PRIME: Platoon Restructuring for Incident Mitigation and Exclusion

Konstantinos Kalogiannis, Michael Hartmann, and Panos Papadimitratos
Networked Systems Security (NSS) Group, KTH Royal Institute of Technology, Stockholm, Sweden
{konkal, mchar, papadim}@kth.se

***Abstract*—Platooning has shown promising results in improving transportation safety and decreasing fuel consumption. Vehicles enter these formations, to form convoys, while traveling to similar destinations. However, this implies trust in the information received by the other platoon members. Insider attackers performing falsification attacks can destabilize the platoon or cause catastrophic vehicle collisions. Detecting this type of misbehavior is not without shortcomings: benign mobility deviations can be, erroneously, flagged as misbehavior. Further, even when an attack is detected, the vehicles remain affected until the attacker is excluded from the formation. Thus, in this work, we address the need for a reliable mitigation approach. We propose a platoon restructuring scheme aiming to mitigate attacks and reduce the attacker's potential for further misbehavior. Our results, and analysis, show the feasibility of our approach, which manages to restore the formation's stability even when an attack is ongoing.**

***Index Terms*—Platooning, Platoon Restructuring, Falsification Attacks, Vehicle Exclusion, Attack Mitigation, Platoon Stability**

I. Introduction

Platooning, a promising application of Intelligent Transport Systems (ITS), provides efficient transportation by better utilizing the current road infrastructure [1], [2] and leads to a reduced fuel consumption [3]. Considering passengers (drivers, or otherwise), platooning is concerned with their safety and comfort [4] attested by several Field Operational Tests (FOTs) [1], [2] in the last decade. Though, despite the efforts to secure the Vehicular Communication (VC) systems through standards, such as the IEEE 1609.2 WG [5] and European Telecommunications Standards Institute (ETSI) [6], the systems remain susceptible to attacks. These efforts promote the security of the networked systems partaking into Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) (V2X), through the use of certificates authorities that comprise the Vehicular Public-Key Infrastructure (VPKI) [7]–[9] and have alleviated issues stemming from external attackers. Nonetheless, platooning remains vulnerable to internal attackers, i.e., vehicles that join platoons possessing valid credentials. Due to the reduced gaps between the vehicles comprising a platoon, attacks that alter the disseminated kinematic properties [10] of the vehicles (through the Cooperative Awareness Messages (CAMs)) can lead to sudden collisions or destabilization of the formation [11], [12]; even when string-stable controllers [13], i.e., controllers capable of reducing the error propagation downstream, are used.

A number of works in the literature [11], [12], [14] focus on implementing Misbehavior Detection Schemes (MDSs) capable of detecting these falsification attacks in an effort to safeguard the platoons. Similar works also build well-crafted datasets to allow a uniform evaluation of those MDS [15], [16]. Recent proposals use machine learning models [17] to detect misbehavior in vehicular networks; ranging from Gaussian Mixture Models (GMMs) to deep learning approaches such as Long Short-Term Memory (LSTM). Despite their improved capabilities, MDSs are susceptible to false positives, i.e., erroneous detection of attacks. Further, detecting the misbehavior is only the first step in ensuring the safety of traveling platoons; effective mitigation is ultimately required.

On one hand, false positives inadvertently affect the platoon's behavior depending on the proposed mitigation. Striving for complete safety, vehicles operating in a platoon can decide to dissolve the platoon when misbehavior is detected. This type of mitigation not only completely negates the benefits of platooning, but also allows attackers to abuse the reaction to easily perform Denial of Service (DoS) attacks. A middle-ground approach would allow the vehicles to gradually increase their gaps based on anomaly suspiciousness [18]; however, such an approach could allow prolonged destabilization of the convoy for the duration of the attack, as the attacker preserves his position in the formation and thus his attacking capabilities.

On the other hand, detecting the misbehavior does not reduce the immediate risk for the vehicles downstream, i.e., following vehicles; the vehicle can be reported and eventually excluded through the revocation of its credentials, but vehicles downstream still require accurate information to safely operate until this happens. Excluding the detected vehicle from the platoon-appropriate information flow alters the topology required by the controller and can make it unstable. Moreover, solutions that enable the platoon to dynamically change the information flow, e.g., from bidirectional to unidirectional to isolate the attacker [19], can indirectly give the offending vehicle some control over the platoon. Thus, a proposed mitigation scheme should reduce the induced impact from misbehavior without reducing the stability of the formation or the ability of the vehicles to operate inside them.

In this work, we tackle the mitigation issues by introducing Platoon Restructuring for Incident Mitigation and Exclusion (PRIME), a mitigation scheme capable of thwarting faulty, malicious or not, information originating from vehicles upstream. Further, we manage to diminish the offending vehicle's attack potential by repositioning it to the tail of the formation.

Deviating from the proposed protocol ensures a stronger identification of a malicious vehicle, facilitating faster exclusion. As an extra step, to avoid abusive use of the misbehavior reporting protocol, we utilize a "suicide"-like approach [20] when reporting attackers, i.e., making a report also harms the reporting entity.

In the rest of the paper, we relate to previous works (Sec. II) and we discuss the threat model we consider for our investigation (Sec. III). We continue with the platoon restructuring protocol (Sec. IV); the experimental setup and evaluation (Sec. V); and a qualitative analysis of the protocol against potential threats under the given threat model (Sec. VI). Finally, we provide the concluding remarks (Sec. VII).

II. Related Work

Detecting falsification attacks in VC systems, has received significant attention: with frameworks that allow the execution and detection of attacks [12], [14], [21], or simulation-generated datasets for attacks, plausibility checks and MDSs [15], [16]. Further, the impact of falsification and jamming attacks has been studied [11], [12], [21], demonstrating that a leader attacker or an attacker further ahead in the formation has better attack potential. Moreover, the effect of such attacks on the maneuvering process of platooning vehicles [12] or of lone vehicles performing cooperative maneuvers can be catastrophic [22].

However, how the vehicles should react to mitigate these scenarios is still a challenge. The responsibility can be left to the controller, i.e., the data are fed to the controller regardless of their validity. However, this assumes string-stable controllers that are resilient to known, and unknown, attacks. Alternatively, by detecting an attack and its source, schemes can alter or disregard certain input data. Modifying the input data based on Kalman Filters [23] or an optimization problem [24] has shown promising results outside vehicular scenarios. Similarly, by predicting the mobility of the predecessor, new inputs can be deemed malicious, even if they are caused by faulty sensors, and disregarded [25]. However, this is susceptible to attacks that aim to gradually and slowly deviate from the nominal data, effectively masking the false information. Nonetheless, these solutions require resilient controllers and accurate mobility predictions to mitigate the attack's impact; with PRIME, the attacker is repositioned nullifying the effect on the vehicles.

Further, completely dropping or disregarding all the incoming data is not applicable, or safe [18], in platooning. Platoon formations require constant information dissemination; missing more than a few messages should immediately cause the vehicles to return to Adaptive Cruise Control (ACC) mode, dissolving the platoon. To avoid this, a suspiciousness-based mitigation technique with vehicles increasing their predecessor gap when a misbehavior is detected, but below a threshold, is proposed in [18]. However, selecting an appropriate threshold can be challenging: if too restrictive, the platoon will dissolve fast negating the platooning benefits; if too flexible, the mitigation cannot avoid the collisions before reverting to ACC. Further, relatively small deviations allow the vehicles to continue platooning, with increased gaps, diminishing the benefits of platooning, but more importantly allowing the attacker to destabilize, however small, the formation. By executing PRIME, the vehicles preserve their platooning operation and avoid any destabilization effect, even from an ongoing attack.

Finally, schemes that enable dynamic information flow topology [19] can allow the attacker's neighbors to still consume kinematic information; the predecessor from the vehicles upstream, while the follower, from its own followers downstream. This ensures that frontal and rear collisions can be avoided respectively. However, the attacker would still remain part of the formation and pose a threat downstream, as the vehicles can only rely on the information from the leader, who may be several vehicles ahead. This creates an extra threat when obstacles, e.g., an animal, appear inside the formation and not in front of the leading vehicle. By positioning the offending vehicle to the end of the platoon, PRIME preserves the information flow topology and avoids this issue.

III. Threat Model

We utilize a threat model for VC systems [26] and we incorporate platoon-specific aspects [10], [12], [27]. We consider attackers that possess valid credentials and are part of the platoon formation (i.e., insider attackers) that can perform falsification attacks, by altering the kinematic data present in the CAMs they disseminate, affecting the platoon stability. We also consider external attacks (from vehicles or other entities), notably jamming attacks against the platoon. Further, internal and external attackers can collude to improve their destructive capabilities. An insider has inherently knowledge of the platoon and can direct a jammer to perform its attack during crucial interactions, e.g., during protocol message transition. Additionally, we assume rational attackers, i.e., attackers who try to preserve the safety of their compromised vehicle. Finally, we treat misbehaving vehicles, even if not malicious, e.g., due to sensor malfunctions, as malicious.

Regarding the falsification attacks, we perform attacks that affect the position, speed and acceleration sent through the CAM messages, either by gradually increasing one kinematic property or by combining them to simulate a more realistic attack scenario; e.g., a change in position, updates the speed and acceleration following the physical mobility laws. In our analysis, we focus on the vehicular reaction and the execution of the protocol under investigation; it is assumed that these attacks can be detected with some form of certainty by existing plausibility checks [15], [16] and MDSs [12], [14].

IV. Platoon restructuring

Considering the threat model presented in Section III, a robust mechanism is needed to mitigate the impact of insiders. In situations where the precision of an MDS is not guaranteed an attacker can remain undetected for a prolonged period continuing to influence the platoon until an action is taken. To address this issue, we propose PRIME; a protocol designed

TABLE I
NOTATION USED IN THE PROTOCOL.

Check_Follower()	Use rear-facing sensor to calculate follower distance
$Id_{req}, Id_{res}, Id_{platoon}$	Request/Response/Platoon Unique Identifiers
K_v^i, k_v^i	Pseudonymous public/private key pairs
Leave_Process_Init()	Deactivate maneuvers and validate exit
$(msg)_{\sigma_v}$	Signed message with the vehicle's private key
N, N'	Nonces
P_v^i	Pseudonym signed by the PCA
Pos, V, S, L, F	Position, Velocity, Size, Lane, Formation
$Sign\ (Lk, msg)$	Sign a message with the private key (Lk)
$Verify\ (LK, msg)$	Verify a message with the public key (LK)

to reorder the formation in order to mitigate deviations from nominal mobility due to an attack or other non-malicious fault.

In Fig. 1 we present the interactions between four involved vehicles in the platoon; the *leader*, the *accuser*, the *accused*, and the *verifier*. We design the protocol in accordance to the state-of-the-art VC security requirements and include all the cryptographic primitives. A complete glossary is presented in Table I. Initially, the victim (*accuser*) notifies the platoon *leader* about an offending vehicle (*accused*) and requests a restructuring of the platoon. The leader, then, notifies the accused vehicle and its predecessor (*verifier*) of the required execution of the PRIME protocol. First, the accused, should it follow the protocol, is to perform an exit maneuver. Any refusal to do so can only strengthen the perceived and reported misbehavior leading to faster exclusion. The verifier is important because it uses its sensors to verify that the exit maneuver physically occures. Considering the uncertain truthfulness of the report, the accuser is to also perform an exit maneuver (if not positioned at the tail); have its maneuver be verified by the *verifier*; and finally temporarily exit the formation. This is equivalent to a "suicide" and deters misuse of the protocol. For brevity, we omit the join requests by the *accuser*, and potentially the *accused*, required by the protocol. It is crucial to mention that the *accuser* is in priority to reenter the formation in order to rejoin before the accused. This guarantees a decrease in the attacker's potential.

In Fig. 2 we present the full mobility patterns of an activated PRIME protocol when the victim's deployed MDS detects or suspects, e.g., by crossing a threshold, the existence of an attack. By executing steps 12 and 22 in Fig. 1, the two vehicles are positioned on the left lane (Fig. 2 steps 2 and 4) free to follow their own trajectories outside the platoon. The *accuser* would then slow down to position itself at the tail of the formation (step 5) and would perform a join maneuver (step 6). Any request from the *accused* to enter will be denied until the *accuser* has rejoined. Only at this time, would the *accused* be allowed to rejoin (steps 7 and 8).

V. SIMULATION ENVIRONMENT

A. Setup

To perform our simulations we used SUMO [28], a mobility simulator, combined with OMNET++ [29], a packet-level network simulator, and Plexe [30] implementing platoon

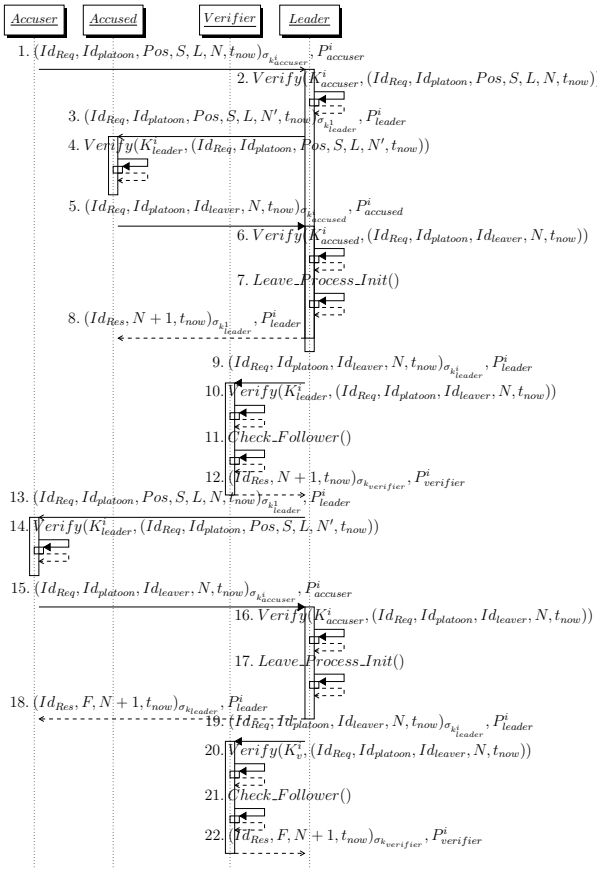


Fig. 1. PRIME: Exclusion Request

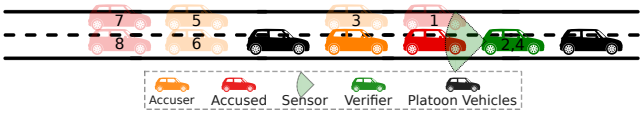


Fig. 2. PRIME step-by-step

formations. Table II provides the parameters we used in our simulations. We consider a straight highway and 7 vehicles as part of a platoon. We experiment with four different types of platoons (one per controller) and we expand their mobility functions to enable our protocol. For intra-platoon spacing, we utilize the default values representing the most stable distances for each controller. We also use different leader speeds, with an oscillating leader to approximate real-world mobility patterns, resulting in different intra-platoon gaps for the Constant Time Headway (CTH) controllers. We perform nine falsification attacks, three constant and six gradual, where the gradual step represent small but plausible mobility changes. We couple PRIME with a suspiciousness-based mitigation [18] and perform simulations deploying them alone or in unison.

To evaluate our approach, we measure the instability caused by any misbehavior through the intra-platoon distances. Vehicles reacting to an attack destabilize the formation; mitigating the effects should allow the vehicles to travel again at the nominal vehicle distances. Considering that vehicles traveling

TABLE II
SIMULATION PARAMETERS.

Parameters	Value	Parameters	Value
Beacon interval	0.1s	Controller	PATH, Ploeg, Consensus, Flatbed
Carrier frequency	5.89 GHz	Spacing	5m, 0.5s, 0.8s, 5m
Physical layer bit-rate	6 Mbps	Leader speed	80, 100, 120 kmph
Area size	5 KM × 25 M 2 lanes	Vehicle length	4 m
Number of vehicles	7	Falsification steps	$Position_{step} = \pm 2.5m$ $Speed_{step} = \pm 0.5m/s$ $Acceleration_{step} = \pm 0.015m/s^2$
Propagation Delays	Randomized	Constant Attacks	$Speed = [-3, 3]\ km/h$ $Acceleration = [-1.5, 1.5]\ m/s^2$ $Position = [-10, 10]\ m$
Vehicle TX Range	600m	Leader Oscillation Freq.	$0.2Hz$
Jammer TX Range	50m	Leader Oscillation Amplitude	$2\ km/h$
TX power	100mW	Duration of simulation	120s
Thermal Noise	-95dBm	Warm-up period	5s
Sensitivity	-94dBm	ACC Headway	2s

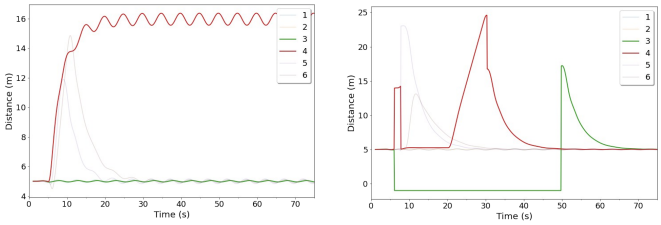
outside a platoon formation do not get its benefits, we measure PRIME's execution time, notably the time it takes to complete the exit and re-join maneuvers, for both the *accuser* and the *accused*. Finally, we quantify the collision impact achieved by our attack scenarios in order to show the mitigation capabilities of our approach. To critically assess the protocol robustness against intelligent attackers, we perform a qualitative analysis adhering to the threat model described in Sec. III.

B. Evaluation

Fig. 3 illustrates the effectiveness of our protocol. We compare PRIME with a suspiciousness-based mitigation technique [18]. When vehicle four (red) detects misbehavior from vehicle three (green), it increases the distance from its predecessor, to the maximum, and the platoon is destabilized for the duration of the attack (Fig. 3.a). In our case, (Fig. 3.b), the protocol requires the vehicles to exit and reenter at the tail in a different order. The accused (green) is the first to exit (a distance of -1 corresponds to an empty road ahead), with the accuser following. The accuser exits the formation and starts decreasing its speed (distance increases) to reach the tail of the platoon, at which point it rejoins and increases its speed (distance decreases) to reach the controller-appropriate distance with its new predecessor (vehicle 6). Observe that the mobility of the platoon is restored despite the ongoing attack.

Fig. 4 showcases the attack impact of the relatively negative falsification attacks (i.e., from a rational attacker) on the PATH controller for different speeds. We compare different PRIME activation timings against a no-mitigation approach. When there is no mitigation, all the gradual attacks and the constant offset speed attack, induce a collision downstream for PATH. Activating PRIME after 750 ms, does not avoid collisions, but the impact is lessened. For activation faster than 750 ms, PRIME mitigates the attacks, eliminating collisions, and reorders the platoon.

Fig. 5 shows the total elapsed time during the protocol execution, for both vehicles, accused and accuser, for each available controller. For PATH and Flatbed, both Constant Vehicle Spacing (CVS) controllers, the speed of the platoon does not affect the time needed for completion. On the other hand, the CTH controllers require more time as the speed increases. This discrepancy is due to the increased intra-platoon distances required by Ploeg and Consensus; the higher the speed the higher the distance. Moreover, the time required is influenced by the number of vehicles in the formation. A vehicle exiting the formation from a middle position needs more time to reposition itself at the tail of the platoon. Finally, we observe that the protocol manages to rearrange the accuser into the platoon in under 40 seconds regardless of the platoon speed, while the accused needs more time.



(a) Increased intra-platoon distances (b) PRIME

Fig. 3. Mitigation comparison between increased gaps and PRIME

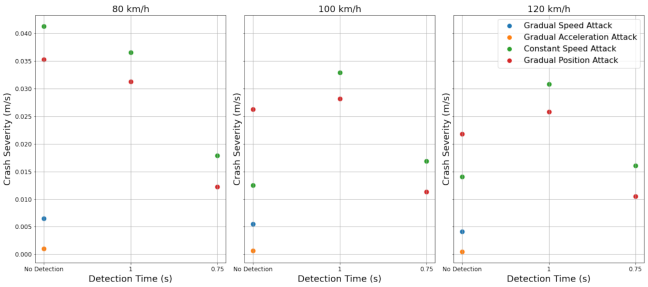


Fig. 4. Collision impact based on reaction timings

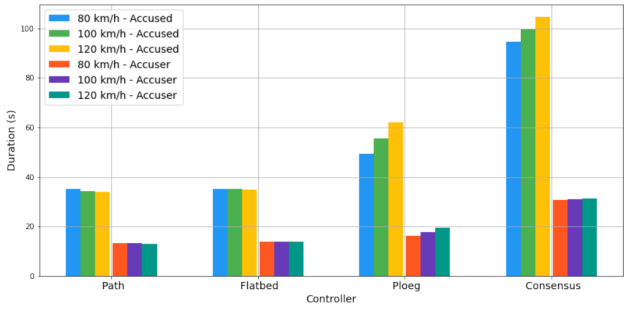
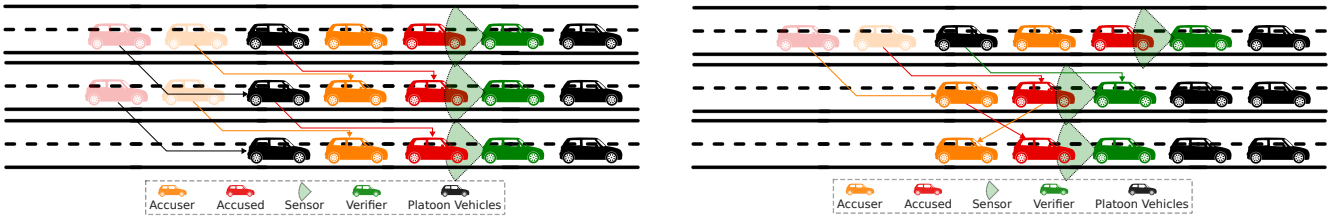


Fig. 5. Total protocol execution times for the maneuvering vehicles

VI. PROTOCOL ANALYSIS

Despite the promising results, we identify issues that could arise during the execution of the protocol and we discuss potential solutions. The cars depicted in Fig. 6 follow the same steps as in Fig. 2; the colored arrows denote the change of role (if any) and the movement of the vehicles inside the platoon for each successive completion of the protocol.

Constant accusations: The nature of the protocol allows vehicles to abuse it by constantly accusing their predecessor of misbehavior. In such a scenario (shown in Fig. 6.a), the *ac-*



(a) Repeat Accusations

(b) Circular Accusations

Fig. 6. Constant accusation abuse cases

cuser will not gain any favorable position, i.e., move upstream within the platoon, thanks to the "suicide" part of the protocol (the orange vehicle remains on the same position). Regardless of the platoon size, the *accuser* will be positioned at the second to last place of the platoon. This ensures that vehicles can only move downstream, reducing their incentive to perform any false reporting attack. Moreover, it is possible that after the end of PRIME, when both vehicles have rejoined, the previously designated *accused* now accuses (becomes orange in Fig. 6.b) its predecessor - leading to a reversal of roles. This type of abuse does not improve the attacker's potential but it can destabilize the tail of the formation. A solution would require the leader to keep an accusation history in order to deny requests that it deems unreliable.

Collusion: Based on our threat model, it is possible for multiple vehicles inside the platoon to collude to gain an advantage. In a scenario where the colluders are distant from each other, execution of the protocol would lead one attacker at the back while the other would advance two positions inside the platoon. Thus, the net position gain cannot be positive as the second attacker would advance to the same position. If the colluding vehicles are neighbors, i.e., one is the follower of the other, then an accusation from the follower would place both at the tail of the platoon. An accusation by the leading colluder, would result in the (colluding) follower to gain one (net) position. Such a scenario can happen once (resulting in a distant-colluders scenario) and further falsification attacks would pose a threat to the distant colluder. It is, however, possible that one of the colluders acts as the platoon leader. We discuss this in the leader attacker section considering the prominent role that a leader possesses.

Defiant attackers: An *accused* vehicle could decide to not comply with the instructions of the leader (as per the PRIME protocol). Even though this would signal to the platoon that the vehicle is indeed misbehaving, expediting its report to the authorities, the car would still remain part of the platoon. Potential measures to alleviate the problem include: warning the vehicle that it travels inside a platoon or increasing the intra-platoon gap from the accused vehicle [31]. The former is considered for non-misbehaving vehicles that enter a platoon formation; in our case, the vehicle can disregard the messages. The latter would create a similar situation to the one PRIME tries to solve but without the increased safety risk for the *accuser*. However, the platoon benefits would still be decreased due to the increased intra-platoon distances. Thus, as part of our future work, we will investigate the ability of the platoon to maneuver around the attacker to restore its cohesion.

Leader attacker: When a leader misbehaves the risk for the platoon increases significantly; a platoon leader can affect all vehicles in the formation (depending on the platoon topology [32]). In our case, the platoon leader facilitates the join and exit maneuvers, and is capable of disrupting the protocol based on its attack needs, e.g., it can disregard a report from the *accuser*. Similarly to a defiant attacker, though, the leader could be reported to the authorities. This would lead to the dissolution of the platoon, or the formation of a new one. Naively, one could delegate the leader status to the immediate follower, but this could lead to a *privilege escalation* attack when the follower and the leader collude [12]. A safer solution would be the re-election of a new leader while excluding the deemed malicious old one. Further, the leader could collude with another platoon member: a defiant leader would be reported facilitating a fast exclusion, while a compliant *accused* leader would be moved to the tail of the platoon.

Pseudonym changes: Adhering with ETSI [6], vehicles utilizing VPKI [7]–[9] are equipped with unlinkable pseudonyms that allow them to roam without revealing identifiable information. These pseudonyms are issued without overlapping lifetimes [33] to avoid Sybil attacks [34], however, a misbehaving vehicle could time its attack to happen before a pseudonym change is due. The attacker could change its pseudonym after being instructed by the PRIME protocol to exit the platoon but before requesting to rejoin. In such a scenario, the attacking vehicle would appear as a new one to the platoon thus requesting an entry at a different position instead of the PRIME-mandated last. A solution could involve tracking the disseminated CAMs in order to create a physical trajectory of the vehicle; unfortunately, such tracking can be abused by altering some or all of the broadcast kinematic values. Better alternatives would involve the use of the verifier's own sensors, e.g., LiDAR, to localize the target vehicle [35]; using the attacker's signal characteristics [36] to measure the distance from the leader; or proofs of location that require other vehicles on the road or Roadside Units (RSUs) [37]. Any further detection of misbehavior by the *accused* would facilitate the faster revocation of its long-term credentials.

VII. Conclusion

We presented PRIME, a protocol capable of securely restructuring the platoon while diminishing the impact of misbehaving vehicles in these formations. Our analysis shows that this is a viable mitigation technique that can operate in conjunction with existing MDSs. We showcase that mitigation techniques can avoid creating increased intra-platoon gaps that diminish platooning benefits, thus facilitating wider adoption. We further analyze our scheme considering stronger attackers and provide possible countermeasures where applicable, towards a better understanding of mitigation techniques' design.

Acknowledgment

This work was supported by the Swedish Research Council (VR).

References

[1] V. Milanés *et al.*, "Cooperative adaptive cruise control in real traffic situations," *IEEE Transactions on ITS*, vol. 15, no. 1, pp. 296–305, Feb. 2014.

[2] "Sweden4Platooning Project," 2020. [Online]. Available: https://www.trafikverket.se/contentassets/e9dec2f430b94466a8aa4572966aeb39/publik-rapport_tsaf_20200130.pdf

[3] M. P. Lammert *et al.*, "Effect of Platooning on Fuel Consumption of Class 8 Vehicles Over a Range of Speeds, Following Distances, and Mass," *SAE Int. J. Commer. Veh.*, vol. 7, pp. 626–639, Sep. 2014.

[4] W. van Willigen, E. Haasdijk, and L. Kester, "A multi-objective approach to evolving platooning strategies in intelligent transportation systems," in *Genetic and Evolutionary Computation Conference (GECCO)*, 2013.

[5] 1609_WG - V2X Communications Working Group , "IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Application and Management Messages," *IEEE Vehicular Technology Society*, Jan. 2022.

[6] ETSI, "Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management," ETSI TS 102-940, Nov. 2016.

[7] W. Whyte *et al.*, "A Security Credential Management System for V2V Communications," in *IEEE Vehicular Networking Conference (VNC)*, Boston, MA, Dec. 2013, pp. 1–8.

[8] M. Khodaei *et al.*, "SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems," *IEEE TITS*, vol. 19, no. 5, pp. 1430–1444, May 2018.

[9] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[10] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving," *IEEE Comm. Mag.*, vol. 53, no. 6, Jun. 2015.

[11] R. van der Heijden *et al.*, "Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC)," in *IEEE Vehicular Networking Conference (VNC)*, Torino, Italy, Nov. 2017.

[12] K. Kalogiannis, M. Khodaei, W. M. N. M. Bayaa, and P. Papadimitratos, "Attack impact and misbehavior detection in vehicular platoons," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2022, pp. 45–59.

[13] A. Alipour-Fanid, M. Dabaghchian, H. Zhang, and K. Zeng, "String Stability Analysis of Cooperative Adaptive Cruise Control under Jamming Attacks," in *IEEE International Symposium on High Assurance Systems Engineering (HASE)*, Singapore, Singapore, Jan. 2017.

[14] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa, and P. Urien, "Simulation framework for misbehavior detection in vehicular networks," *IEEE transactions on vehicular technology*, vol. 69, no. 6, pp. 6631–6643, 2020.

[15] R. W. Van Der Heijden, T. Lukaseder, and F. Kargl, "Veremi: A dataset for comparable evaluation of misbehavior detection in vanets," in *Security and Privacy in Communication Networks*. Springer International Publishing, Dec. 2018, pp. 318–337.

[16] Kamel, J. *et al.*, "Veremi extension: A dataset for comparable evaluation of misbehavior detection in vanets," in *IEEE International Conference on Communications (ICC)*, 2020.

[17] A. Boualouache and T. Engel, "A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1128–1172, 2023.

[18] Wolf, M. *et al.*, "Securing cacc: Strategies for mitigating data injection attacks," in *IEEE Vehicular Networking Conference (VNC)*, 2020.

[19] 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*, 2015.

[20] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, "Fast exclusion of errant devices from vehicular networks," in *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, Jun. 2008, pp. 135–143.

[21] M. Iorio, F. Risso, R. Sisto, A. Buttiglieri, and M. Reineri, "Detecting Injection Attacks on Cooperative Adaptive Cruise Control," in *IEEE Vehicular Networking Conference (VNC)*, Los Angeles, CA, USA, Dec. 2019, pp. 1–8.

[22] K. Kalogiannis, A. Henriksson, and P. Papadimitratos, "Vulnerability analysis of vehicular coordinated maneuvers," in *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2023, pp. 11–20.

[23] C.-Z. Bai, V. Gupta, and F. Pasqualetti, "On kalman filtering with compromised sensors: Attack stealthiness and performance bounds," *IEEE Transactions on Automatic Control*, vol. 62, no. 12, pp. 6641–6648, Jun. 2017.

[24] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 1145–1151, Aug. 2014.

[25] E. Mousavinejad, F. Yang, Q.-L. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE transactions on cybernetics*, vol. 48, no. 11, pp. 3254–3264, Jun. 2018.

[26] P. Papadimitratos *et al.*, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Comm. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[27] S. Ucar *et al.*, "IEEE 802.11 p and Visible Light Hybrid Communication Based Secure Autonomous Platoon," *IEEE TVT*, vol. 67, no. 9, pp. 8667–8681, May 2018.

[28] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO - Simulation of Urban MObility: An Overview," in *The International Conference on Advances in System Simulation*, Barcelona, Spain, Oct. 2011.

[29] "OMNeT++," https://www.omnetpp.org/, Jun. 2017.

[30] "Plexe: The Platooning Extension for Veins," http://plexe.car2x.org/, Aug. 2020.

[31] "V2 Platooning use cases, scenario definition and Platooning Levels," https://platooningensemble.eu/storage/uploads/documents/2022/03/14/ENSEMBLE-D2.3_V2-Platooning-use-cases,-scenario-definition-and-Platooning-Levels_FINAL.pdf, Feb. 2022.

[32] Y. Zheng, S. E. Li, J. Wang, D. Cao, and K. Li, "Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies," *IEEE Transactions on intelligent transportation systems*, vol. 17, no. 1, pp. 14–26, 2015.

[33] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Conference on ITS Telecommunications*, Jun. 2007, pp. 1–6.

[34] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*. Springer, Oct. 2002, pp. 251–260.

[35] R. Barea, C. Pérez, L. M. Bergasa, E. López-Guillén, E. Romera, E. Molinos, M. Ocana, and J. López, "Vehicle detection and localization using 3d lidar point cloud and image semantic segmentation," in *Conference on Intelligent Transportation Systems (ITSC)*, Nov. 2018, pp. 3481–3486.

[36] A. M. Wyglinski, T. Wickramarathne, D. Chen, N. J. Kirsch, K. S. Gill, T. Jain, V. Garg, T. Li, S. Paul, and Z. Xi, "Phantom car attack detection via passive opportunistic rf localization," *IEEE Access*, vol. 11, pp. 27 676–27 692, 2023.

[37] F. Boeira, M. Asplund, and M. Barcellos, "Decentralized proof of location in vehicular ad hoc networks," *Computer Communications*, vol. 147, pp. 98–110, 2019.