em VANETs ofereçam contramedidas contra ataques como roubo de identidade e adulteração de pacotes, um atacante interno que possua credenciais válidas do sistema ainda pode mentir sobre as informações que são transmitidas para outros veículos. Em modelos atuais de redes veiculares, cada veículo é responsável por obter sua localização, normalmente através de GPS (Global Positioning System). A dependência de aplicações VANET na posição correta dos nós introduz a necessidade de mecanismos de garantia de localização. Nesta dissertação são identificados os riscos associados com a falsificação de posição em comboios veiculares. Através de simulações utilizando o ambiente de simulação Veins, mostramos que colisões em alta velocidade podem ser causadas por nós que atuam em conluio na falsificação de mensagens para um comboio. Dado que posicionamento legítimo é essencial para o funcionamento adequado das aplicações VANET, investigamos mecanismos de prova de localização propostos na literatura. Então, projetamos um mecanismo de prova de localização adaptado para VANETs usando equipamentos de estrada (RSUs, *roadside units*), com a capacidade de usar diferentes freqüências de prova de acordo com os requisitos de precisão de detecção e sobrecarga.

Através de simulações usando os ataques estudados neste trabalho, mostramos que o mecanismo pode detectar ataques de falsificação de mensagens e Sybil.

Palavras-chave: redes veiculares, segurança, comboio, confiança, prova de localização.

LIST OF ABBREVIATIONS AND ACRONYMS

3GPP	3rd Generation Partnership Project
AP	Access Point
C-ITS	Cooperative Intelligent Transport Systems
C-V2X	Cellular Vehicle to Everything
CAM	Cooperative Awareness Message
CDA	Cheating Detection Authority
ETSI	European Telecommunications Standards Institute
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IQR	Interquartile Range
IVC	Inter-Vehicular Communication
PBR	Position-Based Routing
STP	Spatial-Temporal Provenance
TTPL	Trusted Third Party for managing Location information
TTPU	Trusted Third Party for managing User information
TraCI	Traffic Control Interface
V2I	Vehicle-to-infrastructure
V2N	Vehicle-to-network
V2P	Vehicle-to-pedestrian
V2V	Vehicle-to-vehicle
VANET	Vehicular Ad Hoc Network
WORAL	Witness ORiented Asserted Location

LIST OF FIGURES

LIST OF TABLES

CONTENTS

1 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 (LAMMERT et al., 2014) and increased driving comfort (VAHIDI; ESKANDARIAN, 2003), 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 (VITELLI, 2016).

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 inter-vehicular communication will be necessary for platooning applications in order to preserve string stability (PLOEG et al., 2014) 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. This work is focused on the inter-vehicular part of the system and may be considered when performing a dependability assessment on the entire platoon logic.

1.1 Context

Enabling vehicles to communicate with each other to achieve cooperative awareness makes it possible to develop safety applications (e.g. emergency braking and blind spot vehicle detection), intelligent highway systems (e.g. platooning) and traffic management applications (e.g. automated T-intersection and roundabouts). Connecting vehicles together, however, introduces risks associated with actors that may exploit the network for self-benefit (i.e. rational attackers) or for destructive actions (i.e. malicious attackers).

The 3rd Generation Partnership Project (3GPP), in its latest release 14, has introduced Cellular Vehicle to Everything (C-V2X) specifications. This sets pace to the development of cellular networks to enable vehicular communication, including Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), Vehicle-to-Vehicle (V2V) and Vehicle-to-Pedestrian (V2P). The next release, numbered 15, will deliver the first set of standards for the 5G communication technologies, with a plan to be completed in 2018. Among the large set of enhancements being proposed for 5G, accurate positioning (KOIVISTO et al., 2017) and low latency communication are specially relevant for our work. They are considered to be components of our mechanism as the positioning and communication technologies are a pluggable part of the scheme. In the present work, the 5G base stations are considered to act as Roadside Units (RSUs) for the proof-of-location mechanism.

In order to provide security measurements for VANETs, the European Telecommunications Standards Institute (ETSI) has established a set of standards with requirements for the development of vehicular communication. In the standards, the usage of elliptic curve digital signatures is included for message sharing. The use of such cryptographic mechanism may thwart attacks on identity hijacking and tampering, for example. Through signed messages, vehicles are able to share information such as positioning. While digital signatures provide authenticity, non-repudiation and integrity of messages, they do not provide correctness assurance. This means that if an attacker signs a false position, even though the signature can be verified successfully this only means that the position was indeed transmitted by the claiming sender and was not tampered with.

The sharing of information among vehicles is crucial to achieve cooperative awareness. A common understanding among researchers and the Industry is that vehicular networks must provide both authentication and privacy. To achieve these requirements, the use of pseudonym authentication protocols has been proposed in vehicular networks (RAJPUT et al., 2017)(RAJPUT; ABBAS; OH, 2016)(RAJPUT et al., 2015). The use

of such protocols (when combined with mix-zones for pseudonym permutation) provides authentication and privacy.

1.2 Problem

Although ETSI specifies the use of cryptographic mechanisms in the vehicular communication, an internal attacker who has valid cryptographic keys may still be able to convey falsified information. A message falsification attack may be carried out by lying in the transmitted data. This attack, especially when combined with false nodes, can pose a serious threat. The use of pseudonyms authentication is a common approach to provide authentication and privacy. In order to avoid identity tracking by unauthorized actors, a node is usually granted several pseudonyms. A user who is capable of using multiple pseudonyms at the same time may conduct a Sybil attack. In the Sybil attack, one entity presents itself as multiple identities in order to have a larger influence in a system or conduct colluding attacks. The combination of using Sybil nodes and message falsification is a threat to vehicles that leverage data from such nodes. There are multiple scenarios in which attackers may present themselves as multiple identities to gain benefits (e.g. simulating a traffic jam to cause other drivers to take detour routes) or harm people (e.g. conveying false information that may cause vehicles to operate in an unwanted way, possibly causing collisions). The position falsification in VANETs may be used to conduct a series of attacks in such networks. Through the analysis of Sybil and platooning message falsification attacks modus operandi, we identify one of the main characteristics that enable them: the capability of lying about a node's position. If an attacker is not able to lie about the position of its Sybil nodes, it would make them very easily detectable given that multiple cars would report the same location. Likewise, not being able to falsify the position interferes directly with the ability to interfere with the platooning controller studied in this research.

1.3 Motivation

Research on the deployment of VANETs has been subject to a great amount of effort from both the Industry and Academia. The contributions and advancements in recent years have been leading theory to real implementations in the foreseeable future. The

latest release from 3GPP includes C-V2X specifications and the next release will deliver the first set of standards for the 5G communication technology in 2018. Communication requirements for autonomous driving will be fulfilled by this new set of technologies. In spite of the benefits provided by connecting vehicles to networks, risks associated with malicious actors must be considered. The falsification of positioning is shown to be a relevant threat in the VANET context, which needs to be addressed before real-world deployment.

1.4 Contribution

The outcome of the research is manifold. First, we identify attacks that may be conducted in the vehicular platoon context based on positioning falsification. Second, we perform a case study on the impacts of colluding nodes that engage on a position falsification in a platooning environment. Then, we study state-of-the-art proof-of-location mechanisms that have been proposed for mobile networks. A VANET-tailored proof-of-location mechanism is then designed and implemented in a simulator to be evaluated against the attack case study.

We show that position falsification can negatively impact the behavior of platooning. The ability to tamper with the position in beacons originates threats to VANET applications provided that neighbor vehicles trust the information conveyed by its peers. Collisions at high speed can occur once false positions are injected into the platoon controllers. In this work we design and evaluate a proof-of-location mechanism that can be used as a countermeasure to position falsification and Sybil attacks in VANETs.

1.5 Organisation

This dissertation is organised as follows: Chapter 2 presents the background needed to understand the remaining of this dissertation, including a literature review on Sybil and message falsification attacks along with the related work about proof of location. Chapter 3 studies the general impact of Sybil nodes that collude on message falsification attacks against a state-of-the-art IVC-based control algorithm in platooning. We analyse different scenarios, including those where a radar system would potentially not be able to detect a problem in time. Chapter 4 presents the design of the proof-of-location mechanism

and includes a qualitative security analysis of the proposed solution. Chapter 5 describes the evaluation environment and the parameters used in the simulations. The quantitative metrics used to assess the mechanism are included and the results are discussed. We demonstrate that the use of the proposed proof-of-location mechanism can be used as a countermeasure to detect Sybil and position falsification attacks. Chapter 6 concludes this dissertation and outlines future work.

2 BACKGROUND AND RELATED WORK

This chapter presents the literature review and provides a background on vehicular platooning that is required to understand the remainder of this work. Section 2.1 contains the communication model and explains how the platooning controller operates the vehicles. The literature review is divided into two sections, one for the attacks, and the other for a possible countermeasure: *Sybil and Message Falsification* and *Proof of Location*. Section 2.2 discusses the related work on Sybil and message falsification attacks in the context of platooning. Section 2.3 reviews the literature in the context of proof-of-location mechanisms.

2.1 Background

Recall that information is shared among vehicles through beaconing, periodic messages that are broadcast. Such beacons are sent at 10 Hz frequency and contain information about the node. Figure 2.1 depicts the structure of the beacon. The *vehicleId* 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. 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.

In this dissertation, we adopt Consensus (SANTINI et al., 2015), a state-of-the-art IVC-based platoon controller. Consensus operates a longitudinal control algorithm and we consider the use the Leader- and predecessor-following topology, which leverages information from both preceding vehicle and leader (see Figure 2.2). Consensus has been shown to outperform other control algorithms in terms of stability under strong interfer-

Figure 2.1: Platoon beacon structure

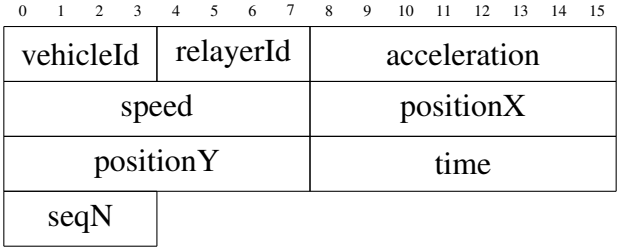
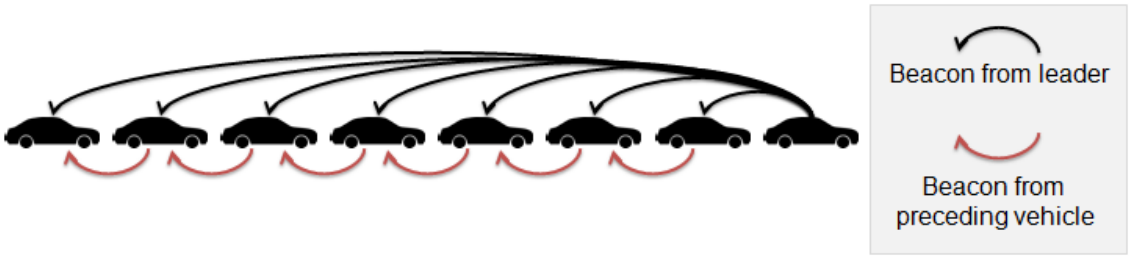


Figure 2.2: Platoon topology based on beacons from the leader and preceding vehicles



ence, delays, and fading conditions.

2.2 Sybil and Message Falsification 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 (RAYA; HUBAUX, 2007), is considered in many cases as an authentication and privacy enabler (SALES et al., 2016; CALANDRIELLO et al., 2007). 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 (BERESFORD; STAJANO, 2003) to ensure that vehicles are not traceable (BUTTYÁN et al., 2009; FREUDIGER et al., 2007; YING; MAKRAKIS; MOUFTAH, 2013). 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 (ZAIDI; RAHULAMATHAVAN; RAJARAJAN, 2013) 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 (ZAIDI et al., 2014), 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 (KAFIL; FATHY; LIGHVAN, 2012), 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 (VITELLI, 2016) 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 (SEGATA et al., 2014)) 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 Sybil attacks, in which the attacker can control the majority of nodes.

Message falsification in platooning can directly influence other members. A malicious insider can negatively affect the platoon by forging data or disrespecting the platoon's control law. An adversarial platooning environment is considered in (DADRAS; GERDES; SHARMA, 2015) 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 gain and applying a sinusoidal acceleration, it is possible to interfere with the platoon string stability and potentially cause accidents. In (SAJJAD et al., 2015), 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 (AMOOZADEH et al., 2015b), the authors model security attacks in VENTOS (AMOOZADEH et al., 2015a), 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 beacons 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 (DEBRUHL et al., 2015). The authors define a set of internal attacks in platooning that are originated by misbehavior or equip-

ment 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 that estimates the state of other members in the platoon and compares it with reported information to determine whether the member is malicious or not.

In (PETRILLO; PESCAPé; SANTINI, 2017), the authors design and evaluate a control strategy to detect and counteract message falsification attacks. In that work, the authors propose the estimation of the average distancing under the 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 between the belief and the reported distance is greater than a threshold, the respective member is marked as malicious and its beacons are not considered in the control algorithm. The cited paper ignores colluding nodes and 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 work to identify and evaluate the impact of vulnerabilities associated with the Sybil attack coupled with message falsification in platoons.

2.3 Proof of Location Related Work

Proof-of-location mechanisms are useful in a variety of situations. In this section, we describe the state-of-the-art mechanisms that have been proposed in the mobile ad hoc network and database-driven cognitive radio network fields.

In (WATERS; FELTEN, 2003), the authors discuss the generation of location proofs that have integrity capabilities and preserve the privacy of the user. They design a scheme that measures the round-trip signal propagation latency and location managers provide the proof to users.

STAMP (WANG et al., 2016) works on Spatial-Temporal Provenance (STP) proofs. It was designed to provide a provenance proof that users can use to attest a certain location history. In order to respect privacy, the authors propose the usage of commitment schemes (HALEVI; MICALI, 1996; DAMGÅRD, 1999; HAITNER; REINGOLD, 2007). The authors define two types of collusion attacks: Prover-Witness (P-W) and Prover-Prover (P-P). In P-W collusion, a witness is able to generate an STP proof even though the prover, the witness or even both are not at that location. In P-P, provers A and B collude in order

to generate a proof for a location that B is not. Suppose A is at the location B wants a proof for, A acts as a relay proxy for B, who signs the request and tunnels it through A. This is considered a wormhole attack, commonly referred as the Terrorist Fraud attack (DESMEDT, 1988) in location verification. In order to protect against P-P collusion attacks, the Bussard-Bagga (BUSSARD; BAGGA, 2005) distance bounding protocol was employed in that work. STAMP also uses an entropy-based trust model to protect against P-W collusion.

APPLAUS (ZHU; CAO, 2011) was designed similarly to STAMP. APPLAUS is also based on co-located users that act as alibis for generating location proofs. Differently from STAMP, APPLAUS use periodically changing pseudonyms in its scheme to preserve user's privacy. This incurs an operational overhead due to the necessity of careful management and scheduling of the identities, in addition to having dummy pseudonyms that require additional storage and data transfer. The authors propose a collusion detection mechanism based on the requirement of a certain number of witnesses to generate proofs. Since it may be hard for a prover to always find the required number of witnesses, APPLAUS also uses its server and the fact that it contains information about the number of pseudonyms at a particular time and location. This requires the server to have access to at least the majority of the proofs issued at the same period of time for a given region.

Witness ORiented Asserted Location provenance (WORAL) (HASAN et al., 2016) is another witness-based scheme framework. It was developed for obtaining location proofs without the requirement of having a centralized model. In fact, the authors consider that the service provider is a centralized entity that manages the accounts of the other three entities: the mobile devices (users/witnesses), the location authority and the auditor. The authors use design principles for secure location provenance presented on the OTIT model (KHAN et al., 2014). WORAL considers that collusion attacks may be conducted by malicious users, location authorities and/or witnesses.

VeriPlace (LUO; HENGARTNER, 2010) is a location-proof system with privacy and cheating detection capabilities. In order to detect cheating users, the system relies on the fact that a user cannot be at two locations at the same time. By observing proofs continuously, the system architecture can detect anomalies if proofs are geographically distant but chronologically close. In order to perform such detection, however, the system requires users to provide frequent proofs. This removes the control of users on deciding if they are willing to provide proofs at certain occasions, enforcing the continuous dispatch of location proofs. In addition, VeriPlace depends upon three trusted third parties in

order to defend against collusion attacks, as follows. The TTPU (Trusted Third Party for managing User information) stores triples that contain the requesting user identity, the time and the encrypted identity of the Access Point (AP) that issued the proof. The TTPL (Trusted Third Party for managing Location information) is responsible for generating the final proof containing the intermediate location proofs, as well as it holds the location database for the APs. Finally, the CDA (Cheating Detection Authority) conducts the anomaly analysis mentioned earlier.

The authors in (HASAN; BURNS, 2011) have proposed a scheme that uses both APs and witnesses to generate a proof. In this mechanism, a user first discovers a location authority and sends a proof request that includes the chronological information from the latest entry of the user's provenance chain. The authors state that a secure distance bounding or visual scanning should be performed in order to ensure that the user is indeed at the location he/she is requesting the proof for. Once it is completed, the location authority generates the location proof with the new chronological ordering information. When the user has received the proof, he/she now contacts a witness to endorse such proof, who also executes a distance bounding or other algorithm to attest the prover's localization. The witness creates an endorsement message and sends it to the location authority for timestamping. Finally, the witness receives the signed timestamp and generates the signed endorsement that will be delivered to the prover. Hash chains and Bloom filters schemes are proposed as privacy-preserving mechanisms to protect the integrity of the location proofs chronological entries.

Existing works on proof of location, presented above, are not suitable for the purposes of dealing with the studied attacks. In order to cope with the requirements of the vehicular environment, we design and evaluate a VANET-tailored proof-of-location mechanism. The proposed scheme can handle the high mobility model and is lightweight so that frequent proofs can be provided. In this dissertation, the combination of these characteristics in the proposed method are proven to be an effective countermeasure to Sybil and position falsification attacks.

3 SYBIL AND MESSAGE FALSIFICATION ATTACKS

Douceur (DOUCEUR, 2002) first describes the Sybil attack, in the context of Peer-to-Peer (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 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 lead a driver to unsafe areas or any region the driver would not willingly drive to, 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.

We perform a set of experiments to quantify the impact of Sybil and message falsification attacks for the defined scenarios. The main purpose is to analyse how the ability to use colluding Sybil nodes affect the severity of the attacks and to quantify these effects. We investigate to what extent 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, and how to leverage third-party vehicles on a highway to conduct this attack.

The presented scenarios are evaluated in Chapter 5 with the proposed proof-of-location mechanism. The use of position falsification is a requirement to insert Sybil nodes, which occurs earlier than the falsification to compromise the platooning controller. This results in the possibility of detection in the first stages of the attack, and will be

described in detail in further chapters.

Section 3.1 presents the threat model and a set of attack scenarios for vehicular platooning that takes into account both IVC-only and IVC-radar enabled vehicles. Section 3.2 includes the simulation environment and evaluation metrics. Section 3.3 contains the results and a discussion on the impacts of the attacks.

3.1 Attacks Overview

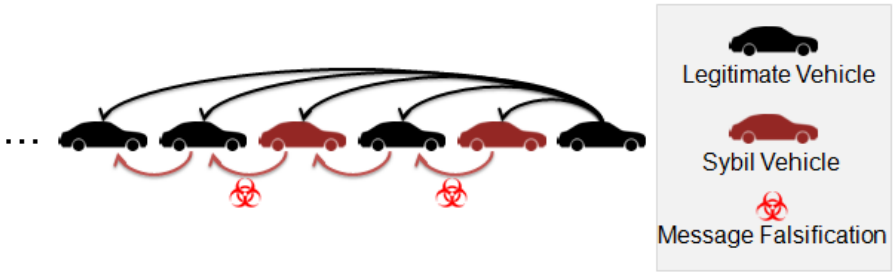
This section describes (i) the threat model considered in the attacks evaluation, and (ii) the scenarios we investigate. We specify the platoon topology, network communication details and assumptions. Then, five attack scenarios are presented, each of them containing two variants.

3.1.1 Attack 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 (NAKAGAMI, 1960) 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, as we follow other works that use similar assumptions (PETRILLO; PESCAPé; SANTINI, 2017; SANTINI et al., 2015). An attacker that travels in a different lane conducts the Sybil and message falsification attacks. In some scenarios, we also consider the presence of a non-platoon car traveling on the highway, as will be detailed later.

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, as depicted in Figure 3.2. It is important to note that the attacker travels right beside the first Sybil node. This is an important aspect on the evaluation of the attack detection using the proposed proof-of-location mechanism. The

Figure 3.1: Influence of Sybil nodes through message falsification



closer the attacker is to the Sybil node's position, the lower is the position error between the proof and the Sybil node's position.

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 3.1, 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.

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 to other platooning members. 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 Figure 2.1.

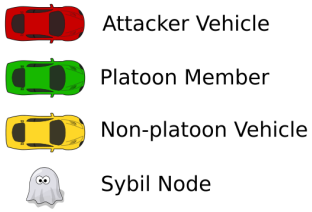
Our model combines the Sybil attack with the falsification of information in order to influence the behavior of other members of the platoon. While performing message falsification and identity theft would potentially allow an attacker to exploit the platoon in similar ways, we consider that only the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

3.1.2 Attack Scenarios

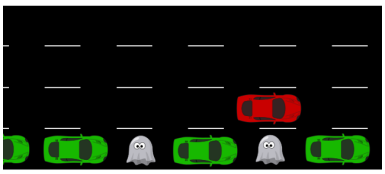
The five attack scenarios are hereby detailed, for each of the scenarios, we evaluated the use of multiple colluding Sybil nodes (scenario variants (a)) and the use of only one false node (scenario variants (b)). In this study, we use the leader- and predecessor-

Figure 3.2: IVC-based Sybil scenarios

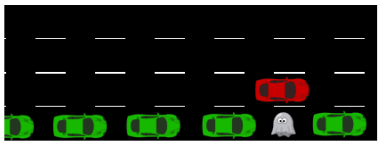
(a) Legend



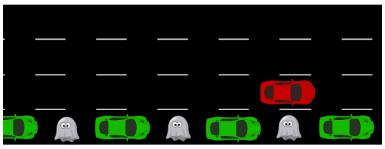
(b) Attack scenarios 1 (a) and 2 (a) on IVC-based platoon



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



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



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.

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.

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 3.1 and 3.2, that add a position error based on a desired acceleration and deceleration falsification.

$$D_{err} = (A_{con} - (D_{des})) * 0.1 \tag{3.1}$$

$$A_{err} = (A_{con} - (A_{des})) * -1 * 0.1 \tag{3.2}$$

Where:

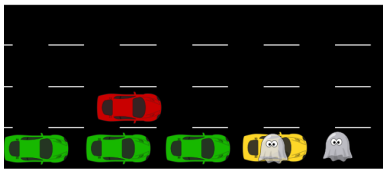
D_{err} = Deceleration distance error (m)
A_{err} = Acceleration distance error (m)
A_{con} = Controller acceleration (m/s^2)
D_{des} = Desired deceleration (m/s^2)
A_{des} = Desired acceleration (m/s^2)

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, at the pace that the beacons are being broadcast.

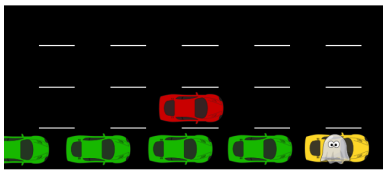
3. Emergency breaking obstruction. Emergency braking is a critical event that is sensitive to faults or attacks. In scenario 3 (a), we assume that an attacker has managed to introduce a Sybil node between every pair of platoon members. This allows the attacker to manipulate the members by forging beacons,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

Figure 3.3: IVC/Radar-based Sybil scenarios

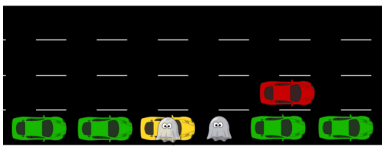
(a) Attack scenario 4 (a) on IVC/Radar-based platoon



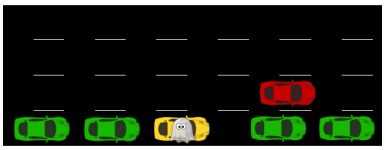
(b) Attack scenario 4 (b) on IVC/Radar-based platoon



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



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



an emergency braking is performed by the leader. In 3 (b) we assess how the emergency breaking 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, as long as a non-platoon vehicle travels 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.

3.2 Evaluation Methodology

In this section, we briefly describe the simulation model and software (PLEXE) employed to implement the attack model defined in Section 3.1. 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).

3.2.1 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 3.1.

Table 3.1: 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 (SANTINI et al., 2015)
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 ($m = 3$)

3.3 Impact

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. 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.

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 3.2.

3.3.1 Falsification

In scenario 1 (a), Sybil nodes are inserted at simulation time 30 s. After a stabilisation period, nodes start to falsify messages and manipulate their following vehicles 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 $\approx$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 scenario 1 (b), only one node is used in the attack and the impact is greatly reduced, the results are found in Table 3.2.

3.3.2 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.

3.3.3 Emergency breaking 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.

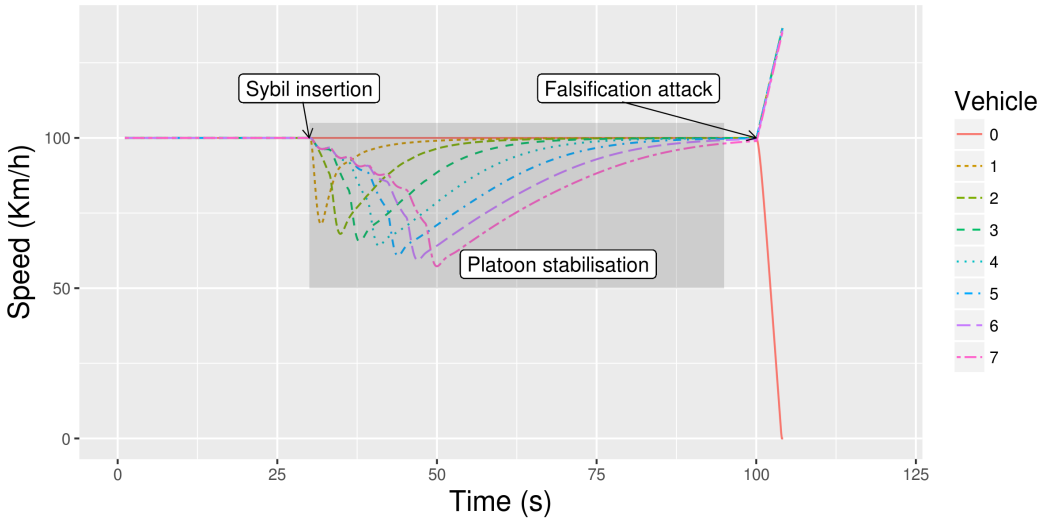
The impact of this attack affects all platoon members, which collide at high speed in a chain-reaction crash. While the leader is applying an emergency brake, the platoon members accelerate to as high as ≈137 km/h until there is a rear-end crash. Like in the previous attack, the time elapsed from the 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 (DEBRUHL et al., 2015), the authors simulate a similar scenario in which a malicious platoon member falsifies its acceleration profile in order to make its following vehicle accelerate.

Table 3.2: Attack scenarios results comparison

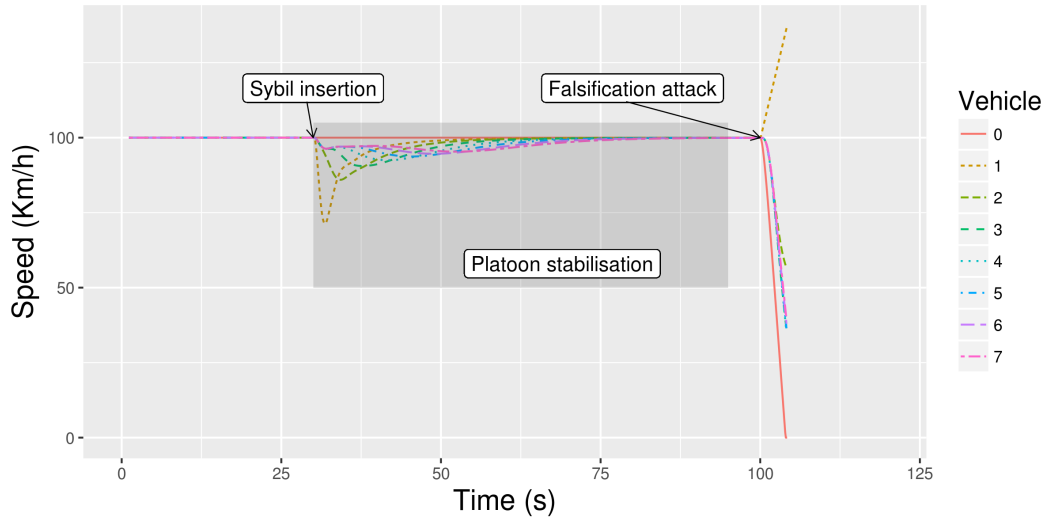
Scenario	Sybil nodes	Time until collision	Speed difference at collision	Collision Type
Falsification	2 1	3.9 s 7.9 s	134.7 km/h 70.6 km/h	Between platoon members
Covert falsification	2 1	19.2 s 37.4 s	12.6 km/h 8.2 km/h	Between platoon members
Emergency breaking obstruction	7 1	4.2 s 4.2 s	137.3 km/h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

Figure 3.4: Platoon member's speed in the Emergency Breaking scenario

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



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



While the follower is speeding up, the attacker aggressively breaks. 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 3.2), 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 3.4 (a) and (b).

3.3.4 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 3.3 (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 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 scenario 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 $\approx$149 km/h. In this case, only the leader identity is used. The absence of multiple colluding Sybil nodes results in the failure to control more than one vehicle in distinct ways (e.g. induce one to accelerate and the other to decelerate), which results in a higher time to collision in scenario 4 (b).

3.3.5 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. While the investigation of this sce-

nario using other topologies such as bidirectional may yield interesting results, we leave it for future work.

The simulations have shown that colluding Sybil nodes can cause high speed accidents with the use of the message falsification attack. We also present the position hijacking attack. In the scenarios that use hijacking, it is possible to use other non-member 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 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.

In the following chapters, we present and evaluate our proposed solution to the aforementioned attacks. By taking advantage of the fact that position falsification is required to conduct such attacks, we tackle the ability to lie about the location by using an IVC approach between RSUs that perform node positioning and vehicles that must prove their location.

4 PROPOSED COUNTERMEASURE: LOCATION-PROOF MECHANISM

Location-based services have become popular in mobile networks. Applications and service providers leverage user's positions to provide customized content or benefits for users that are in a specific region. Users usually determine their location by one or more of the following methods: Global Positioning System (GPS); cellular networks using techniques such as Time/Angle of Arrival (ToA/AoA); or by utilizing the access point position and coverage information (Cell ID). They share this location with a service provider, which in turn processes the request, delivers customized content or performs a task based on the reported location.

The use of positioning is prevalent in VANETs in order to achieve cooperative awareness. Each node finds its position and shares it with neighbors along with additional information such as its current speed, acceleration and identification. The nodes must trust that the transmitted position is legitimate and has not been falsified. In this chapter, we present a location-proof mechanism tailored for VANETs that can be used to tackle Sybil and position falsification attacks presented in Chapter 3. Section 4.1 details the mechanism design in relation to the architecture, protocol and how the proof dissemination occurs. Section 4.2 presents the plausibility model considered in this work, and Section 4.3 provides a qualitative security analysis of the mechanism.

4.1 Mechanism Design

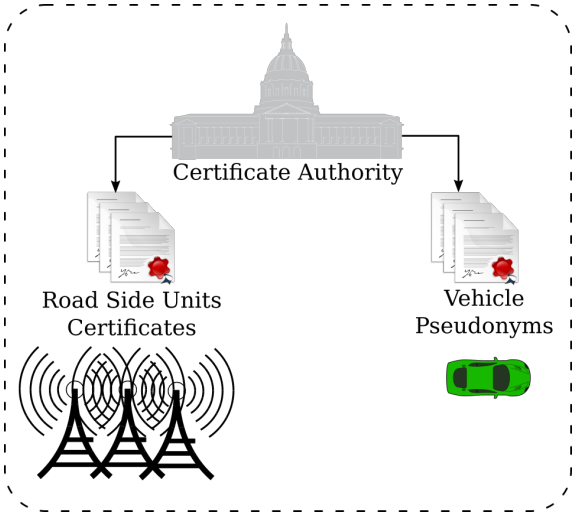
This section presents the VANET-tailored location-proof mechanism. The entities hierarchy is detailed below while the next subsection comprehends the design of the protocol for proof subscription and dissemination.

4.1.1 System Architecture

The design of the proof mechanism takes into account the Public Key Cryptography (PKI) and Elliptic Curve Digital Signature Algorithm (ECDSA) cryptography primitives as building blocks. A Certificate Authority (CA) supplies signed certificates to RSUs and multiple certificates to vehicles, which are used as pseudonyms. Figure 4.1 depicts the certificates distribution. The design of the mechanism was intended to be indepen-

dent to the authentication protocol, that is, distinct pseudonym schemes could be applied provided that the certificates can have its authenticity verified and the nodes have private/public key pairs related to the certificates. This procedure should be performed prior to the proof request as it requires such resources to be loaded at the RSUs and vehicles.

Figure 4.1: Certificates distribution by Certificate Authority



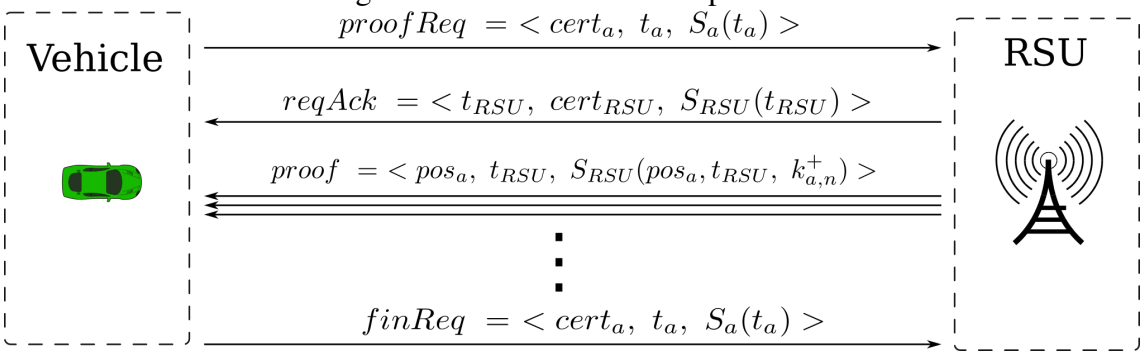
4.1.2 Proof-of-location Protocol

The design accomplishes the support of trusted positioning for neighbor vehicles, and is divided into three phases: register; proof stream; and unregister. The trusted positioning, hereby referenced as *proof*, is provided by RSUs once the vehicles register by using a *proofReq* request. Figure 4.2 details the protocol. As in ETSI standards, the proposed mechanism does not protect the confidentiality of messages, as they are not encrypted. Instead, we focus on protecting the integrity and authenticity through the use of ECDSA. A discussion on the security analysis of the protocol is included in Section 4.3. Once a *proofReq* is received, the RSU validates the certificate, extracts the public key from the certificate and verifies the signature. The timestamp should be checked for a time boundary to avoid replay attacks. A *reqAck* is sent to the vehicle to confirm its registration and includes the certificate of the RSU, a timestamp and a digital signature. The vehicle is then able to verify the authenticity of the RSU and extract the public key from the certificate in order to validate the signature of *reqAck* and the succeeding *proofs*. After sending a *reqAck*, the RSU begins to provide periodic *proofs* to the vehicle. A *proof* consists of the position coordinates, a timestamp and the signature of the data containing

the position, timestamp and the vehicle's public key. This *proof*, as will be further detailed, is relayed by the vehicle to its neighbors as an assurance that it is not lying about its location. For this present dissertation, we assume that the neighbor vehicles already possess the RSU's public key, in order to verify the *proof* digital signature. To unregister, a vehicle may send a *finReq* request at any time.

It is worth noting that only the timestamp is used as data for generating the digital signature of *proofReq*, *reqAck* and *finReq* since the certificate already contains a signature by the CA itself that can be used to assert its integrity and authenticity. Therefore it is not required to double sign the certificate. Figure 4.2 represents a certificate of entity x as $cert_x$, timestamp of entity x as $timestamp_x$, signature of data y by entity x as $S_x(y)$, position of entity x as pos_x and public key of pseudonym n for the entity x as $k^+_{x,n}$. The vehicle entity is represented by a and the roadside unit as RSU.

Figure 4.2: Proof-of-location protocol



4.1.3 Mechanism Operation

Figure 4.4 includes a broader view of the mechanism, presenting not only the *Proof Acquisition*, but also the *Beaconing and Position Verification*. Proof acquisition comprehends the position estimation of the vehicle by the RSU, *proof* generation and transmission. There is no overhead in estimating the position inherent to the proposed mechanism since 5G communication base stations have to continuously track user equipments (in our case, vehicles) in order to apply beamforming to the transmission. The RSU generates the signature and assembles the *proof* for transmission. The proof acquisition is an asynchronous procedure in relation to beaconing and position verification. The ETSI standards define that the *beaconing* is performed at 10 Hz frequency. If *Proof Acquisition* is also performed at 10 Hz frequency, then a *proof* will be included in every *beacon* trans-

mission. Otherwise, nodes will use the latest stored *proofs* received by its peers so that subsequent beacons can be verified based on a plausibility check. If a *proof* was acquired and not yet broadcast, it will be included in the *beacon*. Once neighbors receive a *beacon*, they verify if a *proof* is included and, if so, verify its signature. If the proof passes the test, then it is stored. For every *beacon* that is received, a *Plausibility Check* is executed and the beacon is classified as plausible or anomalous. The *Plausibility Check* is an independent component of our mechanism. Its purpose is to classify a position reported by a vehicle based on the last *proof* received given a time difference between the *proof* and *beacon*. In Section 4.2 we include the model used for the present evaluation. An important aspect of the *proof* is its *staleness*, i.e., its age. As shown in Figure 4.4, there is a gap between the vehicle's position estimation and the usage of the *proof* by neighbor vehicles. As the vehicles are moving, the position contained in the *proof* will always be outdated, meaning that at the time of verification it will have already changed. The *staleness* of the *proof* is directly tied to the plausibility check; the older the proof, the broader will be the position acceptance.

Figure 4.3: Illustration of events for proof dissemination

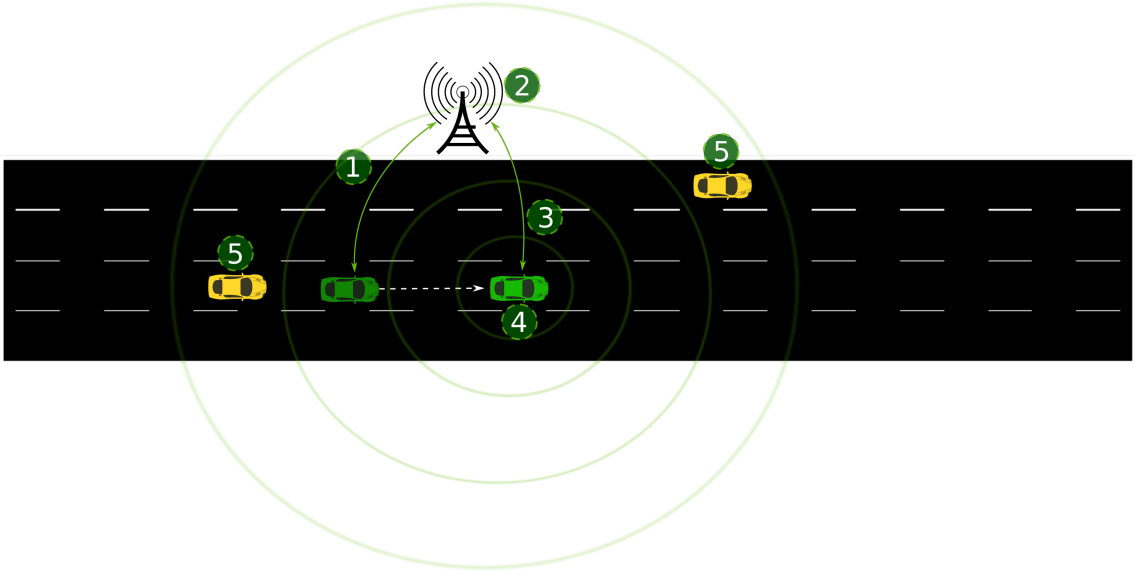


Figure 4.5 includes an example of a timeline comprising the *Proof Acquisition* and *Beaconing and Position Verification*. In this example, a *proof* is acquired at 2 Hz frequency while *beaconing* is performed at 10 Hz frequency. According to the aforementioned design of the mechanism, the plausibility check will be performed at the reception of every *beacon*.

Figure 4.4: Timeline with proof acquisition and beaconing/position verification

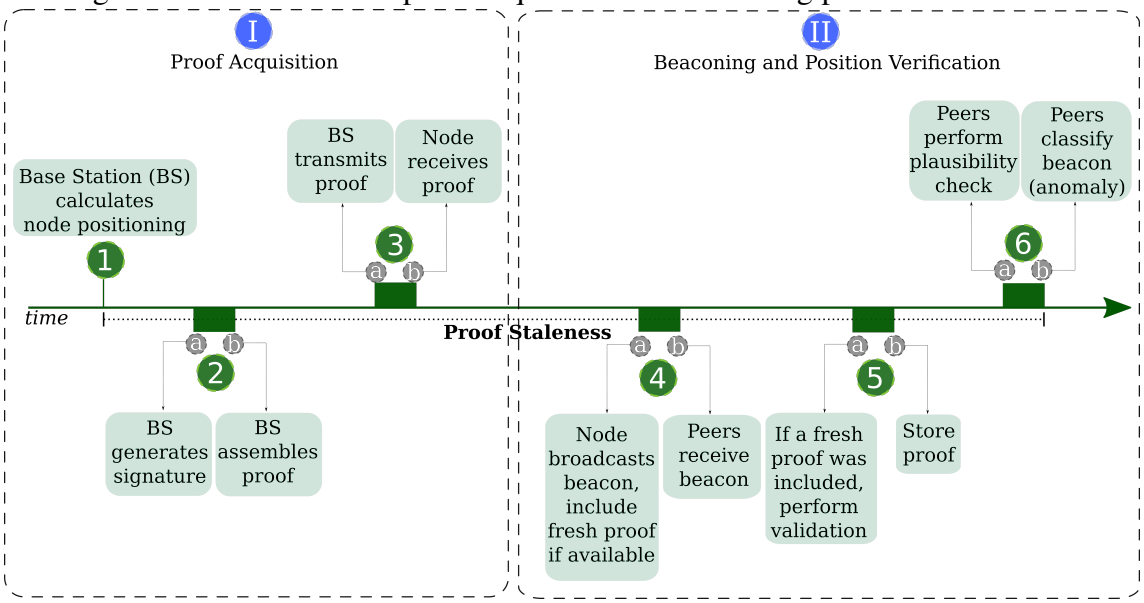
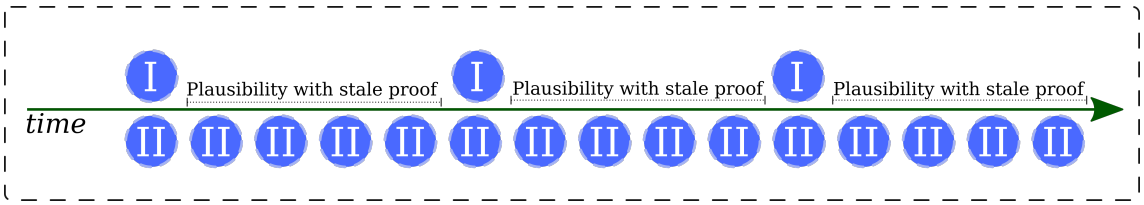


Figure 4.5: Example of proof acquisition with 2 Hz and beacon transmission/plausibility check events



4.2 Plausibility Check Model

The *Plausibility Check Model* is a pluggable component that takes a *proof* and a *beacon timestamp* in order to determine a position boundary that a vehicle could report given a $\delta time$ from the *proof timestamp* and the *beacon timestamp*. That means the plausibility model will calculate the minimum and maximum positions that the vehicle could achieve if it accelerated, braked or turned. Another approach is to use a Probabilistic Density Function (PDF) that calculates the likelihood of the vehicle reaching the position reported in the *beacon*. We leave the study of such approach to a future work.

Equations 4.1 and 4.2 represent the calculation of the X and Y positions, respectively. In this study, we consider a min $\ddot{x} = -8$ and max $\ddot{x} = 2.5$. The max yaw rate is considered to be 30 degrees, which is converted to radians to be applied in the equation. Equation 4.1 is derived from the Constant Velocity (CV) model while Equation 4.2 is

derived from the Constant Turn Rate and Velocity (CTRV) model.

$$x_{k+1} = x_k + \dot{x}_k \cdot \Delta t + \ddot{x}_k \cdot \frac{1}{2}\Delta t^2 \tag{4.1}$$

$$y_{k+1} = y_k + \frac{\dot{x} + \Delta t \ddot{x}}{\dot{\psi}}(-cos(\psi + \dot{\psi}\Delta t) + cos(\psi)) \tag{4.2}$$

x, y : position (m)

$\dot{x}, \dot{y}$: velocity (m/s)

$\ddot{x}, \ddot{y}$: acceleration (m/s^2)

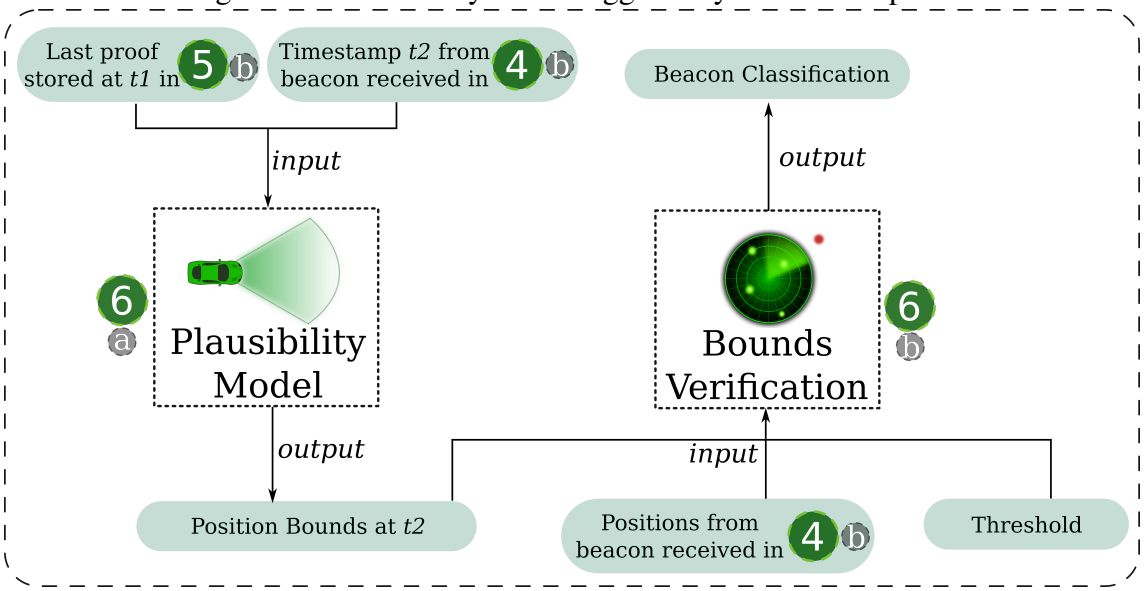
$\dot{\psi}$: Yaw Rate (rad)

ψ: Heading (rad)

Δt: Time difference between proof and beacon (s)

Figure 4.6 depicts the plausibility check process with references to Figure 4.4. The last saved *proof* and the timestamp of the *beacon* to be verified are used as input. As a result, position bounds are derived and used in the bounds verification along with the positions received in the *beacon* and a *threshold*. The *threshold* is a parameter required due to possible inaccuracies in the position estimation.

Figure 4.6: Plausibility check triggered by beacon reception



4.3 Security Analysis

In this section, we provide a qualitative security analysis of the proof-of-location mechanism. We define an attacker model and evaluate threats to the proposed model. The quantitative results are presented later in Chapter 5.

4.3.1 Threat Model

An internal attacker is considered to have valid credentials and to be able to capture and manipulate packets that other peers transmit. In this analysis, attacks on the availability property are disregarded. We consider that these are not specific to the proposed mechanism. The evaluation is focused on the confidentiality/privacy, integrity and authenticity properties. The following list provides an overview of the attacker capabilities.

- Confidentiality/Privacy

  Identity Disclosure

  Vehicle Tracking

  Subscription of Proofs for False Identities

- Integrity

  Establishment of Rogue RSUs

- Authenticity

  Replay of Proofs from Neighbor Peers

  Based on the presented threat model, the risks evaluation is detailed in the following subsection.

4.3.2 Risks Evaluation

Identity Disclosure. The protection of privacy is crucial in the context of VANET and the disclosure of a vehicle's real identity is an important concern. The design of this proof mechanism takes into consideration the use of independent authentication schemes.

The pseudonym protocol can be plugged as a mechanism provided that a vehicle holds a certificate signed by a trusted authority plus a public/private key pair. The registration is then performed with the use of pseudonyms, which preserves the real identity of the nodes.

Vehicle Tracking. Vehicle tracking can occur if the same identity is used for a long period of time. A common approach to avoid tracking is to use pseudonym-changing schemes. The proof mechanism was designed in a way that the employment of these schemes can be sustained with the use of proof of location. When a change of pseudonym occurs, a new registration shall be performed using the fresh pseudonym. A constraint exists in relation to the use of silent periods, in which nodes do not communicate for an extent of time. However, since the absence of communication prevents nodes to share information anyway, this is not a limitation of our mechanism.

Subscription of Proofs for False Identities. In order to disclose the positioning of third party vehicles, an attacker could attempt to register to proofs for other vehicles. Since the *proofReq* request contains a digital signature, the attacker is unable to generate the request. Even though the timestamp is signed in the request, we consider that a replay attack could be successful. Once a vehicle sends a *proofReq*, an attacker could capture it and immediately send it to the RSU. However, once a vehicle has subscribed to location proofs, it is willing to share its location with the neighbors and the attacker would be able to eavesdrop the vehicle's position in the proofs nonetheless. Therefore an attacker would fail to achieve any benefit in performing a replay attack of the *proofReq*.

Establishment of Rogue RSUs. An attacker could attempt to impersonate an RSU in order to feed falsified proofs into subscribing vehicles and disrupt the behavior of VANET applications. By mimicking an RSU, an attacker could lure vehicles into registering in the rogue RSU. The *reqAck* packet exists in order to stop such attacks. Before accepting proofs from an RSU, a vehicle must verify the certificate, the signature and the timestamp included in the *reqAck*. The vehicle should accept the proofs only if the certificate is trustworthy, the signature is valid and the timestamp is within an expected boundary.

Replay of Proofs from Neighbor Peers. Proofs are meant to be shared among a group of nodes interested in verifying the position of peers in a VANET. Attackers may be motivated to conduct the hijacking of positions of victim nodes by attempting to steal their proofs. However, a proof is composed of the node's position, the RSU's timestamp and a signature that contains the position, timestamp and the public identity of the vehicle.

If an attacker replays the proof received from any of its peers, the verification of the proof will not be successful given that the attacker's identity differs from the proof's signed identity. The tampering of the proof would require the attacker to obtain the private key of the RSU. If an attacker has the private key of an RSU, then it would be able to generate its own false proofs without the need of replaying.

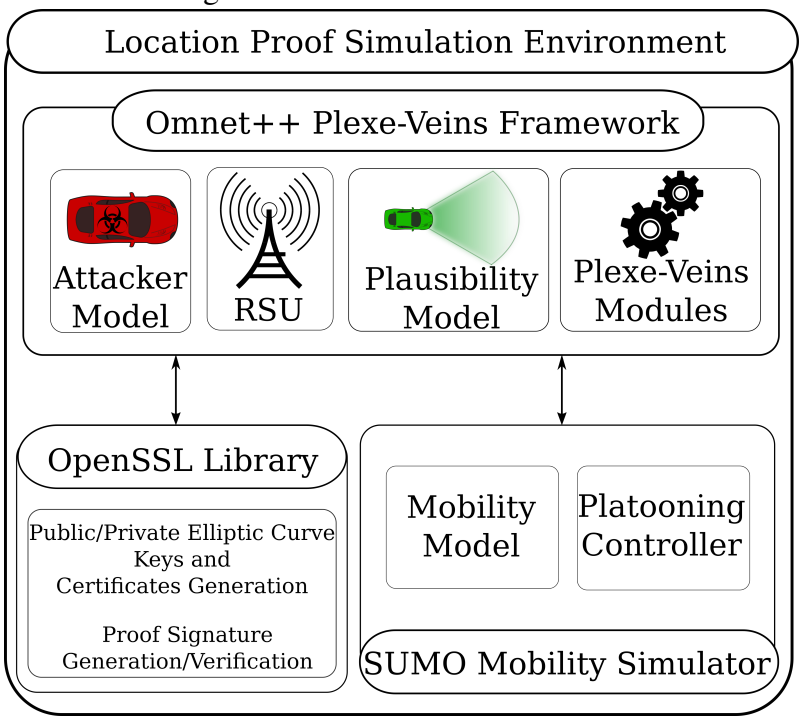
5 PROOF MECHANISM EVALUATION

In this chapter, we perform an evaluation of the proof-of-location mechanism presented in Chapter 4. The attacks presented in Chapter 3 are referenced herein and are used to assess the effectiveness of the proof. Section 5.1 details the simulation environment and the parameters used in the evaluation. Section 5.2 explains the metrics used to evaluate the mechanism. Section 5.3 contains an analysis of the effect of distinct proof frequencies in the proof staleness while section 5.4 shows the evaluation results.

5.1 Simulation Environment

The evaluation of the proof mechanism was performed using the Plexe simulation framework. The mechanism was implemented by using the OpenSSL APIs to perform the cryptographic operations. The networking model was developed using Plexe on top of the Omnet++ framework. As illustrated in Figure 5.1, the attacker model detailed in Section 3.1 is used to evaluate the detection metrics of the mechanism when an attack is being conducted. A model of the RSU that will provide the proofs is implemented in Plexe and connected to the external module that provides the cryptography operations. The plausibility model introduced in Section 4.2 is included as a platooning application of the simulator. The simulation parameters are similar to those presented in Section 3.2, and are included in Table 5.1. Three new parameters are used, *Proof Size*, *Proof Frequency* and *Plausibility Check Threshold*. Proof size is the amount of data that needs to be transferred for each proof and is measured in *bytes*. Proof frequency is the amount of proofs per second that will be provided by the RSU to the vehicles, measured in Hz. The plausibility check threshold is a tolerance of the position accuracy error by the positioning mechanism in the RSU. It is used during the classification of the reported neighbor position. We consider that the positioning technology has a noise given by a normal distribution of mean 0 and a standard deviation 0.5. The combination of distinct proof frequencies and plausibility check thresholds generates 16 simulation setups. Each of these setups has run 33 times with different seeds, resulting in 528 runs in total.

Figure 5.1: Simulation architecture



5.2 Evaluation Metrics

The mechanism evaluation is performed using a set a metrics defined in this section. The following list defines the variables used to derive the accuracy, false positive and negative rates. A falsified beacon is a beacon that contains a position that was manipulated by the attacker. A correct beacon contains a legitimate position that was not modified by an attacker. A *detection* is a classification of the beacon as not being plausible by the plausibility model.

- True Positive (TP): Falsified beacon is detected
- True Negative (TN): Correct beacon is identified as such
- False Positive (FP): Correct beacon is detected as falsified
- False Negative (FN): Falsified beacon is NOT detected

Based on these variables, we evaluate four metrics: Accuracy (ACC), True Positive Rate (TPR), False Negative Rate (FNR) and False Positive Rate (FPR). Accuracy is the description of systematic errors in the detection mechanism and provides a view of the trueness of the results. Equation 5.1 details the accuracy calculation. The TPR, given by Equation 5.2, provides the rate of correct detection of attacks. On the other hand,

Table 5.1: 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 (SANTINI et al., 2015)
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 ($m = 3$)
Proof size	96 bytes
Proof Frequency	10 Hz, 5 Hz, 2 Hz, 1 Hz
Plausibility Check Threshold	1 σ, 2 σ, 3 σ, 4 σ

Equation 5.3 provides the calculation of the FNR that details the rate of attack beacons that were not detected by the mechanism. In Equation 5.4, FPR is defined and represents the rate of correct beacons that were detected.

$$ACC = \frac{TP + TN}{TP + FP + FN + TN} \tag{5.1}$$

$$TPR = \frac{TP}{TP + FN} \tag{5.2}$$

$$FNR = \frac{FN}{TP + FN} \tag{5.3}$$

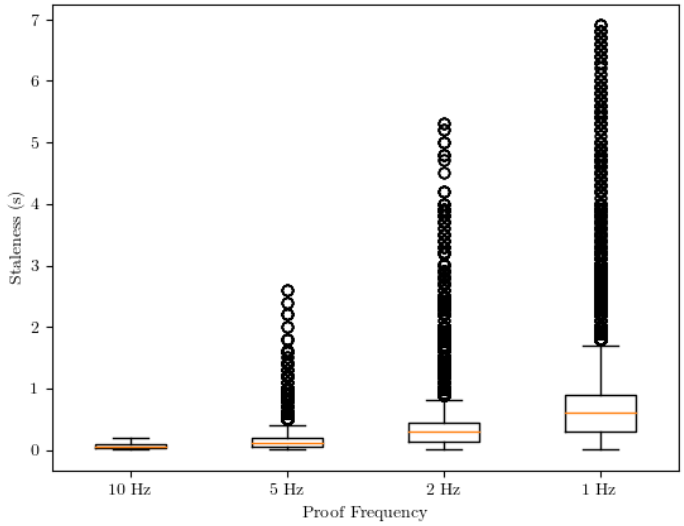
$$FPR = \frac{FP}{FP + TN} \tag{5.4}$$

5.3 Proof Staleness Analysis

The frequency at which vehicles receive fresh proofs dictates the broadness of the position acceptance during the plausibility check. That means that the older the proof is, the larger is the amount of displacement of the vehicle in relation to the proof position. On the other hand, the more recent the proof is, the more certainty a verifier can have about

the location of the prover. We refer to such proof age as the *proof staneless*. The staleness can vary due to different proof providing frequencies or packet loss. Recall Figure 4.4, if a loss occurs in 4b when a proof was provided, there is no retransmission and the node will only receive another proof when the sending node receives a fresh proof from the RSU and transmits it to the neighbors. Such loss will cause the peer to use a previously saved proof with a higher staleness to perform the plausibility verification. Figure 5.2 depicts the proof staleness for distinct frequencies. The box is limited by the first and third quartiles and the median is represented by the orange line in the box. The black circles are outliers that fall out of the third quartile plus 1.5 IQR (Interquartile Range).

Figure 5.2: Proof staleness given distinct proof frequencies



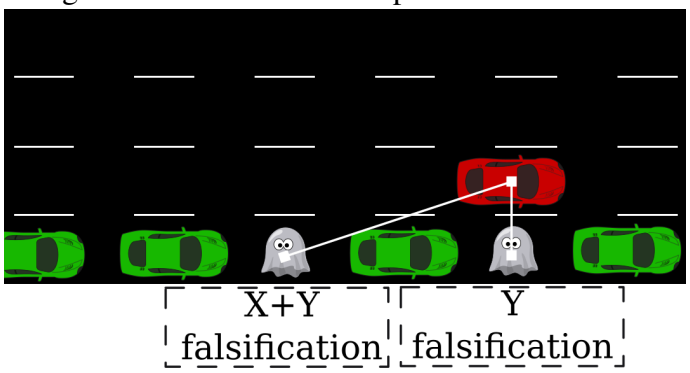
The increase in the staleness consequently causes a rise in the false negative rate, as shown in the results in the next section. Although the use of lower proof frequencies incur in a lower overhead in the vehicular network, false beacons might have a lower chance to be detected and negatively influence a VANET application. The next section provides detailed results regarding simulations with distinct proof frequencies and the effect they cause in detection in conjunction with varying thresholds.

5.4 Attack Simulation Results

Given that the simulation environment and evaluation metrics have been presented, the attack simulation results are described in this section. While the plots and results analysis are related to the first attack scenario, the relevance of these results for other presented attacks is equal. Since the attack requirements are alike, detailed results are

shown for the first attack scenario only (Falsification presented in Section 3.1). Results show that falsified nodes can be detected during the first phase of attack, even before they begin the position falsification that will cause unwanted behavior in the controllers. Recall from Section 3.1 that an attacker travels on the lane besides the platoon. Figure 5.3 illustrates the coordinates falsification that the attacker must perform in order to conduct the attack. To make the attack harder to detect, the attacker could travel right beside the position of the false node, which in turn minimizes the amount of position error. We consider this to be the case so that the mechanism detection effectiveness can be evaluated against the case that is most beneficial to the attacker.

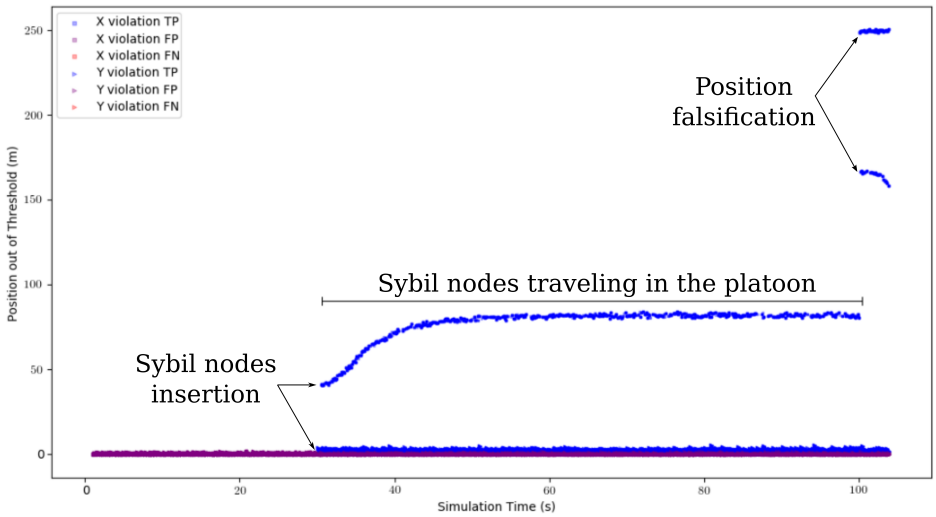
Figure 5.3: Attack scenario position falsification



As described in the simulation environment, two parameters are iterated to evaluate the detection of attacks: proof frequency and threshold. For each of the proof frequencies, there is a distinct simulation considering one of the thresholds. In Figure 5.4, results are included for 10 Hz frequency and 1 σ threshold. In this plot, blue marks are either X or Y positions that are out of the bounds and were correctly detected by the model, hence classified as true positives. False positives are represented by purple marks and can be caused by noise in the positioning accuracy combined with an insufficient threshold. False negatives are red marks in the Y axis value of zero since they are within bounds but were not detected. In the plot, the Y axis measures the amount of distance that the beacon fell out of the bounds calculated by the model while the X axis is the simulation time.

At simulation time 30 s, the Sybil nodes are introduced in the platoon formation. Even though the attacker operates the controller without any modification until 100 s, it is possible to detect incorrect positions with the use of the proofs. As it can be observed, purple marks are noticeable specially before simulation time 30 s. These marks represent false positives, it means that the position noises of the beacon and the proof combined were sufficient to make the reported position to fall out of the bounds. It also means that

Figure 5.4: Detection results using 10 Hz proof frequency and 1 σ



the use of such threshold is prone to cause false positives. In Figure 5.5, the detection metrics for this simulation are shown. The use of a small threshold resulted in a high detection rate, that is, a high TPR and low FNR. Associated with a high TPR, a high FPR causes the drop in accuracy once correct beacons are often detected. The use of small thresholds are suitable when positioning technologies are better, i.e., the better the positioning accuracy, the lower the threshold can be.

Figure 5.5: Metrics using distinct proof frequencies and 1 σ

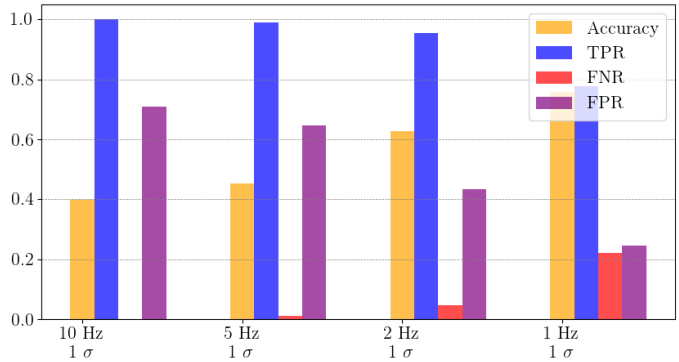
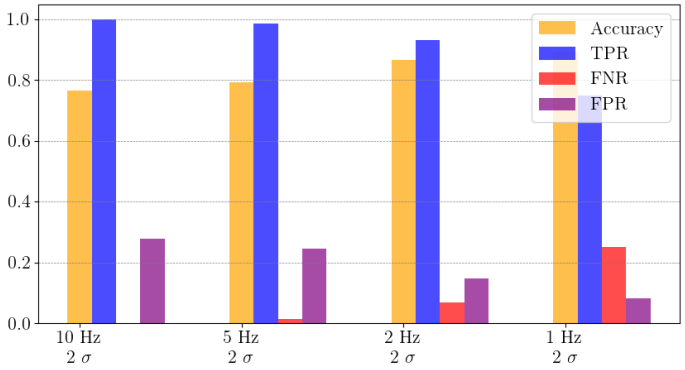


Figure 5.6 depicts the detection metrics for 2 σ threshold. As can be observed, the reduction in the false positive rate is significant and causes a rise in the accuracy. The increase of threshold incurs in a slight increase of the FNR for 5, 2 and 1 Hz proof frequencies. This occurs since the acceptance of error boundaries increases and ends up in accepting a higher number of false positions. Recall from Figure 5.3, the required position falsification for the Sybil node beside the attacker is short. A high threshold in

conjunction with a lower proof frequency means that such distance may fall within the permitted bounds and therefore increase the FNR.

Figure 5.6: Metrics using distinct proof frequencies and 2 σ



The results for threshold 3 σ are depicted in Figure 5.7 and the tendency presented in the last graphs is preserved. False positives are further reduced while false negatives are slightly increased. For brevity reasons, we do not include plots for threshold 4 σ as the same behavior is maintained. It is possible to observe that the lower the threshold is, the higher the FPR. Likewise, the higher the threshold is, the higher the FNR. It is fair to highlight that this evaluation considers the best scenario for the attacker, the malicious vehicle travels right beside the false node's position and remains driving stable during the course of the attack. While in a real world attack it would be harder to achieve such scenario, a well-motivated attacker could still be able to accomplish this action.

Figure 5.7: Metrics using distinct proof frequencies and 3 σ

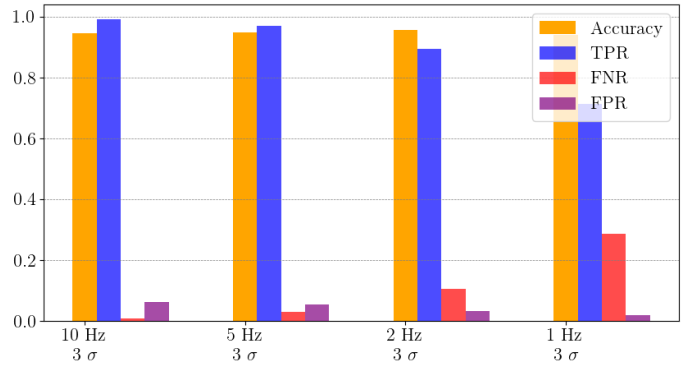
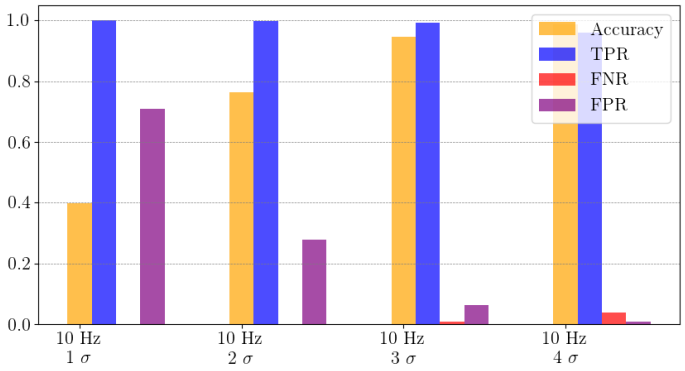


Figure 5.8 shows a comparison of distinct thresholds for 10 Hz frequency proofs. In this graph, it becomes easier to observe the mentioned relation between the thresholds and decreasing false positive rate in relation to the increasing false negative rate. Recall that the metrics correspond to each evaluated beacon. Provided that the environment will not likely be under attack for the majority of time, a lower FPR at the cost of a small FNR

increase appears to be feasible. This reduces the amount of false alarms and increases the trustworthiness of the detection when an alarm does occur.

Figure 5.8: Metrics comparison of 10 Hz proofs



A consolidated view of the detection parameters is provided in Figure 5.9. The results show that lower thresholds tend to generate more false positives. The wealth of false alarms may discourage users to trust the mechanism or induce systems to take wrong decisions in the first place. Therefore, a more conservative approach would be to choose higher thresholds combined with higher proof frequencies in order to minimize the amount of false positives and false negatives.

Figure 5.9: Consolidated metrics results

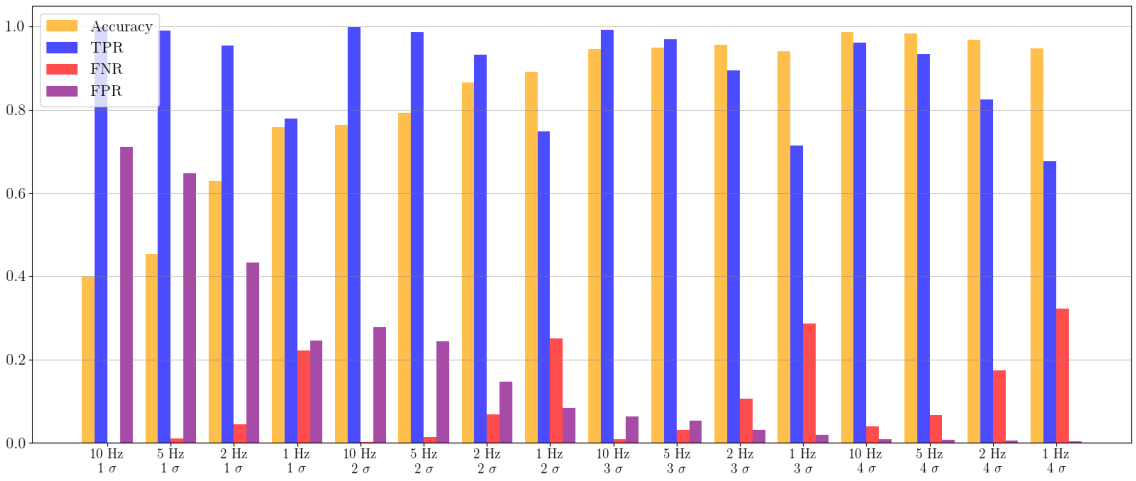
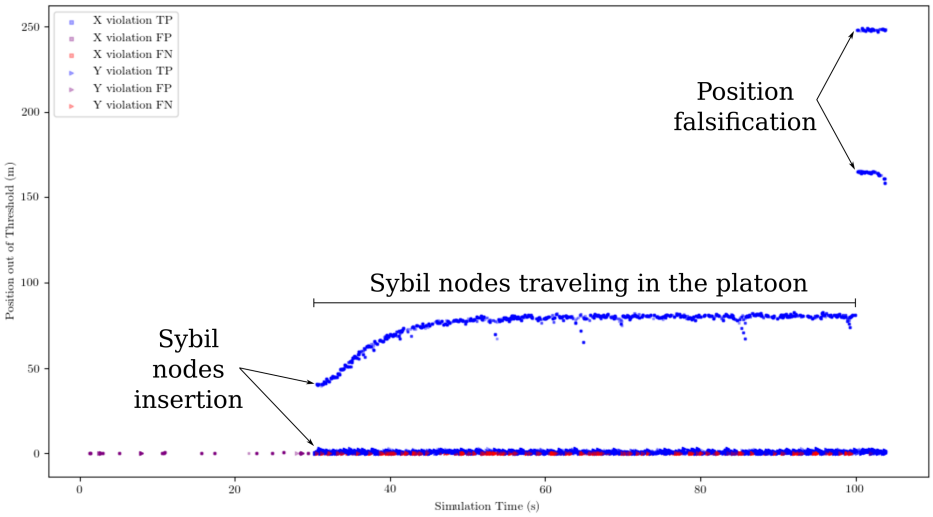


Figure 5.10 illustrates a conservative approach. There are few false positives, and true positives become predominant once Sybil nodes join the platoon. The first part of the detection is generic to all evaluated attack scenarios in this work. Since the detection does not depend on the manipulation of position to cause disturbances in the controller (represented by "Position falsification" in Figure 5.10), false nodes may be detected in the first phase of the attack (represented by "Sybil nodes traveling in the platoon" in Figure

5.10). One could claim that an attacker would start the second phase immediately after the first phase, which could reduce the time window available for detection. The authors consider that the proof-of-location mechanism should be used as a security requirement for position-critical applications, such as platooning. The proofs supply should start at the join request of a vehicle to a platoon so that a bond of trust is established between the nodes. With that said, the proposed mechanism may be convenient in the trust establishment between nodes and the protection against position-based attacks.

Figure 5.10: Detection results using 5 Hz proof frequency and 4 σ



6 CONCLUSION AND FUTURE WORK

Vehicular ad hoc Networks are emerging to provide fascinating novel technologies that may ameliorate vehicular traffic altogether. The challenges to create secure and dependable connected vehicular applications are as substantial as the benefits that can be produced. Security must be an essential design requirement as cyber attacks could result in the injury of people or ultimately in the loss of lives. The increasing interest in Industry has led to the design and deployment of many vehicular network applications. The attention in Academia has also increased given the research challenges associated, where security is of paramount relevance.

Summary of contributions

In this dissertation, we first work on identifying risks associated with misbehaving vehicles, either by attackers or possibly due to the effect of malware. Through the modeling of a threat agent in the context of Sybil and message falsification attacks, the impacts of different attack scenarios are evaluated. The simulation results have 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 that is not trustworthy. 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.

Position falsification is the fundamental requirement to execute Sybil and the falsification attacks to interfere with the platooning controller. Based on that, a proof-of-location mechanism is designed and evaluated in order to provide position assurance. We demonstrate that the use of location proofs combined with a plausibility model can counteract the presented attacks. Results show that by tuning the threshold and proof frequency it is possible to achieve a low false positive and false negative rates in the detection metrics. Finally, the use of the proposed proof-of-location mechanism is motivated as a security control for position-dependent critical applications as platooning. Requiring

nodes to share location proofs since the platoon join request can be a countermeasure to Sybil and further falsification attacks.

Directions for future research

The proposed proof-of-location mechanism has shown to perform well in the detection metrics under the studied constraints. However, future work opportunities are open and are outlined below.

Regarding use cases, the experiments have covered Sybil and message falsification attacks in platooning although the application of the proposed mechanism may be useful in other contexts. For example, Sybil attacks are also a threat to the VANET context in which a misbehaving node desires to control a large portion of the system or generate a large amount of alarms. In addition, position-based routing could also benefit from the location proofs to thwart attacks on the routing protocols.

With respect to the plausibility model, the more sophisticated and confident of the prediction of a peer state is, the better the detection metrics will be. Given that the proof-of-location mechanism is not bound to any specific model, the advancement of this component can certainly improve the detection results.

In dense networks, vehicles may experience higher collision rates and may need to switch RSUs frequently. The present study focuses on the analysis of the sharing of the proofs and attack detection. An analysis of the behavior of the mechanism in dense networks is left for future research.

REFERENCES

AMOOZADEH, M. et al. Platoon management with cooperative adaptive cruise control enabled by vanet. **Vehicular Communications**, Elsevier, v. 2, n. 2, p. 110–123, 2015.

AMOOZADEH, M. et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. **IEEE Communications Magazine**, v. 53, n. 6, p. 126–132, June 2015. ISSN 0163-6804.

BERESFORD, A. R.; STAJANO, F. Location privacy in pervasive computing. **IEEE Pervasive Computing**, IEEE Educational Activities Department, v. 2, n. 1, p. 46–55, jan. 2003. ISSN 1536-1268.

BUSSARD, L.; BAGGA, W. Distance-bounding proof of knowledge to avoid real-time attacks. In: SASAKI, R. et al. (Ed.). **Security and Privacy in the Age of Ubiquitous Computing**. [S.l.]: Springer US, 2005. p. 223–238. ISBN 978-0-387-25660-3.

BUTTYÁN, L. et al. Slow: A practical pseudonym changing scheme for location privacy in vanets. In: IEEE. **2009 IEEE Vehicular Networking Conference (VNC)**. [S.l.], 2009. p. 1–8.

CALANDRIELLO, G. et al. Efficient and robust pseudonymous authentication in vanet. In: **Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks**. [S.l.]: ACM, 2007. (VANET '07), p. 19–28. ISBN 978-1-59593-739-1.

DADRAS, S.; GERDES, R. M.; SHARMA, R. Vehicular platooning in an adversarial environment. In: **Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security**. [S.l.]: ACM, 2015. (ASIA CCS '15), p. 167–178. ISBN 978-1-4503-3245-3.

DAMGÅRD, I. Commitment schemes and zero-knowledge protocols. In: **Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School, Aarhus, Denmark, July 1998**. [S.l.]: Springer-Verlag, 1999. p. 63–86. ISBN 3-540-65757-6.

DEBRUHL, B. et al. 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**. [S.l.]: ACM, 2015. (WiSec '15), p. 22:1–22:11. ISBN 978-1-4503-3623-9.

DESMEDT, Y. Major security problems with the 'unforgeable'(feige)-fiat-shamir proofs of identity and how to overcome them. In: **Proceedings of SECURICOM**. [S.l.: s.n.], 1988. v. 88, p. 15–17.

DOUCEUR, J. R. The sybil attack. In: **Revised Papers from the First International Workshop on Peer-to-Peer Systems**. [S.l.]: Springer-Verlag, 2002. (IPTPS '01), p. 251–260. ISBN 3-540-44179-4.

FREUDIGER, J. et al. Mix-zones for location privacy in vehicular networks. 2007.

HAITNER, I.; REINGOLD, O. Statistically-hiding commitment from any one-way function. In: **Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing**. [S.l.]: ACM, 2007. (STOC '07), p. 1–10. ISBN 978-1-59593-631-8.

HALEVI, S.; MICALI, S. Practical and provably-secure commitment schemes from collision-free hashing. In: **Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology**. [S.l.]: Springer-Verlag, 1996. (CRYPTO '96), p. 201–215. ISBN 3-540-61512-1.

HASAN, R.; BURNS, R. Where have you been? secure location provenance for mobile devices. **arXiv preprint arXiv:1107.1821**, 2011.

HASAN, R. et al. Woral: A witness oriented secure location provenance framework for mobile devices. **IEEE Transactions on Emerging Topics in Computing**, v. 4, n. 1, p. 128–141, Jan 2016. ISSN 2168-6750.

KAFIL, P.; FATHY, M.; LIGHVAN, M. Z. Modeling sybil attacker behavior in vanets. In: **2012 9th International ISC Conference on Information Security and Cryptology**. [S.l.: s.n.], 2012. p. 162–168.

KHAN, R. et al. Otit: Towards secure provenance modeling for location proofs. In: **Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security**. [S.l.]: ACM, 2014. (ASIA CCS '14), p. 87–98. ISBN 978-1-4503-2800-5.

KOIVISTO, M. et al. Continuous high-accuracy radio positioning of cars in ultra-dense 5g networks. In: **2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)**. [S.l.: s.n.], 2017. p. 115–120.

LAMMERT, M. P. et al. 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**, v. 7, n. 2014-01-2438, p. 626–639, 2014.

LUO, W.; HENGARTNER, U. Veriplace: A privacy-aware location proof architecture. In: **Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems**. [S.l.]: ACM, 2010. (GIS '10), p. 23–32. ISBN 978-1-4503-0428-3.

NAKAGAMI, M. The m-distribution—a general formula of intensity distribution of rapid fading. In: HOFFMAN, W. (Ed.). **Statistical Methods in Radio Wave Propagation**. [S.l.]: Pergamon, 1960. p. 3 – 36. ISBN 978-0-08-009306-2.

PETRILLO, A.; PESCAPé, A.; SANTINI, S. 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)**. [S.l.: s.n.], 2017. p. 110–115.

PLOEG, J. et al. Controller synthesis for string stability of vehicle platoons. **IEEE Transactions on Intelligent Transportation Systems**, v. 15, n. 2, p. 854–865, April 2014. ISSN 1524-9050.

RAJPUT, U. et al. A two level privacy preserving pseudonymous authentication protocol for vanet. In: **2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)**. [S.l.: s.n.], 2015. p. 643–650.

RAJPUT, U. et al. A hybrid approach for efficient privacy-preserving authentication in vanet. **IEEE Access**, v. 5, p. 12014–12030, 2017.

RAJPUT, U.; ABBAS, F.; OH, H. A hierarchical privacy preserving pseudonymous authentication protocol for vanet. **IEEE Access**, v. 4, p. 7770–7784, 2016. ISSN 2169-3536.

RAYA, M.; HUBAUX, J.-P. Securing vehicular ad hoc networks. **J. Comput. Secur.**, IOS Press, v. 15, n. 1, p. 39–68, jan. 2007. ISSN 0926-227X.

SAJJAD, I. et al. 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**. [S.l.]: ACM, 2015. (CPS-SPC '15), p. 43–53. ISBN 978-1-4503-3827-1.

SALES, T. B. M. de et al. Asap-v: A privacy-preserving authentication and sybil detection protocol for {VANETs}. **Information Sciences**, v. 372, p. 208 – 224, 2016. ISSN 0020-0255.

SANTINI, S. et al. A consensus-based approach for platooning with inter-vehicular communications. In: IEEE. **2015 IEEE Conference on Computer Communications (INFOCOM)**. [S.l.], 2015. p. 1158–1166.

SEGATA, M. et al. PLEXE: A Platooning Extension for Veins. In: **6th IEEE Vehicular Networking Conference (VNC 2014)**. [S.l.]: IEEE, 2014. p. 53–60.

VAHIDI, A.; ESKANDARIAN, A. Research advances in intelligent collision avoidance and adaptive cruise control. **Trans. Intell. Transport. Sys.**, IEEE Press, v. 4, n. 3, p. 143–153, set. 2003. ISSN 1524-9050.

VITELLI, D. **Security Vulnerabilities of Vehicular Platoon Network**. Dissertação (Mestrado) — Universita' degli studi di Napoli Federico II, 2016.

WANG, X. et al. Stamp: Enabling privacy-preserving location proofs for mobile users. **IEEE/ACM Transactions on Networking**, v. 24, n. 6, p. 3276–3289, December 2016. ISSN 1063-6692.

WATERS, B.; FELTEN, E. Secure, private proofs of location. **Department of Computer Science, Princeton University, Tech. Rep. TR-667-03**, 2003.

YING, B.; MAKRAKIS, D.; MOUFTAH, H. T. Dynamic mix-zone for location privacy in vehicular networks. **IEEE Communications Letters**, IEEE, v. 17, n. 8, p. 1524–1527, 2013.

ZAIDI, K. et al. Data-centric rogue node detection in vanets. In: **2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications**. [S.l.: s.n.], 2014. p. 398–405. ISSN 2324-898X.

ZAIDI, K.; RAHULAMATHAVAN, Y.; RAJARAJAN, M. Diva - digital identity in vanets: A multi-authority framework for vanets. In: **2013 19th IEEE International Conference on Networks (ICON)**. [S.l.: s.n.], 2013. p. 1–6. ISSN 1531-2216.

ZHU, Z.; CAO, G. Applaus: A privacy-preserving location proof updating system for location-based services. In: **2011 Proceedings IEEE INFOCOM**. [S.l.: s.n.], 2011. p. 1889–1897. ISSN 0743-166X.

APPENDIX A. IEEE VNC ARTICLE

- Title: Effects of Colluding Sybil Nodes in Message Falsification Attacks for Vehicular Platooning
- Conference: 2017 IEEE Vehicular Networking Conference (VNC)
- URL: <www.ieee-vnc.org>
- Date: November 27-29, 2017
- Location: Torino, Italy

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*

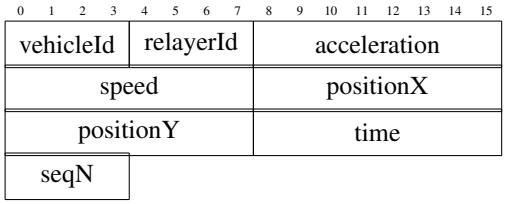


Fig. 1: Platoon beacon structure

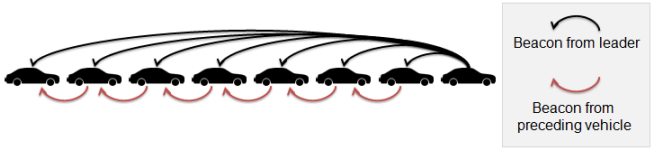


Fig. 2: Platoon topology based on beacons from the leader and preceding vehicles

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.

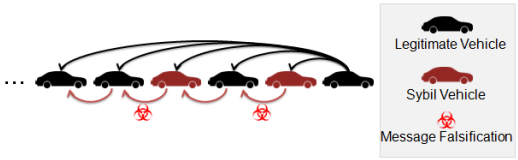


Fig. 3: Influence of Sybil nodes through message falsification

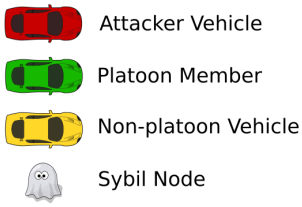
In this attack model, we assume that the owner of the identity of a vehicle is able to interfere with the content of the beacons transmitted to other members, i.e., the attacker is able to falsify information sent through IVC. This is a feasible assumption since an attacker may be able to manipulate 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.

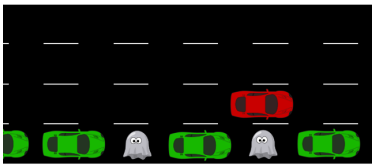
C. Attack Scenarios

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)).

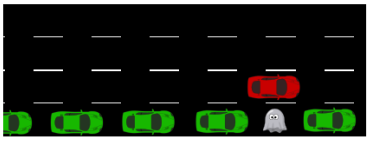
1. Falsification. The attack simulation in scenario 1 (a) consists on inserting two Sybil nodes at logical positions within the platoon that enable the attacker to control the behavior of two platoon members. An accident can be caused by manipulating the beacons during a short period so that the preceding 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.



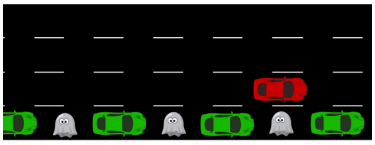
(a) Legend



(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:

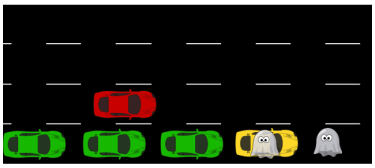
D_{err} = Deceleration distance error (m)
A_{err} = Acceleration distance error (m)
A_{con} = Controller acceleration (m/s^2)
D_{des} = Desired deceleration (m/s^2)
A_{des} = Desired acceleration (m/s^2)

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.

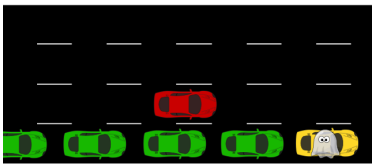
3. Emergency braking obstruction. Emergency braking is a critical event that is sensitive to faults or attacks. In scenario 3 (a), we assume that an attacker has managed to introduce a Sybil node between every pair of platoon members. This allows the attacker to manipulate the members by forging beacons, 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.

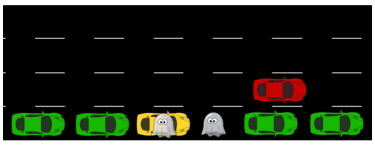
5. Vehicle position hijacking to falsify member. In this scenario, again a non-platoon vehicle is employed so that it is identified by the joining platoon member's radar. The introduction of Sybil nodes would also be possible in an already formed platoon, should a non-platoon vehicle travel close to 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.



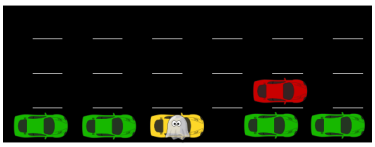
(a) Attack scenario 4 (a) on IVC/Radar-based platoon



(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.

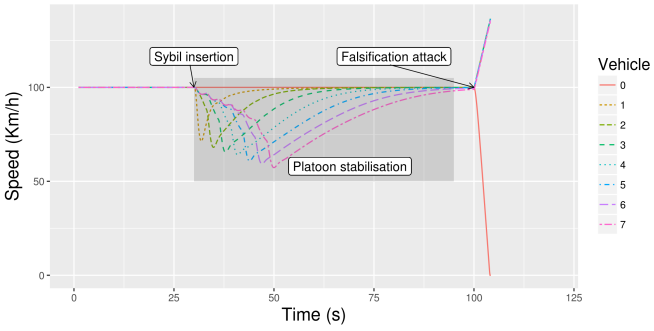
The impact of this attack affects all platoon members, which collide at high speed in a chain-reaction crash. While the leader is applying an emergency brake, the platoon members accelerate to as high as ≈137 km/h until there is a rear-end crash. Like in the previous attack, the time elapsed from the 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.

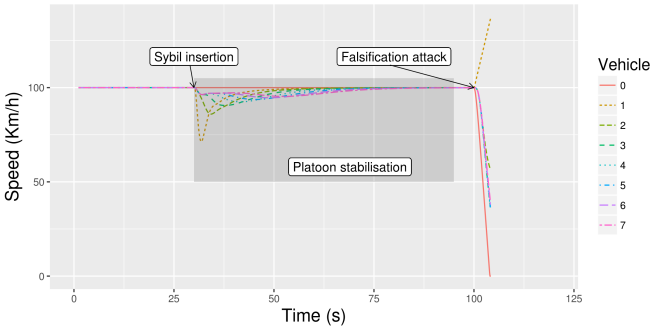
In terms of time to collision and speed difference at collision (see Table II), scenarios 3 (a) and (b) are very similar. The main difference is that, by inserting a Sybil node between every pair of vehicles, the attacker is able to make all members accelerate. This behavior can be observed in Figures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