Vouch: A Secure Proof-of-Location Scheme for VANETs

Felipe Boeira
Dept. of Computer and Information Science
Linköping University
Linköping, Sweden
felipe.boeira@liu.se

Mikael Asplund
Dept. of Computer and Information Science
Linköping University
Linköping, Sweden
mikael.asplund@liu.se

Marinho P. Barcellos
Institute of Informatics
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
marinho@inf.ufrgs.br

ABSTRACT

In Vehicular Ad Hoc Networks (VANETs), nodes periodically share beacons in order to convey information including identity, velocity, acceleration and position. Truthful positioning of nodes is essential for the proper behavior of applications, such as formation of vehicular platoons. Incorrect position information can cause problems like increased fuel consumption, reduced passenger comfort, and in some cases even accidents. In this paper, we design and evaluate Vouch: a secure proof-of-location scheme tailored for VANETs. The scheme leverages future deployment of fifth generation (5G) wireless network roadside units, and is able to operate using different overhead constraints. Through simulations using an adversarial model, we show that Vouch can detect position falsification attacks while incurring in low overhead.

CCS CONCEPTS

•Security and privacy → Intrusion detection systems; •Networks → *Peer-to-peer protocols;*

KEYWORDS

VANET, security, proof of location

1 INTRODUCTION AND BACKGROUND

VANETs are defined as the exchange of information among vehicles and enable novel intelligent transportation systems. Safety and traffic control systems are at the center of VANET-based supported applications. To enable them, vehicles achieve cooperative awareness through the exchange of periodic broadcast messages called *beacons*. Vehicles in the vicinity can leverage information contained in the beacons to, e.g., detect traffic jams, emergency brake, and operate platoons.

A vehicular platoon is a group of vehicles that travel closely together in a highway. Each vehicle executes an instance of a platoon controller that takes advantage of IVC-broadcast beacons to perform longitudinal and lateral control. A leader dictates the behavior of the platoon while the followers adapt to preserve stability. By reducing the inter-vehicular distance (headway time), a platoon lowers fuel consumption as a result of reduced air drag [15], and relieves the drivers in the following vehicles from controlling them.

Although platoons present clear benefits for traffic efficiency and driving comfort, using IVC for vehicle control introduces a relevant threat surface that may be exploited by malicious actors. In earlier work we have shown that carefully crafted beacons can cause collisions with increased impact when multiple nodes collude in position falsification [1]. Attacks in vehicular platooning may result in injury or ultimately in loss of lives, which enforces the need for secure and dependable mechanisms.

Cooperative awareness relies on perceiving the vehicular environment correctly and the legitimate positioning of neighbor vehicles is essential. The European Telecommunications Standards Institute (ETSI) has stated that messages must be signed to provide authenticity, non-repudiation and integrity [10]. However, insider attackers may still falsify information that is contained in the signed message. While sensor fusion algorithms [17] might ameliorate position perceiving of neighbors, sensors themselves have limited capabilities and require IVC to be trustworthy.

To attest neighbor localization, position verification systems have been extensively studied in mobile networks. Three main techniques have been employed in the literature: location estimation, plausibility verification and proof of location. Location estimation is enabled by angle of arrival or distance measurement techniques, such as radio signal strength or time of fight. Plausibility verification is also employed as a technique to identify false positions by calculating feasible boundaries. Finally, proof-of-location countermeasures have been proposed in mobile and cognitive radio networks to provide truthful positioning. While the aforementioned countermeasures aim at providing location assurance, the main limitations are related to handling the high mobility environment of VANETs and the real-time requirements of safety applications while preserving privacy. Our approach uses a combination of these techniques and aims at overcoming the presented limitations.

To provide location awareness, vehicles are envisioned to use a combination of sensors such as lidar, radar, cameras and Global Navigation Satellite Systems (GNSS) like the Global Positioning System (GPS). Typically, cellular radio networks have not been considered for safety-critical localization due to insufficient accuracy. However, attributes of 5G wireless technologies aim to enable the high-precision and low-latency requirements for vehicular positioning [11, 13, 26]. While dedicated vehicular-only RSUs are often considered to have limited deployment, cellular signals are ubiquitous and inexpensive to process. Therefore, it is likely that vehicles will be able to leverage 5G-enabled base stations as roadside units.

In this work, we propose and evaluate a proof-of-location scheme tailored for VANETs called Vouch. The key insight of our design is leveraging 5G-enabled roadside units and combining distinct techniques as components in the scheme. Our proposal supports privacy-preserving authentication protocols and uses a trusted authority to provide authentic proofs. A plausibility model is included to account for high mobility and handling of stale proofs. This allows the mechanism to operate using low proof frequencies, resulting in lower overhead by exchanging less data.

The contributions of this paper are outlined below:

- We design Vouch: a proof-of-location scheme tailored for VANETs that couples distinct truthful positioning techniques as components.
- We evaluate a mobility-aware plausibility technique that supports high-speed mobility.
- Vouch is evaluated according to accuracy metrics and an overhead analysis is performed. We show that the our proposal incurs in low overhead given lower proof frequencies usage while maintaining anomaly detection.

The paper is organized as follows: Section 2 presents the literature review on proof-of-location systems. Section 3 provides the design proposal while Section 4 shows the evaluation results. Section 5 concludes the paper and outlines future work.

2 RELATED WORK

Proof-of-location mechanisms have been employed in diverse mobile environments. In this section, we describe the state-of-the-art mechanisms that have been proposed in the fields of mobile ad hoc network and database-driven cognitive radio networks.

Waters and Felten [25] 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 [24] uses 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 [3, 6, 7]. 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. In order to protect against P-P collusion attacks, the Bussard-Bagga [2] distance bounding protocol was employed. STAMP also uses an entropy-based trust model to protect against P-W collusion.

APPLAUS [27] 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.

Witness ORiented Asserted Location provenance (WORAL) [9] is another witness-based scheme framework. The authors consider a service provider 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 [14]. WORAL considers that collusion attacks may be conducted by malicious users, location authorities and/or witnesses.

VeriPlace [16] is a location-proof system with privacy and cheating detection capabilities. 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. VeriPlace depends upon three trusted third parties in order to defend against collusion attacks, one that manages user information, one that manages location information and one that performs anomaly detection.

Hasan and Burns [8] 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 mechanism uses a distance bounding and time stamping to generate chronologically-ordered proofs. 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 VANETs due to real-time, high-mobility and privacy constraints combined. In order to cope with the requirements of the vehicular environment, we design and evaluate a VANET-tailored proof-of-location scheme. Our proposal can handle high mobility and is lightweight so that the channel load is minimally impacted. In this paper, the combination of these characteristics in the proposed method are proven to be an effective countermeasure to position falsification attacks.

3 DESIGN OF VOUCH

This section describes the design of Vouch. The scheme includes a **protocol** used for *proof acquisition and dissemination* and a **classifier mechanism** that applies the *plausibility model* to detect inconsistencies. In this section, these components are presented. For presentation purposes, the workflow is presented under a static scenario in Section 3.2 and the mobility-aware component of the classification is presented in Section 3.3.

For this present work, we assume that the neighbor vehicles already possess the RSU's public key, in order to verify the *proof* digital signature.

Three parameters are used to define the operation of Vouch, *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.

3.1 Protocol

The protocol is divided into three phases: *registration*, *proof acquisition and dissemination*, and *unregistration*. The trusted positioning, hereby referenced as *proof*, is provided by RSUs once the vehicles register by using a *proofReq* request. Figure 1 details the protocol, representing 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, confidence of positioning as C_{pos}, 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. The protocol

uses Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure integrity, authenticity and non-repudiation, which is in line with the objectives of current vehicular communication standards.

Once a *proofReq* is received, the RSU validates the certificate, extracts the public key from the certificate and verifies the signature of the request. The timestamp is compared with the current clock reading at the RSU 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 *proof* messages. After sending a *reqAck*, the RSU begins to provide periodic *proof* messages to the vehicle. A *proof* consists of the position coordinates, a timestamp, its confidence on the position accuracy and the digital signature. This *proof*, as will be further detailed, is relayed by the vehicle to its neighbors as an assurance of its legitimate location. 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 Certificate Authority (CA) that can be used to assert its integrity and authenticity.

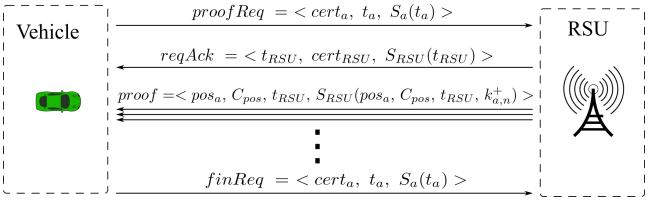


Figure 1: Proof-of-location protocol

3.2 Beacon Classification

To simplify the presentation of the beacon classification, consider a scenario in which the nodes are static. Figure 2 shows the main steps of the full mechanism including the beacon classification. Figure 3 presents the corresponding timeline of events containing the *Proof Acquisition* and *Beaconing and Position Verification*. The RSU is represented by the antenna in the highway's border, the node willing to prove its location is represented by the green car (prover) while peers that will verify the proof are the yellow ones (verifiers).

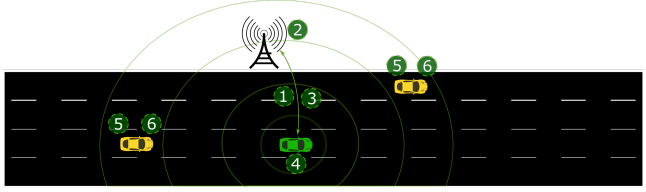


Figure 2: Timeline with proof acquisition and beaconing/position verification using static nodes

After registration, a prover will continuously receive a stream of proofs. The proof acquisition comprehends the position estimation of the vehicle by the RSU (step 1), *proof* generation (step 2) and transmission (step 3). The overhead associated with estimating the position is not inherent to the proposed mechanism since 5G communication base stations have to continuously track user equipments (in our case, vehicles) in order to utilize beamforming [12]. Once the prover acquires the proof, it will be transmitted in the next broadcast beacon (step 4). Proof acquirement and beaconing are asynchronous procedures as they can work in distinct frequencies. ETSI standards define that beaconing is performed up to 10 Hz frequency. A proof will be included in every beacon transmission if the acquisition is also performed at the same frequency. Otherwise, nodes can share proofs less frequently and verifiers will use stale proofs to perform the plausibility check in subsequent beacons. Once neighbors receive a beacon, they verify if a proof is included and, if so, verify its signature. If the proof is authentic, then it is stored (step 5). For every beacon that is received, a plausibility check is executed and the beacon is classified as plausible or anomalous (step 6).

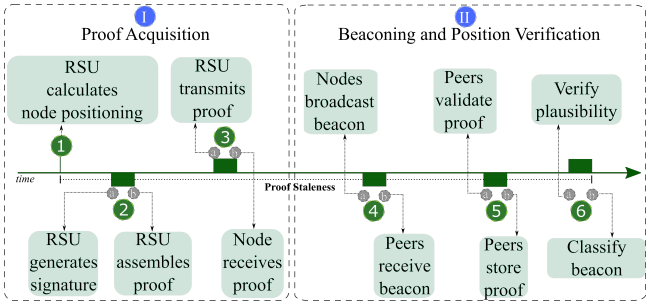


Figure 3: Timeline with proof acquisition and beaconing/position verification

Figure 4 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.

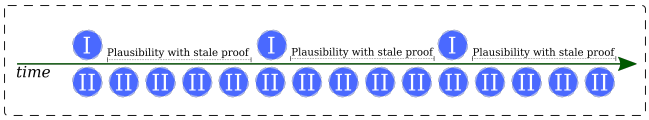


Figure 4: Example of proof acquisition with 2 Hz and beacon transmission/plausibility check events

In a static scenario, verifiers only need to validate if the reported position is situated under the proof location given a certain threshold. The threshold is derived from the RSU's confidence in the positioning accuracy, transmitted as C_{pos} in the proof. Figure 5 depicts the classification in a static scenario. The position contained in the beacon along with the position and threshold contained in

the last received proof are used as input to the classifier. The output is a classification of the position as plausible or not. The bounds verification is merely a comparison of the beacon position to the accepted boundary as shown in Algorithm 1.

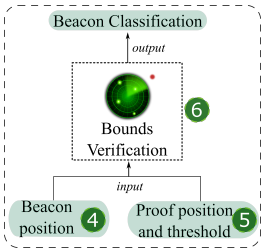


Figure 5: Beacon classification procedure in a static scenario

Algorithm 1 Bounds Verification

```
1: procedure BoundsVerification
2:     (X_b, Y_b) ← beacon position
3:     (X_p, Y_p) ← proof position
4:     (T_x, T_y) ← positioning accuracy threshold
5:     if |X_p − X_b| ≥ T_x OR |Y_p − Y_b| ≥ T_y then
6:         return not plausible
7:     else
8:         return plausible
```

3.3 Mobility-aware Classification

In mobile scenarios, such as when vehicles are traveling in a highway, the position accuracy noise is not the only source of the uncertainty. As vehicles change their speed and possibly turn, the position error may differ in lateral and longitudinal coordinates according to their movement. This scenario requires the classification to take into account the mobility of the nodes.

An important aspect of the proof then becomes its *staleness*, i.e., its age. As shown in Figure 3, there is a gap between the vehicle's position estimation in step 1 and the usage of the proof by neighbor vehicles in step 6. 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. This is illustrated in Figure 6 as the prover moves between proof generation by the RSU and verification by its peers.

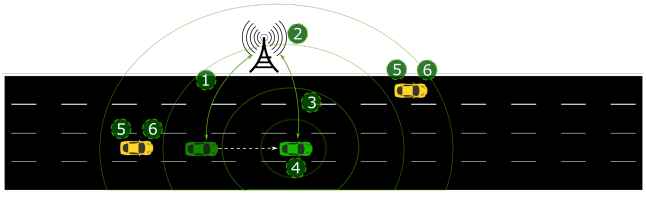


Figure 6: Illustration of events for proof dissemination

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. The proof staleness is directly tied to the plausibility check; the older the proof, the broader will be the position acceptance. In the present work, the mobility models are derived from the Constant Velocity (CV) for the X dimension while Y takes Constant Turn Rate and Velocity (CTRV) [20] to account for turning.

Figure 7 depicts the mobility-aware classification. The last stored proof and required information from the beacon are used in the presented plausibility model to calculate the position bounds. Then, the resulting bounds are combined with the proof C_{pos} accuracy confidence as threshold and compared with the claimed position in the beacon. The output is a classification as plausible or not.

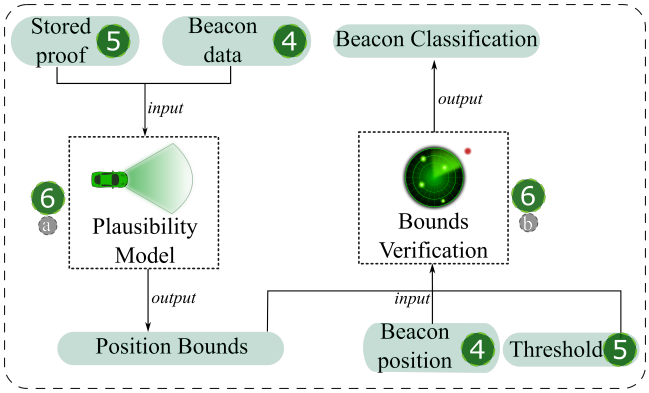


Figure 7: Mobility-aware beacon classification procedure

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

$$y_{k+1} = y_k + \frac{\dot{x} + \Delta t \ddot{x}}{\dot{\psi}}(-cos(\psi + \dot{\psi}\Delta t) + cos(\psi)) \tag{2}$$

Equations 1 and 2 take the following variables for position estimation in time $k+1$ given information from time k: x and y are absolute positions (m), $\dot{x}$ represents velocity (m/s), $\ddot{x}$ represents acceleration (m/s^2), $\dot{\psi}$ represents the yaw rate (rad), ψ determines heading (rad) and Δt is the timestamp difference between proof and beacon (s). The bounds are determined using minimum and maximum values for acceleration and yaw rate while the remaining information is obtained via beacons.

4 EVALUATION OF VOUCH

In this section, Vouch is evaluated in terms of detection performance and overhead costs in a platooning context. The effectiveness of the scheme is verified through simulations that use both benign and colluding attacker nodes. The attacker model presented in our previous work [1] is employed in the evaluation, and an overview is included in this section.

4.1 Attack Scenario Overview

Consider a vehicular platoon composed of eight vehicles that travel along a highway. Vehicles in the vicinity of the platoon may request to join the formation to leverage platooning benefits. Our

threat model is composed of an attacker that forges false vehicles by tampering with the position in the beacons, which are then signed with valid cryptographic keys. The attacker impersonates multiple false vehicles (joining them into the platoon) by conducting a Sybil attack [1, 5] or possibly by having stolen credentials to support the attack. Figure 8 illustrates the attack scenario and the coordinates falsification (represented by X and Y) that the attacker must perform in order to situate the false vehicles. To make the attack harder to detect, the attacker travels closely beside the position of the false node, which minimizes the amount of position error. In this attack, one false vehicle is inserted between the first pair of legitimate members and another false vehicle between the second pair. After introducing the false vehicles into the platoon (which occurs at 30 s in our simulation), the attacker manipulates the beacons by increasing the position error to cause unwanted effects in the controllers of following vehicles (which occurs at 100 s in our simulation). The first false node subtracts its position in 250 m while the second increases by the same amount, resulting in a collision.

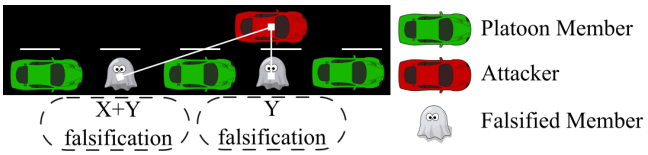


Figure 8: Attack scenario overview

4.2 Simulation Environment

The evaluation of Vouch was performed using Plexe [21]. Plexe is an extension to Veins [22], a VANET simulator that combines network simulation though the Omnet++ framework and mobility simulation through SUMO. The cryptographic operations of the scheme were implemented using the OpenSSL APIs. As illustrated in Figure 9, the attacker model is used to evaluate the detection performance of the scheme when an attack is being conducted. A model of the RSU that provides the proofs is implemented in Plexe and connected to the external module that provides the cryptographic operations. The plausibility model introduced in Section 3 is included as a platooning application of the simulator. The simulation parameters are included in Table 1. Each simulation setup was executed 33 times with distinct seeds.

4.3 Evaluation Metrics

In this section, the detection and overhead metrics are presented.

Detection Metrics. The evaluation of detection performance is performed using a set of metrics which are derived from the variables defined below. The following nomenclature is used: 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. Beacons with positions in the acceptable boundaries are *plausible* while out-of-boundary beacons are *implausible*.

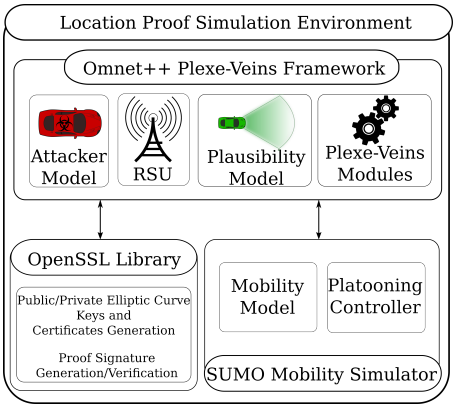


Figure 9: Simulation architecture

Table 1: Traffic simulation parameters

Freeway length	10 km
Number of lanes	4
Car speeds	20/40/60/80/100 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 [18]
Simulation time	200 s
Beaconing frequency	10 Hz
Communication interface	802.11p
Radio frequency	5.89 GHz
Transmission power	20 mW
Position noise mean/σ	0/0.5 m
Path loss model	Free space (α = 2.0)
Proof size	100 bytes
Proof frequency	10 Hz, 5 Hz, 2 Hz, 1 Hz
Plausibility check threshold	1 σ, 2 σ, 3 σ, 4 σ

- True Positive (TP): Falsified beacon is classified as implausible
- True Negative (TN): Correct beacon is classified as plausible
- False Positive (FP): Correct beacon is classified as implausible
- False Negative (FN): Falsified beacon is classified as plausible

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. Equation 3 details the definition of the accuracy metric. The TPR, given by Equation 4, provides the rate of correct detection of attacks. Equation 5 provides the calculation of the FNR that details the rate of attack beacons that were not detected by the mechanism. In Equation 6, FPR is defined and represents the rate of correct beacons that were detected.

$$ACC = \frac{TP + TN}{TP + FP + FN + TN} \quad (3) \qquad TPR = \frac{TP}{TP + FN} \quad (4)$$

$$FNR = \frac{FN}{TP + FN} \quad (5) \qquad FPR = \frac{FP}{FP + TN} \quad (6)$$

Overhead Metrics. As presented in the design details of Vouch in Section 3, the scheme can operate in varying frequencies. The usage of higher dissemination frequencies means that a larger amount of data must be exchanged and consequently results in a higher channel load, which could cause information loss [19]. Vehicular networks aim at supporting the execution of safety-critical applications that require low-latency and transmission reliability. These applications may be negatively impacted as network collisions and instabilities occur, thus it is desirable to minimize such conditions. As stated by Sommer et al. [23], the computation of collision rates in 802.11 networks is complex and simulators currently lack simple models to study these effects. While the increase in network utilization does not necessarily result in degradation of safety performance, it is a good indicator of the network load. To determine the additional channel utilization introduced by our mechanism's overhead, we analyze the channel busy time ratio to measure the potential additional load by means of transmitting proof data in beacons. The evaluation scenario consists of a platoon composed of eight members and fifty additional interfering vehicles traveling close to the platoon that also broadcast proofs. The busy time is computed in all vehicles of the scenario and a mean is calculated for each simulation run. In addition to the four proof frequencies, we also evaluate the busy time ratio under the absence of proofs, which is represented by the 0 Hz frequency. In addition to network load, our scheme also depends on the execution of cryptographic operations. While CPU overhead is not measured in this work, we capture the effects of crypto-generated delays during the scheme operation. The ECDSA signature generation and verification overheads are accounted according to benchmarks in [4] for ECDSA *nistp256*.

4.4 Simulation Results

This section describes the simulation results. High mobility is the key characteristic of VANETs that renders existent proof-of-location schemes unsuitable for this environment. Figure 10 shows the accuracy and FPR results for distinct platoon speeds using 5 Hz proof frequency and 3 σ threshold. It is noticeable that as vehicles move at higher speeds, detection metrics degrade when using static classifiers (presented in Section 3.2). The mobility-aware classifier presented in Section 3.3 shows consistent detection results under higher speeds.

Figure 11a includes Receiver Operating Characteristic (ROC) curves that present FPR and TPR relations for distinct parameters. For each curve, the threshold parameter is varied (from 1 σ to 4 σ). It is clear that the 5 and 10 Hz proof frequencies result in very similar detection performance, whereas the lower frequencies (1 Hz and 2 Hz) result in significantly worse performance.

Figure 11b shows another view of the results for 5Hz proof frequency. It is clear that for low thresholds (below 3 σ), the false positive rate is completely unacceptable. Even for higher thresholds (3 σ and 4 σ), the FPR is higher than what would be acceptable for an intrusion detection system for corporate networks. However,

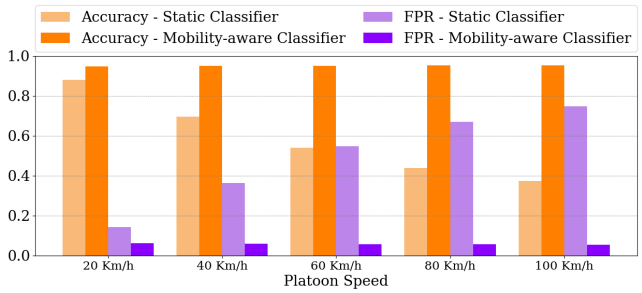


Figure 10: Detection results using the static and mobility-aware classifiers under distinct speeds

as noted in Section 3 the classifier should be complemented with a mechanism for reacting to the outcome of the classification. For example, if all implausible beacons are dropped (filtered), having a false positive is no worse than regular packet loss.

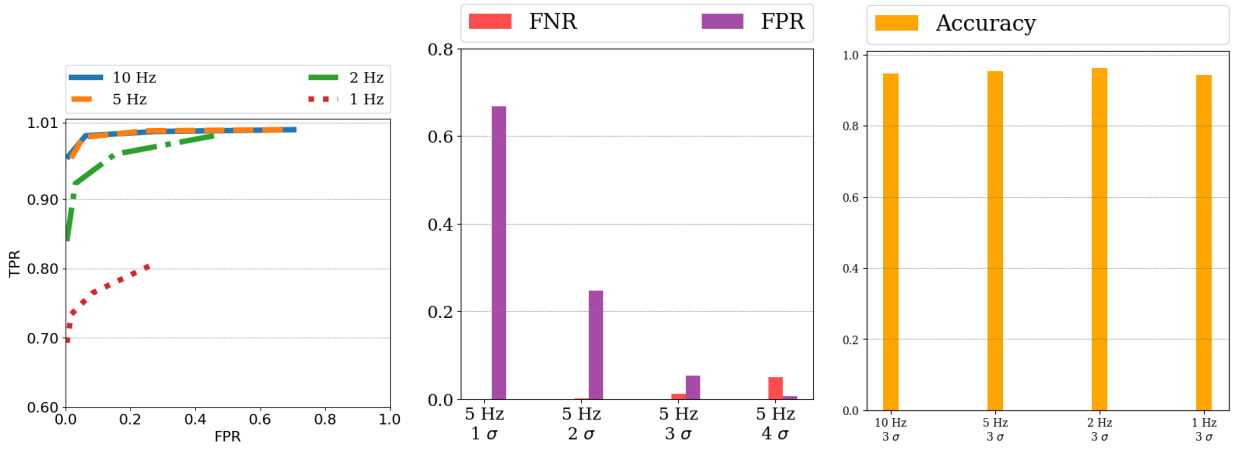
Finally, it is interesting to investigate which beacons that are incorrectly classified. In Figure 12, beacon detection results are included for 5 Hz frequency and 3 σ threshold. In this plot, the X axis represents the simulation time and the Y axis measures the position error between the beacon position and the plausible boundary. The higher the Y value, the farther the beacon position is from the plausible range. Blue marks are beacons 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.

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. Purple marks represent false positives, which means that the position noises of the beacon and the proof combined were sufficient to be classified out of the bounds. Vouch allows the detection of falsified nodes during the first phase of attack, even before they conduct the position falsification that will cause unwanted behavior in the controllers.

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. Also, the dangerous beacons (the ones far away from the real locations) are correctly classified as implausible.

Figure 13 depicts the busy time ratio 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. Outliers are represented by black circles. As can be observed, the mechanism has a low impact in the channel load especially under low frequencies operation. Given that accuracies for lower proof frequencies show similar detection performance (illustrated by Figures 11c and 11a), it is possible to achieve lower channel utilization overhead.

To summarize, results show that the mechanism provides the location-assurance requirement for safety-critical applications. The proof dissemination may be enforced by nodes before they accept



(a) ROC curves **(b) FPR and FNR under 5 Hz** **(c) Detection accuracies**

Figure 11: Detection results

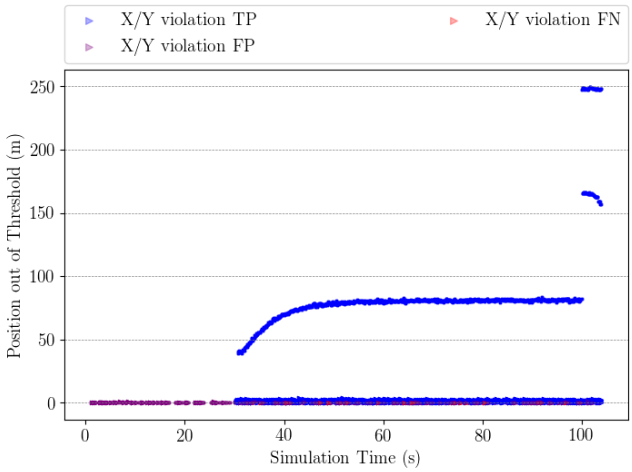


Figure 12: Detection results using 5 Hz proof frequency and 3 σ

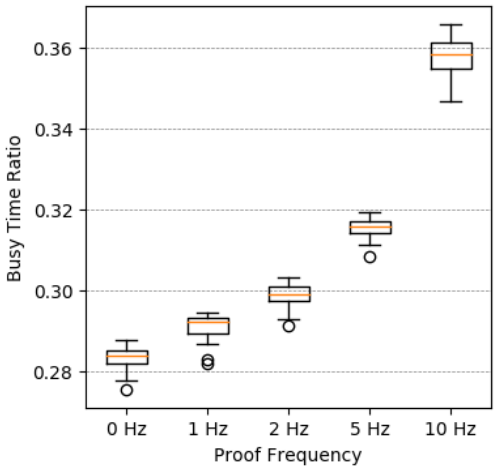


Figure 13: Busy time ratio under distinct proof frequencies

beacons from neighbors (e.g. in a platoon join or merge request) or to continuously ensure proper behavior (e.g. in a platoon operation).

5 CONCLUSION AND FUTURE WORK

VANETs are emerging to provide fascinating novel technologies that may ameliorate vehicular traffic altogether. The challenges to create secure and dependable connected vehicular applications are substantial, and position assurance is a fundamental requirement to support vehicular trust. Based on that, we design and evaluate a proof-of-location mechanism tailored for VANETs. We demonstrate that the use of location proofs combined with a plausibility model can counteract position-based 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. The proposed proof-of-location mechanism has shown to perform well in the detection metrics under the studied constraints, however, future work opportunities exist. Particularly, reaction strategies have to be designed and evaluated so that applications can effectively take advantage of the mechanism. In addition, advancements in the mobility model is prone to result in better detection metrics, which can consequently enable further reduction in the proof frequency dissemination and overall network channel utilization.

REFERENCES

[1] F. Boeira, M. P. Barcellos, E. P. de Freitas, A. Vinel, and M. Asplund. 2017. Effects of colluding Sybil nodes in message falsification attacks for vehicular platooning. In *2017 IEEE Vehicular Networking Conference (VNC)*. 53–60. https://doi.org/10.1109/VNC.2017.8275641

[2] Laurent Bussard and Walid Bagga. 2005. Distance-Bounding Proof of Knowledge to Avoid Real-Time Attacks. In *Security and Privacy in the Age of Ubiquitous Computing*, Ryoichi Sasaki, Sihan Qing, Eiji Okamoto, and Hiroshi Yoshiura (Eds.). Springer US, 223–238.

[3] Ivan Damgård. 1999. Commitment Schemes and Zero-Knowledge Protocols. In *Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School, Aarhus, Denmark, July 1998*. Springer-Verlag, 63–86.

[4] Joerie de Gram. 2011. Speeding up EC cryptography on embedded hardware. (2011).

[5] John R. Douceur. 2002. The Sybil Attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS '01)*. Springer-Verlag, 251–260.

[6] Iftach Haitner and Omer Reingold. 2007. Statistically-hiding Commitment from Any One-way Function. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing (STOC '07)*. ACM, 1–10. https://doi.org/10.1145/1250790.1250792

[7] Shai Halevi and Silvio Micali. 1996. Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing. In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '96)*. Springer-Verlag, 201–215.

[8] Ragib Hasan and Randal Burns. 2011. Where have you been? secure location provenance for mobile devices. *arXiv preprint arXiv:1107.1821* (2011).

[9] R. Hasan, R. Khan, S. Zawoad, and M. M. Haque. 2016. WORAL: A Witness Oriented Secure Location Provenance Framework for Mobile Devices. *IEEE Transactions on Emerging Topics in Computing* 4, 1 (Jan 2016), 128–141. https://doi.org/10.1109/TETC.2015.2401394

[10] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil. 2011. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Communications Surveys Tutorials* 13, 4 (Fourth 2011), 584–616. https://doi.org/10.1109/SURV.2011.061411.00019

[11] P. Kela, M. Costa, J. Salmi, K. Leppanen, J. Turkka, T. Hiltunen, and M. Hronec. 2015. A Novel Radio Frame Structure for 5G Dense Outdoor Radio Access Networks. In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. 1–6. https://doi.org/10.1109/VTCSpring.2015.7145635

[12] P. Kela, M. Costa, J. Turkka, M. Koivisto, J. Werner, A. Hakkarainen, M. Valkama, R. Jantti, and K. Leppanen. 2016. Location Based Beamforming in 5G Ultra-Dense Networks. In *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. 1–7. https://doi.org/10.1109/VTCFall.2016.7881072

[13] P. Kela, J. Turkka, and M. Costa. 2015. Borderless Mobility in 5G Outdoor Ultra-Dense Networks. *IEEE Access* 3 (2015), 1462–1476. https://doi.org/10.1109/ACCESS.2015.2470532

[14] Rasib Khan, Shams Zawoad, Md Munirul Haque, and Ragib Hasan. 2014. OTIT: Towards Secure Provenance Modeling for Location Proofs. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '14)*. ACM, 87–98. https://doi.org/10.1145/2590296.2590339

[15] Michael P Lammert, Adam Duran, Jeremy Diez, Kevin Burton, and Alex Nicholson. 2014. 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* 7, 2014-01-2438 (2014), 626–639.

[16] Wanying Luo and Urs Hengartner. 2010. VeriPlace: A Privacy-aware Location Proof Architecture. In *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS '10)*. ACM, 23–32. https://doi.org/10.1145/1869790.1869797

[17] M. Ma, J. An, Z. Huang, and Z. Cao. 2015. Sensor data fusion based on an improved dempaster-shafer evidence theory in vehicular cyber-physical systems. In *2015 IEEE International Symposium on Intelligent Control (ISIC)*. 683–687. https://doi.org/10.1109/ISIC.2015.7307289

[18] S Santini, A Salvi, AS Valente, A Pescape, M Segata, and R Lo Cigno. 2015. A consensus-based approach for platooning with inter-vehicular communications. In *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 1158–1166.

[19] R. K. Schmidt, T. Leinmuller, E. Schoch, F. Kargl, and G. Schafer. 2010. Exploration of adaptive beaconing for efficient intervehicle safety communication. *IEEE Network* 24, 1 (Jan 2010), 14–19. https://doi.org/10.1109/MNET.2010.5395778

[20] R. Schubert, E. Richter, and G. Wanielik. 2008. Comparison and evaluation of advanced motion models for vehicle tracking. In *2008 11th International Conference on Information Fusion*. 1–6.

[21] Michele Segata, Stefan Joerer, Bastian Bloessl, Christoph Sommer, Falko Dressler, and Renato Lo Cigno. 2014. PLEXE: A Platooning Extension for Veins. In *6th IEEE Vehicular Networking Conference (VNC 2014)*. IEEE, 53–60. https://doi.org/10.1109/VNC.2014.7013309

[22] Christoph Sommer, Reinhard German, and Falko Dressler. 2011. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Transactions on Mobile Computing* 10, 1 (January 2011), 3–15. https://doi.org/10.1109/TMC.2010.133

[23] C. Sommer, S. Joerer, M. Segata, O. K. Tonguz, R. L. Cigno, and F. Dressler. 2015. How Shadowing Hurts Vehicular Communications and How Dynamic Beaconing Can Help. *IEEE Transactions on Mobile Computing* 14, 7 (July 2015), 1411–1421. https://doi.org/10.1109/TMC.2014.2362752

[24] X. Wang, A. Pande, J. Zhu, and P. Mohapatra. 2016. STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users. *IEEE/ACM Transactions on Networking* 24, 6 (December 2016), 3276–3289. https://doi.org/10.1109/TNET.2016.2515119

[25] Brent Waters and Edward Felten. 2003. Secure, private proofs of location. *Department of Computer Science, Princeton University, Tech. Rep. TR-667-03* (2003).

[26] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson. 2017. 5G mmWave Positioning for Vehicular Networks. *IEEE Wireless Communications* 24, 6 (Dec 2017), 80–86. https://doi.org/10.1109/MWC.2017.1600374

[27] Z. Zhu and G. Cao. 2011. APPLAUS: A Privacy-Preserving Location Proof Updating System for location-based services. In *2011 Proceedings IEEE INFOCOM*. 1889–1897. https://doi.org/10.1109/INFCOM.2011.5934991