SVM: Secure Vehicle Motion Verification with a Single Wireless Receiver

Mingshun Sun, Yanmao Man, Ming Li
Department of ECE, University of Arizona
Tucson, Arizona
{mingshunsun,yman,lim}@email.arizona.edu

Ryan Gerdes
Department of ECE, Virginia Tech
Arlington, Virginia
rgerdes@vt.edu

ABSTRACT

Connected vehicles leverage wireless interfaces to broadcast their motion state information for improved traffic safety and efficiency. It is crucial for their motion claims (location and velocity) to be verified at the receivers to detect spoofing attacks. Existing approaches typically require multiple cooperative distributed verifiers, which is not applicable to vehicular networks. In this work, we propose a secure motion verification scheme based on Angle-of-Arrival and Frequency-of-Arrival that only requires a single verifier, by exploiting opportunistic signal reflection paths in the environment to create multiple virtual verifiers. We analyze the security of our scheme both theoretically and under realistic road topology. We also carry out real-world experiments with two vehicles in a campus environment, and results show that our scheme can accurately detect false motion claims in a low relative speed vehicular network.

CCS CONCEPTS

• **General and reference → Measurement**; • **Hardware → Digital signal processing**; • **Security and privacy →** *Intrusion detection systems*; **Mobile and wireless security**.

KEYWORDS

Secure Motion Verification, Secure Vehicle Tracking, Angle-of-Arrival, Doppler Effect, Multipath

ACM Reference Format:
Mingshun Sun, Yanmao Man, Ming Li and Ryan Gerdes. 2020. SVM: Secure Vehicle Motion Verification with a Single Wireless Receiver. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), July 8–10, 2020, Linz (Virtual Event), Austria.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3395351.3399348

1 INTRODUCTION

Autonomous systems have gained significant research interests recently, such as connected/autonomous vehicles (CAVs) [40], unmanned aerial vehicles (UAVs) [2]. In such systems, vehicle-to-everything (V2X) communication can be adopted to broadcast the vehicle state information such as position, velocity and acceleration (PVA), which can improve the traffic safety and efficiency. For example, in vehicle platooning applications[10], Vehicle-to-Vehicle (V2V) communication helps platoon vehicles to maintain proper speed and inter-vehicle distance to increase the road capacity and enhance safety. In the air, UAVs typically broadcast their motion states (position and velocity) to be tracked or controlled by ground stations [59], for air collision-avoidance and geo-fencing applications [20].

If the PVA information is incorrect (e.g., maliciously falsified by an adversary at the message source or during transmission), severe consequences may entail. For example, if a misbehaving connected vehicle in a platoon broadcasts a false message that it is running at 10 mph but the actual speed is 60 mph, it may cause all following vehicles to enter traffic congestion while itself may gain unfair advantage. To carry out such spoofing attacks, an adversary who gains control of the vehicle may alter the communication interfaces (e.g., via reprogramming electronic control units [49]), or compromise on-broad sensors [5].

Traditional crypto-primitives, such as digital signatures and message authentication codes, can only verify the authenticity and integrity of messages during their transmission [19], but not the veracity or truthfulness of the data content as it can be modified at the source. Approaches that leverage *out-of-band* sensing modalities have been proposed for vehicle/UAV detection, ranging and tracking, such as cameras [47], radar [1], lidar [23], etc. However, these methods require extra hardware which incurs additional cost (e.g. around one thousand dollars for a usable on-board radar[30] or lidar[37]). And those sensors can also be compromised remotely [5]. *In-band* techniques have been proposed for source localization and tracking, but they are insecure and/or need multiple verifiers. For example, received signal strength (RSS) can be easily spoofed by power control/directional antennas. In addition, Doppler effect (DE) is often used to measure the relative speed for vehicle tracking [38]. However, a malicious source may manipulate the center frequency of the transmitted signal to deceive the DE-based velocity verifiers. Recent work [32] proposed DE-based secure motion verification for aircraft which can detect such attacks, but it requires multiple spatially-distributed verifiers and assumes static adversaries. It is too costly to install multiple trustworthy verifiers. Besides, multiple verifiers on the same vehicle do not provide additional security than one verifier, since they are very close to each other.

In this work, we aim to securely verify a target vehicles' motion state information with a single verifier (e.g., an on-board unit on a moving car or a ground station), without assuming any restrictions on the target vehicle (adversary)'s motion, who is also able to manipulate both motion claims and its signal carrier frequency. There are multiple challenges involved. First, the receiver should

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
WiSec '20, July 8–10, 2020, Linz (Virtual Event), Austria
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-8006-5/20/07…$15.00
https://doi.org/10.1145/3395351.3399348

be able to independently verify the target vehicle's claims without the help of other nearby devices/vehicles since there may not exist trusted infrastructure in a V2V scenario Also, if we assume that the verifier trusts its receiver only, many existing localization/tracking approaches become inapplicable. In addition, existing methods that directly estimate Doppler spread/shift from channel state information [16] tend to be error-prone in such low relative speed, fast-changing, multi-path rich channel environments [57].

To deal with the aforementioned challenges, we propose an in-band secure motion verification framework, which exploits the Angle-of-Arrival (AOA) and Frequency-of-Arrival (FOA) measured from the received RF-signal (by a multi-antenna receiver). In contrast to previous works in source localization that predominantly leverage only the line of sight (LOS) path, we find that the multi-path effect (e.g., caused by reflection) can be used as an opportunity to enhance security, because each signal path results in a different Doppler shift, due to different radial velocity (related to the AoA). Our basic idea is to check if the expected FOA (computed from the motion claim) is close to the measured FOA on each signal path. Assuming the AoA measurement is unforgeable, an adversary who falsifies its claim will be infeasible to simultaneously bypass all the checks if there are more than three paths. The main challenge is that the FOA on each path depends on the physical environment, specifically the location and orientation of the reflectors which may not be known in advance. To address this, we first model the potential reflectors based on public maps, then use a Maximum Likelihood Estimator (MLE) to infer the most probable source location based on signal reflection models and the AoA measurement. To handle the unknown signal frequency offset between the transmitter and receiver, a Frequency Difference of Arrival approach (FDOA) [32] is adapted to compare the measured FDOA with the expected ones on each path. In summary, we make the following contributions:

(1) To the best of our knowledge, we propose the first single-verifier based in-band secure motion claim verification scheme, by exploiting the multi-path signal propagation effect. Security analysis shows that it is secure against powerful attackers who can both spoof the claims and also change the signal carrier frequency, given enough number of paths.

(2) We resolve several practical challenges in our scheme, including modeling and inferring real-world signal reflectors in a probabilistic manner, which helps locate the signal source and verify its velocity without knowing the exact reflectors in advance. In addition we adopt an FDOA-based approach to eliminate the unknown carrier frequency offset, which is significant for low relative-speed source/receiver pairs.

(3) We carry out extensive real-world experiments on software-defined radio platforms to evaluate the effectiveness of the proposed scheme in a campus environment. We report the receiver-operating characteristic (ROC) curves for the detection of false claims as well as errors for location estimation. Results show that we can securely verify the vehicle claims and approximately track the movement of a target vehicle within 30 meters.

2 RELATED WORK

In this section, we discuss two areas of related work: wireless signal localization and vehicle motion claim verification and tracking.

2.1 Wireless Signal Source Localization

Numerous works have studied this topic, and the basic principle is based on triangulation. For example, RSS [28], Time-of-Flight (TOF), Time-Difference-of-Arrival (TDOA) [4, 33] measurements were used to estimate the distance from the source to each anchor. AOA measures the LOS signal directions and intersection locates the source position [12, 43, 52]. However, multiple spatially-separated anchors (receivers) are required for triangulation (at least three for 3-D), which does not apply to the problem setting in this paper. For a complete survey of wireless localization methods, readers can refer to [6].

On the other hand, some recent works proposed to utilize a single receiver for source localization. For example, Du et. al. [12] leverages one moving anchor node to estimate the location of a static signal source based on AoA intersection, which is not applicable to our setting as the source is mobile. Vasisht et. al. [42] proposed a single AP based accurate localization method by finding the LOS path angle and estimate the distance with RSS. In [43] they also propose simultaneous localization and channel estimation for cellular networks, which requires estimating each path's channel gain, whereas our approach does not need it. A few works in indoor mmWave communication [46, 61] do channel prediction based on the reconstruction of the multi-paths in the environment, however, they require full and exact knowledge of reflectors via significant training. Also, these works are not directly applicable to localization. Note that mmWave has much higher frequencies than the ones considered in our work (sub 6 GHz), and the latter is much more challenging due to different propagation characteristics.

2.2 Location and Motion Verification

All the above studies were done under a non-adversarial setting. Capkun et.al. [6, 7] showed that distance estimation based wireless positioning techniques are subjected to malicious attacks (for example, distance spoofing with RSS and TOF by changing signal power and timing). They propose a verifiable multilateration scheme based on distance bounding. However, distance bounding is not yet practical and it usually requires out-of-band channels or special hardware [1, 26].

Other secure positioning or location verification schemes [11, 14, 22, 45] use multiple verifiers to filter out the false position claims and improve the localization accuracy, while cooperation among the verifiers is needed which may limit their practicality. More recently, several works exploit the inherent mobility of the prover [31], or the verifier [4], or both [33], to relax the requirements of previous approaches. However, random [4] or controlled [33] mobility is not applicable to vehicular networks nor stationary ground stations as verifiers. On the contrary, our approach does not assume stationary provers [31, 33], while we can handle both stationary and mobile provers and verifiers.

On the other hand, several works utilize Doppler effect for motion verification, e.g., [16] and [32] focusing on aircraft motion verification only, while this work considers cars and UAVs that move slower and in a more complicated (noisy) environment such as urban areas. A secure vehicle tracking scheme is proposed by Sun et al. [38], which exploits the implied effect of Doppler Shift (DS) and AoA measurements to verify a target vehicle's movement

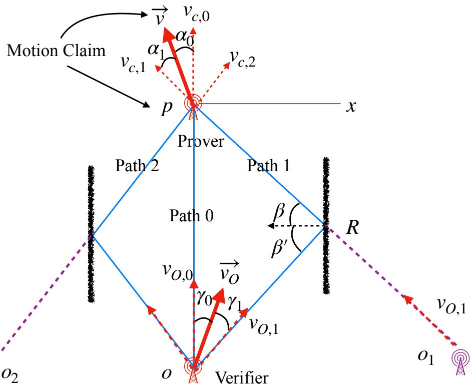


Figure 1: System model. R **stands for a reflection point;** o_i **is a virtual verifier for the path** i **(mirroring** O**).**

and uses a modified extended Kalman filter for secure tracking. However, they assume that DS can be securely measured without proposing a concrete design, and require at least one trustworthy neighboring vehicle to provide extra measurements. In contrast, in this work we do not make such assumptions and aim at using only one receiver for in-band motion verification.

For more specific applications such as vehicular networks or platooning, various methods have been proposed for misbehavior detection or position verification/authentication. These works either detect location spoofing or measure spacing between vehicles using other modalities (e.g., radar [55], cameras [26], LiDARs [10, 61], accelerometers [21]) and use AoA/TDOA/RSS but assume static provers [9], focus on detecting other attacks such as Sybil attacks using RSS [56], or assume honest majority of vehicles [58]. However, these works require extra hardware or out-of-band channels, and these sensors are subject to varying attacks [5, 24]. In contrast, our approach is in-band and has more general applications.

For in-band location verification approaches, a recent scheme [36] based on RSS distribution can only roughly verify the distance of a vehicle since RSS is noisy in reality, and is not secure against stronger adversaries that can change the transmission power. There are other methods for location verification using channel signatures trained from the CSI[60], however they are vulnerable to multipath camouflage attacks [13], in which a device's CSI can be forged by an attacker at a different location using precoding assuming the CSI is known. Our proposed method is based on AOA, which is not subjected to the camouflage attack.

3 PROBLEM STATEMENT

Our problem is defined as follows: A (stationary or moving) verifier $\mathcal{V}$ aims to verify whether the motion claim C of a (stationary or moving) prover $\mathcal{T}$ is true or not. The motion claim tuple is defined as $C = (p, \overrightarrow{v})$, where p represents the prover's position claim and $\overrightarrow{v}$ denotes the velocity claim vector. For simplicity, we consider a 2D Cartesian coordinate system in the following. Similar analysis can also be extended to 3-D.

3.1 System Model and Assumptions

As illustrated in Fig. 1 (a snapshot), the prover periodically broadcasts its current claim tuple $C = (p, \overrightarrow{v})$ via wireless messages with a pre-defined signal center frequency f_0. For simplicity, we assume the transmitter uses omnidirectional antennas[1]. Meanwhile, the verifier, which locates within the transmission range of the prover, moves at a velocity $\overrightarrow{v_o}$ at position o and receives the signal by a fixed antenna array. We consider a generic multi-path signal propagation model [41], which can include both the LOS path[2] (Path 0) and reflection paths (e.g., Paths 1 and 2). Such models are widely adopted in vehicular networks [25, 39, 44]. However, we do not assume any knowledge on the statistical parameters of the channel model (such as path loss exponent etc.). Instead, since our goal is not to estimate the channel but verify the location and velocity, we assume there are only one-hop reflections on each path which is dominant over multi-hop reflection in terms of received power for outdoor applications [34], and there are several *potential* reflectors in the surrounding environment, whose positions and orientations are known by the verifier a priori (which can be extracted from public maps, or deployed by the verifier in advance). Note that exact signal reflectors are not known in advance which must be inferred in real-time. Besides, we consider imperfect signal reflection directions (such as the probabilistic distribution in [18]) due to non-smooth reflector surfaces, i.e., β is not necessarily equal to β' (Fig. 1). We assume that the verifier always knows its own location and velocity (e.g., via GPS).

3.2 Doppler Effect

As illustrated in Fig. 1, we define $v_{c,0}$ and $v_{o,0}$ as the radial speed of the prover's and verifier's claim along the direction of Path 0:

$$v_{c,0} = |\overrightarrow{v}| \cdot \cos(\alpha_0) \quad v_{O,0} = |\overrightarrow{v_O}| \cdot \cos(\gamma_0) \tag{1}$$

Because of the Doppler effect, the frequency of arrival (FOA) along Path 0 can be expressed as

$$f_{r,0} = f_0 \cdot \frac{c + v_{O,0}}{c + v_{c,0}} = f_0 \cdot \frac{c + v_o \cdot \cos(\gamma_0)}{c + v \cdot \cos(\alpha_0)} \tag{2}$$

where c is the speed of light and f_0 is the carrier frequency. We denote $v = |\overrightarrow{v}|$ and $v_o = |\overrightarrow{v_o}|$ for convenience. The above equation is for the true FOA, thus it does not include the frequency offsets and measurement noise.

Meanwhile, signal reflections in non-line-of-sight (NLOS) paths lead to different amounts of Doppler shifts on each path. In general, a reflector changes the Doppler effect by changing the radial speed of both transmitter and receiver. Take Path 1 for an example, where the signals transmitted from the prover is reflected by R and then arrives at the verifier. The Doppler shift of this signal can be divided into two parts: the first is induced between the prover and the reflection point R, and the second part appears between R and the verifier. For a stationary reflection point R, the FOA is computed by the following two equations:

$$f_{m,1} = f_0 \cdot \frac{c}{c + v_{c,1}}, \tag{3}$$

$$f_{r,1} = f_{m,1} \cdot \frac{c + v_{O,1}}{c} = f_0 \cdot \frac{c + v_{O,1}}{c + v_{c,1}}, \tag{4}$$

where $f_{m,1}$ is the signal FOA at reflection point R, and $f_{r,1}$ is the FOA at the verifier. Also, $v_{c,1} = v \cdot \cos(\alpha_1)$ and $v_{o,1} = v_o \cdot \cos(\gamma_1)$. We can

[1] Directional antennas can also be used but it may not result in as many paths needed for security, as with omnidirectional antennas.

[2] Existence of the LOS path is not necessary but will enhance performance.

see that the position and orientation of the reflection point R only changes the radial speed of both the prover and the verifier, but it does not cause any additional frequency shifts. The same result holds even when the reflector is moving (omitted due to space limitations). In fact, adding one reflection path can be regarded as adding a virtual verifier located at the mirror position with respect to the reflection surface (as shown in Fig. 1). Therefore, each multi-path can provide an additional virtual verifier that is spatially separated from each other, which is leveraged to enhance security in our scheme.

3.3 Threat Model

We consider an attacker who gains full control of the prover, that aims to successfully claim a false motion $C = (p, \overrightarrow{v})$ different from its real one $C_a = (p_a, \overrightarrow{v_a})$ without being detected by the verifier. First, the attacker can modify/shift the signal carrier frequency f_0. There can be two types of changes: one is arbitrary shift [32] (which is stronger but makes sense for unidirectional communication), the other is restricted within the correctable central frequency offset range (CCFOR), which guarantees the successful message decoding [16, 17] in the wireless system (more suitable for bi-directional communication). However, the transmitted signal frequency remains the same in all directions[3]. Second, we assume an arbitrarily mobile prover whose velocity claim v_c is only constrained by the physical limitations of the source vehicle. For example, for a signal source mounted on vehicles or UAVs, the maximum moving speed and heading are limited by the engine power as well as traffic rules. Besides, we assume the prover/adversary is always aware of the position and velocity of the verifier (e.g., from the V2V messages), and also the whereabouts of the reflectors in the environment (e.g., from publicly available maps). The verifier trusts its own measurements, and the AOA is assumed to be unforgeable [52, 53], because it is difficult for attackers to deploy their own or change existing reflectors in the physical environment.

4 BASIC IDEA AND CHALLENGES

We introduce our basic idea for motion claim verification with a single receiver, and analyze its security properties and challenges.

4.1 Basic Idea of Claim Verification

The main idea of our motion claim verification is to measure the *actual* FOA measured on each individual path and cross-check its consistency with the respective *expected* FOA computed from the claim. Once the verifier detects a mismatch on any path, an alarm will be raised. Specifically, let us define a set M containing all the signal paths (including the LOS and several reflected ones) that arrive at the receiver. Define $f_{c,m}$ and $f_{a,m}$ as the expected and actual signal FOA, respectively, for a path $m \in M$ as follows

$$\begin{aligned} f_{c,m} &= f_0 \cdot \frac{c + v_{O,m}}{c + v_{c,m}} = f_0 \cdot \frac{c + v_O \cos(\gamma_m)}{c + v \cdot \cos(\alpha_m)}, \\ f_{a,m} &= f_a \cdot \frac{c + v'_{O,m}}{c + v_{a,m}} = f_a \cdot \frac{c + v_O \cos(\gamma'_m)}{c + v_a \cos(\alpha'_m)}, \end{aligned} \tag{5}$$

where $v_{O,m}$ and $v_{c,m}$ are the expected radial speed of the verifier and prover based on the prover's claimed motion tuple, respectively; $v'_{O,m}$ and $v_{a,m}$ are the actual radial speed of the verifer and prover based on the actual prover's motion tuple; f_0 is the expected (nominal) signal carrier frequency; f_a is the modified (actual) carrier frequency; γ_m and α_m, γ'_m and α'_m are the projection angles of the claimed velocity $\vec{v}$ and actual velocity $\vec{v}_a$ at Path m, respectively.

The verification criteria: If there exists at least one path $m \in M$ that violates the following constraints, an alarm is raised:

$$|f_{c,m} - f_{a,m}| \leq \mathcal{T}, \forall m \in M, \tag{6}$$

where $\mathcal{T}$ is a properly defined threshold. In other words, all measured paths should satisfy Eq. (6) to pass the verification.

4.2 Security Analysis and Challenges

The attacker aims to make $f_{c,m} = f_{a,m}$ for all $m \in M$ with $C \neq C_a$:

$$f_0 \cdot \frac{c + v_O \cos(\gamma_m)}{c + v \cdot \cos(\alpha_m)} = f_a \cdot \frac{c + v_O \cos(\gamma'_m)}{c + v_a \cos(\alpha'_m)}, \forall m \in M, \tag{7}$$

Since several variables above are related to each other, we re-express the α_m as a function of the motion claim p and $\overrightarrow{v}$, such as $\alpha_m = g_m(p, \overrightarrow{v})$. For example, α_0 in Fig. 1 can be written as

$$\alpha_0 = g_0(p, \overrightarrow{v}) = \angle \overrightarrow{v}, \overrightarrow{op} = |\angle \overrightarrow{v}, \overrightarrow{x} - \angle \overrightarrow{op}, \overrightarrow{x}|$$

where $\overrightarrow{x}$ is the x axis direction. Similarly, γ_m is a function of p and we can express it as $\gamma_m = h_m(p)$. Note that α_m and γ_m are also related to the reflection point R_m, but since the verifier's position and reflectors are out of adversary's control, we omit it for simplicity. Therefore, (7) can be re-written as:

$$f_0 \cdot \frac{c + v_O \cos(h_m(p))}{c + v \cdot \cos(g_m(p, \overrightarrow{v}))} = f_a \cdot \frac{c + v_O \cos(\gamma'_m)}{c + v_a \cos(\alpha'_m)}, \forall m \in M, \tag{8}$$

where v_O, γ'_m, α'_m and v_a capture the actual value, which cannot be modified, and f_0 is fixed. The attacker can control $\overrightarrow{v}$, f_a, γ_m and α_m by manipulating the carrier frequency f_a, position claim p, velocity claim $\overrightarrow{v}$ (include both heading and speed). In general, if we only focus on one time step, heading and speed can be independently claimed. The attacker has 4 variables (degrees of freedom) and theoretically we need at least 5 independent constraints (paths) to make the attack fail to find a feasible tuple.

One major challenge is that, there may not always exist 5 observable paths in real-world outdoor environments (even if there are enough reflectors the received power on a path may be too weak). Thus, we need to reduce the path requirement. A straight-forward way is to verify at multiple consecutive time steps. For example, we can require that the claimed positions and velocity of adjacent times to be consistent with kinematic equations, which means the verifier needs one less path for each time step. But we still need to minimize the number of free variables that the attacker can control to make our scheme both secure and practical. In addition, another challenge is to deal with measurement noise and error. The central frequency offset (CFO) of the signal transmitter is unknown which impacts the measured FOA, and the error incurred by Doppler resolution, which is low when the data sampling rate is low. Moreover, the receiver needs to infer which reflectors are actually used in each path, and obtain their positions and orientations. In a typical channel environment for sub-6GHz, reflection and refraction often

[3] We assume the attacker cannot use multiple devices to simultaneously transmit the same signal in different carrier frequencies along different directions (commonly assumed by previous works [16, 32])

coexist and different surfaces exhibit different reflection characteristics. Last but not least, the verifier needs to correctly match the frequency peaks in the measured FOA profile to their corresponding paths measured by AOA distribution. We will describe our ideas to address each of them in Sec. 5.

5 SECURE VERIFICATION METHOD

Fig. 2 shows the high-level overview of our claim verification scheme to examine the motion claim. To further reduce the number of adversary controlled variables, we decompose the problem into two sub-problems and sequentially verify position claim p and velocity claim $\overrightarrow{v}$. In short, after receiving the RF signal, the verifier measures the AOA and FOA distributions and decodes the motion claim. Then, if multiple paths exist, based on the measured AOA and prior knowledge of the candidate reflectors, we employ an MLE to infer the most probable reflector on each path. This is used as input to location claim verification, and also provides an estimated location as a byproduct. This helps to reduce the number of controllable variables of the attacker by one for velocity verification. Then, an FDOA-based approach is adopted to verify the velocity claim which eliminates the unknown frequency offset, as well as circumvents the complicated path AOA-to-FOA matching. The detailed algorithms and security analyses are presented next.

5.1 Identify the Signal Directions of Arrival

Our method makes use of the opportunistically reflected signals to obtain the AOAs of each path and corresponding frequencies. The verifier first identifies the signal paths by estimating the AOA distribution of the received signal, which is the incoming signal's power distribution at different arrival directions. For illustration, we pick the MUSIC [52] algorithm where the signal power distribution $P_{\text{AOA}}(\phi)$ is computed as:

$$P_{\text{AOA}}(\phi) = \frac{1}{a(\phi)E_N E_N a(\phi)} \tag{9}$$

Detailed explanations can be found in [52]. Next, the verifier locates all the potential paths from the AOA distribution, including both LOS path and reflected paths, by finding peaks in the distribution. The number of peaks represents the number of potential paths in the received signal. For example, in Fig 3, the red distribution around the verifier represents the AOA distribution, which has 3 peaks. If not blocked, the direction of the LOS path usually exhibits the highest incoming power. In general, if there are M peaks, we pick the highest peak as the direct (LOS) path (path 0) and other $M-1$ peaks as reflection signal paths.

5.2 Position Claim Verification

After we find out the number of paths and their arriving directions, we verify the position claim p by modeling and inferring the most likely environmental reflectors on each path, and subsequently verifying the source location claim. As a result it also outputs an estimated location. This is presented in algorithm 1.

5.2.1 *Problem Formulation.*

The basic idea of the position verification is to estimate the most probable signal location first and then compare it with the claimed p. Therefore, it becomes a secure localization problem which is formulated as follows. We first define a search boundary $\mathcal{K}$, as the possible area that the prover can be locate in. The basic idea is to go through all the candidate locations $k \in \mathcal{K}$ (discretized according to a certain resolution), and find the most likely position k^* which is consistent with the measured AOA distribution. The likelihood of observing an AOA distribution $P_{\text{AOA}}(\phi)$ given a candidate source position k, the potential reflector set $\mathcal{R}$ and the verifier position o, is defined as follows:

$$L_k = Pr(P_{\text{AOA}}(\phi)|o, \mathcal{R}, k). \tag{10}$$

The verifier aims to find the best candidate position k^* which maximizes the likelihood of the AOA distribution $P_{\text{AOA}}(\phi)$, i.e.,

$$k^* = \arg\max_{k \in K} L_k. \tag{11}$$

Since $P_{AOA}(\phi)$ consists of multiple different peaks, and we can assume that the probability distribution of each path (direction) is independent of each other (typical assumption in rich-scattering channel models [50]), we can express the likelihood L_k by multiplying the likelihoods of each individual path $L_{m,k}$:

$$L_k = \prod_{m \in M} L_{m,k} = \prod_{m \in M} Pr(m|o, \mathcal{R}, k), \tag{12}$$

where $Pr(m|o, \mathcal{R}, k)$ represents the likelihood of the m-th path/peak appearing in $P_{AOA}(\phi)$. The next question is how to calculate $L_{m,k}$.

5.2.2 *Likelihood of the Direct Path.*

For the direct (LOS) path, since there is no reflection, the verifier can directly calculate the direction of arrival $\phi_{m,k}$ of a candidate location k based on the coordinates of k and verifier o. The difference between the measured AOA ϕ_m and the expected angle $\phi_{m,k}$ (under mirror reflection) is $\tilde{\phi}_{m,k} = \phi_{m,k} - \phi_m$. It is caused by AOA measurement error, which is usually modeled as standard Gaussian distribution [18]. Denoting it by N_{AOA}, the likelihood $L_{m,k}$ can be expressed as

$$L_{m,k} = N_{\text{AOA}}\left(\tilde{\phi}_{m,k}\right). \tag{13}$$

When $\phi_{m,k}$ approaches to ϕ_m, the likelihood increases.

5.2.3 *Likelihood of a Reflection Path.*

Assume the verifier already extracted the set of candidate surrounding reflectors $\mathcal{R}$ and their orientations from a map. Due to the complexity of the environment, it is difficult to find the exact reflector and reflection points that correspond to each reflection path. Also, we cannot assume perfect mirror reflection because the reflection surface is not perfectly smooth. Therefore, we need to first infer the most probable reflector for each path. The idea is illustrated in Fig. 3 where we show a reflection path 1 at direction oR_1.

Based on the AOA distribution $P_{AOA}(\phi)$, the verifier draws an extended line along the AOA peak direction and find its intersection with all known surfaces $R \in \mathcal{R}$. The orientation of each reflector is denoted as $\theta_R, \forall R \in \mathcal{R}$. We assume there are N_m potential reflectors along path m. Then the probability of obtaining this path m from the candidate position k can be expressed using the total probability theorem as follows

$$L_{m,k} = Pr(m|k, o, \mathcal{R}) = \sum_{R=1}^{N_m} Pr(m|k, R, o) \cdot Pr(R) \tag{14}$$

Without any knowledge of R, we assume a uniform distribution for $Pr(R)$, thus $Pr(R) = 1/N_m$. Also, the $Pr(m|k, R, o)$ can be modeled by considering the signal reflection distribution P_{ref}.

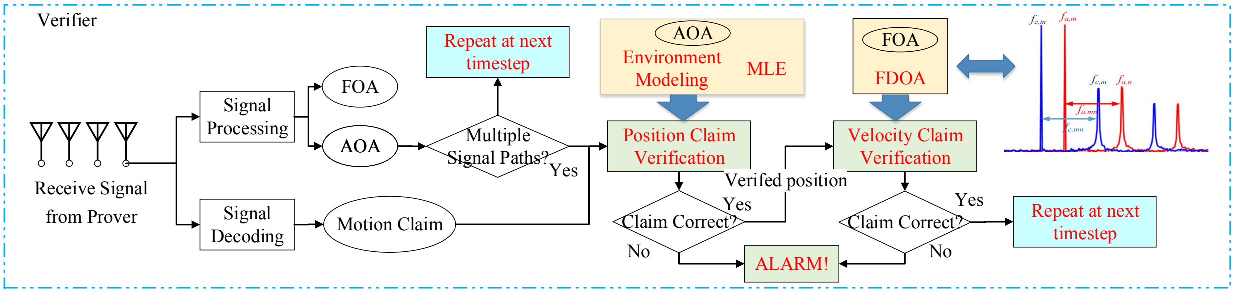


Figure 2: Overview of SVM, our Secure Motion Verification Scheme

Since the mirror reflection cannot always be assumed due to the non-smoothness of the reflection surface, the incident and exit angles of a reflector are not necessarily equal. For example, we can see that the reflector R_1 is more likely than R_2 to be the actual reflector on Path 1 since it is closer to mirror reflection (Fig. 3). We model it in a probabilistic manner as follows. For reflector R_1, the incident ray is kR_1. Then, the likelihood of R_1 being the actual reflector of Path 1 for candidate position k is equal to the conditional probability that the signal reflects according to the exit angle β' given an incident angle β. This conditional distribution, denoted as P_{ref}, can be expressed as

$$Pr(m|k, R, o) = P_{\text{ref}}\left(\beta'_R|\beta_R\right), \tag{15}$$

where β_R and β'_R are the incident and exit angle of reflector The above assumes that the measured AOA is on a perfect line. However, the AOA is a distribution around a peak angle and we need to account for AOA estimation error. Thus, we can relax the AOA directions to a range/cone of angles (determined by the error distribution), which changes the intersection with each reflector R_n from a point to a segment. It is illustrated in Fig. 3 using path 2 on the left. We denote this range as C_R for the reflector R. Then, integrating P_{ref} over all reflection points within this range, for a given $k \in \mathcal{K}$ and $R \in \mathcal{R}$:

$$Pr(m|k, R, o) = \int_{r \in C_R} P_{\text{ref}}\left(\beta'_R(r)|\beta_R(r)\right)\, \mathrm{d}r \tag{16}$$

Here r is a point in segment C_R. $\beta_R(r)$ and $\beta'_R(r)$ are both a function of r, k, and o. After we get $Pr(m|k, R, o)$ for any $R \in \mathcal{R}$, we calculate $L_{m,k}$ using Eq. 14.

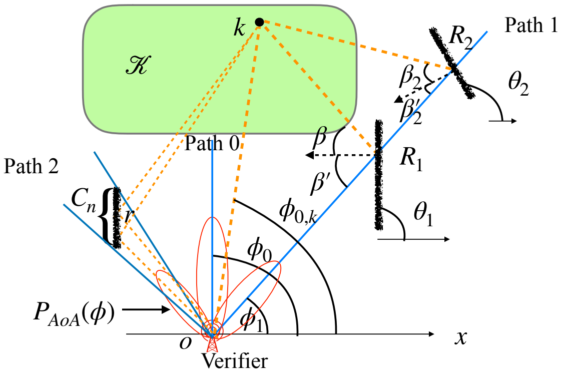


Figure 3: Position verification method

5.2.4 Position Estimation Using Combined Likelihood. After the verifier computes the likelihoods of the direct path and reflection paths from Eqs. (16) and (13) for each candidate location k, it multiplies the likelihoods $L_{m,k}, \forall m \in M$ to obtain the total likelihood L_k by Eq. (12). Finally, the estimated position k^* can be derived by solving (11). More explicitly, we cannot accept a very low-likelihood k^* even though it is relatively larger than other positions in the feasible region. More detailed discussion is in Sec. 6.2.

5.2.5 Position claim verification. After the verifier obtains the estimated position k^*, it computes the distance between k^* and the claimed position p. If the distance is larger than a threshold Q, an alarm will be raised. Otherwise, it accepts the position claim p and uses it as input to the velocity claim estimation. We discuss how to choose Q in Sec 5.4.3. However, if there is no multipath in the environment (only LOS path available), the k^* becomes a line along the direction of LOS path because points on this line share the same highest likelihood. If the LOS path is not available, two reflection paths are required to provide an intersection in the estimated area. Therefore, our position estimation framework requires at least two signal paths for position estimation.

5.3 Velocity Claim Verification

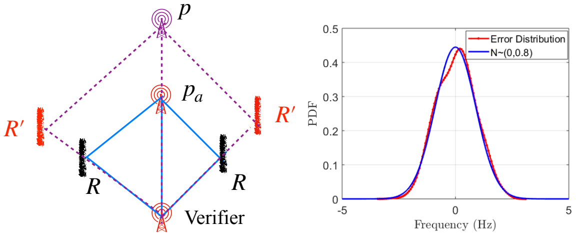
After estimating the source position, we adapt the FDOA approach from [32] into our problem to verify the velocity claim $\overrightarrow{v}$, meanwhile eliminate the unknown frequency offset and avoid the complicated signal FOA-path matching. First we revisit our system equations in (5) and add the frequency offset and errors in the measured FOA:

$$\begin{aligned} f_{c,m} &= f_0 \cdot \frac{c + v_o \cos(\gamma_m)}{c + v \cdot \cos(\alpha_m)} \\ f_{a,m} &= f_a \cdot \frac{c + v_o \cos(\gamma'_m)}{c + v_a \cos(\alpha'_m)} + \epsilon_p + \epsilon_o + \epsilon_m \end{aligned} \tag{17}$$

where ϵ_m accounts for FOA resolution error, ϵ_p and ϵ_o denote the frequency offset in the prover and verifier, respectively. The measured (actual) FDOA between two paths m and n is defined as $f_{a,mn} = f_{a,m} - f_{a,n}$, where the unknown frequency offset ϵ_o and ϵ_p are canceled, the only remaining error term becomes $\epsilon_{mn} = \epsilon_m - \epsilon_n$. Similarly, the expected FDOA is computed as $f_{c,mn} = f_{c,m} - f_{c,n}$

The idea of our proposed FDOA-based velocity verification scheme is to verify the FDOA between pairs of paths instead of FOA from a single path. Specifically, for each pair of paths m and n in M, the verifier checks the following conditions:

$$\left|f_{a,mn} - f_{c,mn}\right| \leq \mathcal{T}, \forall m, n \in M, m \neq n. \tag{18}$$



(a) Wrong Position Estimation **(b) Error Approximation**

Figure 4: A corner case (a), and error distribution (b).

If there exists one pair of m and n that violates the above criterion, the verifier will raise an alarm. We refer to $|f_{a,mn} - f_{c,mn}|$ as FDOA deviation, where we also let $f_{a,mn} - f_{c,mn} = f_{d,mn} + \epsilon_{mn}$ for future security analysis. If the motion claim is true (i.e., $\gamma_m = \gamma'_m$, $\alpha_m = \alpha'_m$, $f_a = f_0$), $f_{d,mn}$ will be zero and only the FOA resolution error ϵ_{mn} is left. Thus, the threshold $\mathcal{T}$ should be large enough to bound ϵ_{mn} while small enough to increase false claim detection probability (discussed later).

5.4 Security Analysis

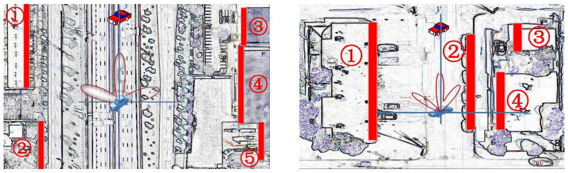
5.4.1 Security of Position Verification. Our position verification algorithm only uses the measured AOA distribution, and the public maps to infer the reflector likelihoods. In general, as long as the AOA cannot be forged and the adversary has no control over environmental reflectors, we need at least two paths to achieve secure location verification and estimation. For the attacker to succeed it needs to find another plausible location p different from the actual one p_a yielding higher likelihood than the actual one. Apart from the false acceptances that depend on measurement error distributions, this is only possible when p and p_a both lead to the same AOA distribution, but with a different set of reflectors.

For example, in Fig. 4a, the prover is actually at position p_a but claims to be at p, and coincidentally, there are two reflectors (other than the actual ones) on both sides, our scheme may output two positions with high likelihood which may make the wrong decision. In this case, we can utilize multiple measurements to improve security and performance. Basically, it is increasingly unlikely for the adversary to find such plausible locations in a continuous manner, since such alternative reflector sets may not always exist.

5.4.2 Security of Velocity Verification. Once the position claim p is verified, for every path, $\gamma_m = \gamma'_m$, and the difference between the claimed projection angle α and the actual angle α' w.r.t. the prover's radial speed also becomes the same. Also, the radial speed angle cannot be changed. As a result, Eq. (17) becomes:

$$f_{a,m} = f_a \cdot \frac{c + v_o \cos(\gamma_m)}{c + v_a \cos(\alpha_m + \eta)} + \epsilon_p + \epsilon_o + \epsilon_m, \tag{19}$$

where η is the difference between the claimed velocity heading and actual heading, which is the same for every path. The attacker's objective is to make the deviation between $f_{a,mn}$ and $f_{c,mn}$ as small as possible in order to bypass the detection. There are three variables that the attacker can control: f_a, η and v, which we group together as an attacking tuple $\mathcal{A} = \{f_a, \eta, v\}$. Theoretically, because the degree of freedom of the attacker is three, the verifier needs at least 4 different pairs of m and $n \in M$ to form a system of linearly-independent equations of the FDOA deviation, in order to prevent the attacker from finding any $\mathcal{A}$ that makes all deviations zero even if it can arbitrarily change its $\mathcal{A}$. In other words, at least 5 different signal paths are required to form 4 linearly-independent equations.



(a) Highway **(b) Urban**

Figure 5: Maps and Reflector Extraction

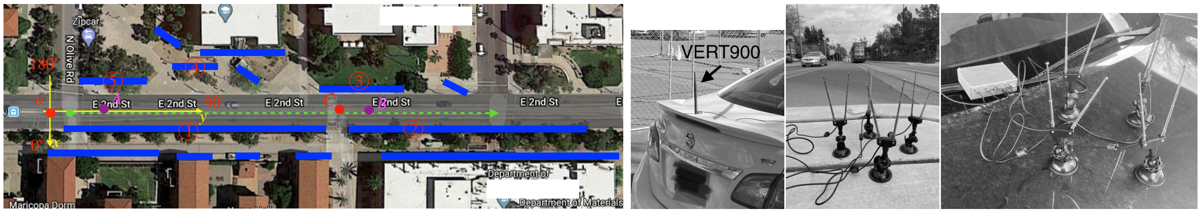
However, when the attacker's claim $\mathcal{A}$ is constrained by the signal decoding requirement and physical limitation of the source vehicle traffic regulations (giving a feasible region $\mathcal{F}$), the number of paths that are required to detect false claims can be reduced. In this case, we formulate the optimal attack strategy as a min-max problem:

$$\min_{f_a} \max_{m,n \in M} \left|f_{a,mn} - f_{c,mn}\right| = \min_{f_a} \max_{m,n \in M, m \neq n} \left|f_{d,mn} + \epsilon_{mn}\right|, \tag{20}$$
$$s.t.\ \ \{f_a, \eta, v\} \in \mathcal{F}, \ \ \forall(\eta, v) \in \mathcal{F} \neq (0, v_a)$$

where the attacker aims to find a modified frequency f_a that minimizes the maximum FDOA deviation among all possible pairs $m, n \in M$, given any false motion claim. However, since the ϵ_{mn} is a non-controllable error, the actual attack strategy becomes minimizing the maximum $|f_{d,mn}|$ regarding all possible pairs $m, n \in M$. If the attacker fails to find any claim within the feasible region that gives a min-max FDOA less than the threshold $\mathcal{T}$, then it achieves practical security. Next we will show that under realistic error distributions and proper thresholds, our scheme can reduce the number of needed paths to three under certain environmental topology.

5.4.3 Error Distribution and Threshold Selection. In our scheme, there are two types of error/noise, i.e. signal reflection noise and FOA resolution error, which dominates the error in the position and velocity claim verification. The FOA resolution error ϵ_m exists when doing FFT over arrived signal samples. This resolution error can be significantly reduced by Gaussian interpolation with Gaussian window [15]. We use experiments to show the resolution error distribution, which is measured with a stationary prover/verifier vehicle pair (same for mobile case). When the sampling duration is 0.128s, we use FFT interpolation and approximate the resolution error distribution as a zero-mean Gaussian with a variance of 0.8 as shown in Fig 4b. Therefore, ϵ_{mn} becomes a zero-mean Gaussian distribution with variance 1.6. Based on [3], different surface materials have different signal reflection angle distributions. Generally, the exit angle distribution P_{ref} can be approximated as a Gaussian $\mathcal{N}(\beta, \sigma^2_{ref})$. where β is the incident angle and σ^2_{ref} is variance. For real-world surfaces and walls in urban buildings, we use 4° as the variance (for metal, this is as low as 1°).

For the selection of thresholds $\mathcal{T}$ and $\mathbf{Q}$, they should be larger than the error of location estimation/FDOA measurement for legitimate provers to reduce false positive rates (FPR). Larger thresholds yield lower FPR but also lower attack detection rate (true positive). Since we use Gaussian error distributions, standard methods can be used to compute thresholds for given FPR, e.g., [27]. Next, we demonstrate the detection performance by simulations.



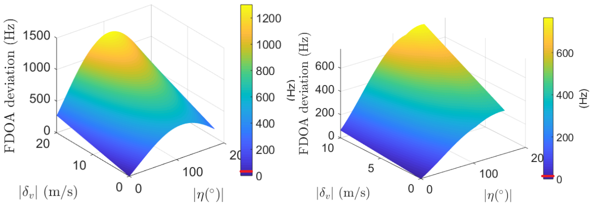
(a) Real-world experiment in an urban campus area **(b) Prover** **(c)** **(d)**

Figure 6: (a) Real-world experiment setup. (b) Prover setup. (c) In Scenario One, Kerberos SDR is the verifier placed on the ground (a street car station in the middle of a street). (d) In Scenario Two, the verifier is on the hood of the following vehicle.

5.4.4 Attack Detection Performance. We demonstrate that security guarantee can be achieved under 3 available paths by evaluating the detection performance via simulation using two representative cases: highway and urban, shown in Figs. 5a and 5b along with the reflector position, orientation (using automatic edge extraction from Google maps). In both figures, the red car denotes the prover, and the verifier (blue car) is at the origin. Detailed parameters are shown as follows: *(a) Highway:* The actual state is p_a=(0,20 m), $\overrightarrow{v_a}$ =(30 m/s, $\zeta_a = \pi/2$(going straight up)). All reflectors are vertical to the horizontal axis, of which distance to the y axis are 40 m, 36 m, 52 m, 50 m, and 57 m for reflectors 1, 2, 3, 4, and 5, respectively. *(b) Urban*: The actual vehicle state is p_a=(0,8 m), $\overrightarrow{v_a}$ =(10 m/s, $\zeta_a = \pi/2$). Reflector's distance to the y axis are 4.5 m, 2 m, 4.5 m, and 3.5 m for 1, 2, 3, and 4, respectively. The verifier runs straight up with the same speed as the prover. Besides, we use same error parameters as described in Sec 5.4.3. We search a 20 × 50 m rectangular area for highway, and a 10 × 50 m rectangle for urban, which is discretized with a resolution 0.1 m, in front of the verifier.

We first present the position estimation error. The average error is 1.38 m and 0.79 m for case 1 and 2, and the variance is 0.79 and 0.62 respectively. For the highway case, we can confidently detect position deviations larger than 4.3 m with TPR≥ 0.99 and FPR≤ 0.01 . If we choose 3 Hz as threshold, the FPR is around 4.6%. Besides, the reflector sets does not lead to the corner cases such as Fig. 4a in both cases.

Then we use the verified position claim to verify the velocity claim. We bound the attacker's claims by realistic constraints. In vehicular networks, DSRC protocol [54] sets f_0 = 5.9 GHZ and f_a should be within from $f_0 - 37.5$ MHz to $f_0 + 37.5$ MHz. The claimed speed v should be less than the maximum speed $v_{\max}$. We define the speed deviation and heading deviation as $\delta_v = v - v_a$ and $\eta = \zeta_c - \zeta_a$, respectively. We examine the minimum FDOA deviation given every possible combination of δ_v and η by searching through all possible $f_a \in [f_0 - 37.5\,\text{MHz}, f_0 + 37.5\,\text{MHz}]$ to solve (20), where $|\delta_v| \leq 20$ m/s and $|\delta_v| \leq 10$ m/s for highway and urban case respectively due to speed limitation. The heading $|\eta| \leq 180°$ contains all possible driving directions. From Fig. 7, we can see that, no velocity deviation leads to zero $|f_{d,10}|$ and $|f_{d,20}|$ values. The red segment in color bar represents the deviation threshold $\mathcal{T}$ = 10 Hz, that can achieve a TPR>0.999 and FPR<0.001 simultaneously. In other words, the claim region which can deceive our scheme only leads to tiny amount of deviations. In summary, if there are less than 5 paths, the practical security of our proposed scheme depends on the topology and we can reduce to three paths in the cases we studied.



(a) Highway **(b) Urban**

Figure 7: FDOA deviations under optimal $\mathcal{A}$

6 EXPERIMENTAL EVALUATION

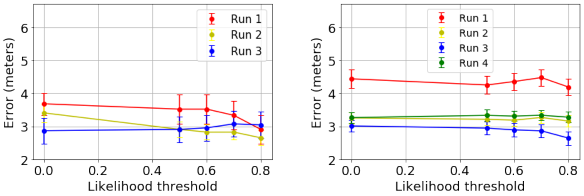
We conducted experiments in an urban street to evaluate the performance of our proposed motion verification scheme (Fig. 6a). In the first scenario, the prover is moving and the verifier is stationary at o; for the second, both the prover and verifier are moving in the same direction but with varying relative speed with an initial relative distance of 3 m and a maximum distance of 19.5 m. The experiment is conducted for multiple runs (3 and 4 runs for scenario one and two respectively) to illustrate our scheme's performance.

6.1 Experimental Setup

6.1.1 Wireless nodes setup. In the prover's vehicle, a signal transmitter, consisting of a USRP N200, constantly broadcasts a single frequency sinusoidal signal at 915 MHz using an omnidirectional antenna (VERT900) attached on the vehicle trunk. The verifier is a Kerberos SDR, which is either located on the ground (Scenario One), or on the front hood of the following vehicle (Scenario Two). The Kerberos SDR works in the frequency range of 24 MHz to 1.7 GHz. We selected a 915 MHz carrier frequency, f_0, as it is in the unlicensed ISM band and this band less congested than Wi-Fi bands[4]. Four antennas were used in a uniform circular array, with an inter-antenna distance $d = \lambda/2$ = 16.4 cm. The sampling frequency is 1.024 MHz. We divide the signal into equal length segments, each containing 32768 × 4 data points, with about 8 segments per second.

6.1.2 Ground truth and synchronization. A PCAN-USB device was used to collect the vehicle ground-truth speed via the OBD-II port at 50 Hz. A GPS-equipped smartphone running GPS2IP was used to collect ground-truth location data at 1 Hz for both vehicles. The actual heading direction is straight to the right. The true trajectory is from the location (0,2) m to (0,123) m. Data from two vehicles was synchronized by having the smartphone transmit, via a common WLAN, the same GPS coordinates to both the prover and verifier.

[4] The DSRC standard for V2V communications adopts the 5.9 GHz band. We note that the larger f_0 the better our scheme will perform as it amplifies the Doppler shift (and FDOA deviation $|f_{d,mn}|$) while maintaining the same frequency resolution error ϵ_{mn}.



(a) Scenario One **(b) Scenario Two**

Figure 8: Position estimation error for different $\mathcal{T}_l$

Computers at each (a laptop and Raspberry Pi 3, respectively) noted the time at which the messages were received; the clock offset between the two is approximately the difference in the timestamps. GPS data is processed by *pynema2* to get actual positions.

6.1.3 Environmental Description. In Fig. 6a, the prover runs straightly along the green dashed line from the left end (dot) to the right end (arrow) for both scenarios. We focus on the AOA on the right hand side of the x axis from 0° to 180°. Besides, the potential reflector set is marked via blue bars in Fig 6a, which include walls, building and stone surfaces, etc. We obtain these surfaces by first extracting them from google map and then observing it in-person to proofread it real material, location and orientation. Fortunately, most of the potential reflectors are parallel to the road. We number some of the reflectors for later illustration. The distances from Reflector 1 to 5 to the y axis are 4.1 m, 4.1 m, 4.2 m, 7.7 m and 5.8 m, respectively. The road width is about 8 meters with one lane on each direction. No other vehicles appeared during the duration of the experiment.

6.2 Results for Position

Data Processing: We adopt a 10 s and 17.5 s time horizon (80 and 140 raw data segments) for scenarios one and two respectively. Then, we apply the AOA analysis for each raw data segments and pick all data segments which have more than 2 peaks (called valid data) because our scheme needs at least two paths. We find peaks by identifying local maximums in the AOA profile. Since the number of antennas of one Kerberos SDR is limited to 4, the maximum number of signal peaks (paths) that it can resolve is 3. Our scheme can output one position estimate for each valid data segment with a likelihood. In order to filter the position estimates with a low likelihood (usually less accurate), a likelihood threshold $\mathcal{T}_l$ is used in the evaluation. We plot the GPS data and position estimates of all runs using our algorithm in Figs. 12a and 12b for both scenarios, where the latitude and longitude are converted to meters plotted as x and y coordinate respectively. We use GPS data of run 1 to approximately represent the GPS position of vehicles since the prover runs the same route every run in both scenarios respectively. We also plot the raw estimates (that are inside the plausible region).

When the prover runs beyond 30 m, the verifier can barely detect paths other than LOS because the reflection paths are too weak (more antennas will enable verification at longer ranges). Therefore, we only consider a possible search area of $8 \times 30\,\text{m}^2$ rectangle, such as $\mathcal{K}_A$ and $\mathcal{K}_B$ (i.e. a dashed rectangle) in Figs. 12a and 12b. Position estimates of valid data are plotted as square, circle, star and triangle, which represent different runs in Figs. 12a and 12b. Black points represent estimates with a likelihood larger than 0.5. Blue points denote those whose likelihood is less than 0.5. We can see higher likelihood estimates locate closer to the ground truth (red line). Most of the low likelihood estimates locate on the edge of the search area. Moreover, Fig. 12a (Scenario One) shows that a larger distance between the prover and verifier leads to a larger estimation error because it increases the impact of the signal reflection error which scales with distance. Similarly, in scenario Two (Fig. 12b), position estimates on the left are closer to the GPS compared with the right part because inter-vehicle distance at the beginning is shorter than that at the end. The average estimation error and corresponding 95% confidence interval are shown in Figs.8a and 8b. The percentage of remaining data after applying each threshold are scenario one: (62%, 29%,28%, 24%, 18%) and scenario two: (91%, 55%,51%, 41%, 27%) for $\mathcal{T}_l = (0,\ 0.5,\ 0.6,\ 0.7,\ 0.8)$ respectively. When $\mathcal{T}_l$ changes from 0 (no threshold) to 0.5, the overall average error across all runs decreases from 3.4 m to 3.04 m for scenario one and from 3.5 m to 3.31 m for scenario two. Similarly, when $\mathcal{T}_l = 0.8$, the average error reduces to 2.88 m and 3.19 m for scenario one and two respectively, which is comparable to the consumer-grade GPS systems with an accuracy of around 2 m in open sky [48]. In summary, as $\mathcal{T}_l$ increases, the estimation error decreases for most runs. Also, the error in scenario two is slightly larger than scenario one, we postulate this can be due to both vehicles' mobility.

We use point $A = (0.1\,\text{m}, 13.7\,\text{m})$ from run 2 in Fig. 12a and Point $B = (0.4\,\text{m}, 77.9\,\text{m})$ from run 2 in Fig. 12b to demonstrate the position estimation for the two scenarios. Note that the verifier was at $o = (0\,\text{m}, 0\,\text{m})$ or $C = (0.11\,\text{m}, 68.7\,\text{m})$, respectively. We plot the measured signal AOA distributions at points A and B in Figs. 11a and 11b in Appendix. Then, we use our position estimator to output the position likelihoods in the searched area $\mathcal{K}_1$ and $\mathcal{K}_2$ in Figs 10a and 10b, from which we can see that the positions with the highest likelihoods are around the true location of A and B.

6.3 Results for Velocity

We first plot the prover and verifier speed profile of both scenarios in Fig. 11e and 11f in Appendix. The FFT of the signals is plotted in Fig. 11c and 11d. In the measured FOA, the highest peak (Peak 0) represents the FOA of LOS path in Fig. 11a in Appendix. However, due to the low speeds of vehicles, the signal FOA of the two reflection paths differs in a very small amount for both scenarios. In scenario one, the actual FDOA $|f_{a,10}|$ between path 1 (right hand side path) and 0 should be 5.22 Hz, and the actual $|f_{a,20}|$ should be 4.67 Hz. We obtain the signal frequency peaks by identifying the three largest local maximums. Also, we treat the largest maximum peak as the LOS signal FOA. The actual FDOA is around 10 Hz for scenario one and 15 Hz scenario two, which is larger than actual signal FOA due to the resolution error. Then, we evaluate the verification performance using the same attack strategy formulation as in (20), where $f_0 = 915$ MHz. We evaluate three different deviation vectors (δ_v, η) by the ROC curve. They are: (1): $(\delta_v = 10, \eta = 10)$; (2): $(\delta_v = 10, \eta = 5)$ and (3): $(\delta_v = 5, \eta = 5)$, and the unit is (m/s) and (°) respectively. The results are shown in Figs. 9a and 9b in Appendix. Our scheme can only confidently detect large deviation vectors (e.g. vector 1) because of the low relative speed between vehicles. Also, a larger speed deviation is easier to detect because the surrounding environment restricts the reflection angles. The detection performance of point B is better than point A, due to a larger reflection angle and a higher relative speed at point B (2.7 m/s) than A (2.1 m/s). For example, in scenario two, when $\mathcal{T} = 9.5$ Hz, the corresponding TPR is 0.98, 0.82 and 0.29 for deviation vectors 1, 2, 3 respectively, given the error distribution in Sec.5.4.3. Selecting different $\mathcal{T}$ of 9.1 Hz, 7.3 Hz and 5 Hz for each vector can provide an equal error rate of 2.6%, 7% and 22% respectively.

Results on Timing: In our experiment, it takes 1.84 s to process one segment of data (131k data points with AOA analysis and position estimation) via Jupiter Notebook on a PC (i7-7700@3.6GHz, 128G SSD and 12G DDR4 RAM) in an offline manner for a search region of ($8 \times 30\,\mathrm{m}^2$). While we used Spider, a lower-level programming language such as C/C++ or an embedded software can improve the timing performance to make it suitable for online processing.

7 DISCUSSION

Limitations. First, our scheme requires the presence of enough number of reflectors in the environment. When the verifier is stationary, one can first do a site survey to find a suitable location for deploying the receiver to let ample reflectors surround it. Or we can deploy our own reflectors (e.g., metal boards) near the verifier. Note that, for most vehicle applications, the ground/roadway can always provide one reliable reflection path. Thus there are at least two paths (including LOS) in most cases. Neighboring vehicles can impact the performance of our algorithm either positively or negatively. We conducted similar experiments in one parking lot with sparsely parked vehicles. Results show that, for a non-crowded parking lot, signal reflected from vehicle surface is usually not that consistent and obvious compared with that from nearby buildings/walls. We hypothesize that on roads without large roadside reflectors, nearby parallel vehicles can be used as reflectors in our method. Besides, inaccurate reflector modeling, such as inaccurate reflector information from maps, unexpected pedestrians, bicycles or vehicles, can deteriorate the system performance. Although our current method heavily relies on accurate environment modeling and the experiment is still preliminary, it serves as a proof-of-concept.

For mobile verifiers, our scheme is more opportunistic since there is less control over the number of reflectors in the surrounding, thus it may not detect sporadic false claims (which is not a very effective attack). However, over a longer time span (e.g., a few seconds), as long as the path requirement is satisfied for a few time steps, it can detect persistent liers with high success probability. On-board reflectors would make virtual verifiers too close to the original verifier due to the vehicle size limit, therefore is not very helpful.

Besides, in our experiment, we have used a single-frequency source signal for simplicity. In reality when data packets are sent, the base-band signal frequency spans a range depending on the bandwidth (typically on the order of kHz or even MHz). If FFT is done directly on the received signal, obviously it becomes difficult to identify frequency shifts of each individual path since their spectrum superimpose while the DS may be as low as a few Hz. Fortunately, most wireless standards use OFDM modulation (e.g., 802.1x, DSRC), which contains hundreds of narrow-band subcarriers. Pu et. al. [29] proposed a signal processing technique that exploits this feature to do gesture recognition using WiFi, effectively reducing the bandwidth of the signal to a few Hz in each sub-band. We can also adopt this method in our scheme.

Performance enhancement. Our scheme performance can be enhanced by more reflectors or resolvable signal paths, more accurate AOA distribution measurement and smaller FOA resolution error. For AOA, the number of antennas in the receiver array should be larger than the number of multipaths. Increasing antenna number can significantly increase the accuracy and resolution of estimating AOA [51]. For the signal FOA accuracy, the Gaussian interpolation method can significantly reduce the FFT resolution error, which we have already adopted [29]. In addition, using a higher central carrier frequency can also improve the detection performance because it increases the Doppler shift and the FDOA.

Applications. The main application scenarios of this work are in vehicular networks or connected vehicles within short ranges (e.g., < 100m). Both the verifier and prover can either be stationary or mobile. For stationary verifiers, this can be applied to intelligent traffic lights that verify the claimed positions/speeds of vehicles approaching an intersection to prevent spoofing attacks against traffic control systems (where a single malicious vehicle can cause severe traffic congestion) [8]. When the verifier is mobile, this can be applied to V2V communication, where each vehicle should be able to verify nearby vehicle's motion claims from their periodically broadcast safety messages [54]. For secure tracking applications, our scheme may not achieve real-time tracking since it is opportunistic, and during periods of low reflection it may not be accurate.

We also postulate applications to UAV geo-fencing [35] with fixed ground stations, where unauthorized UAVs encroaching restricted airspace should be detected with their locations/headings verified. Typically this happens at short to medium ranges, such as a few hundred meters to kilometers. The main challenge is the longer range than ground vehicles, and the UAVs travel in 3D space and we may need more paths/reflectors for secure verification. But on the positive side, UAVs can travel in much higher relative speeds to the ground than the ones among vehicles.

8 CONCLUSION

In this paper, we propose a single receiver based secure motion claim verification scheme which utilizes the multipath signal reflections from the environment to mimic multiple virtual verifiers at different locations. Our scheme uses a maximum likelihood estimator to model potential reflections and locate the most probable signal source. Meanwhile, a FDOA-based approach is adopted to eliminate the unknown frequency offsets to verify the velocity claim. Security analysis show that at least five unique paths are needed in theory (for a single time step), and with realistic road topology it can be reduced to three. Our real-world road vehicle experiments show that, in a low relative-speed local vehicular network, our scheme can confidently detect large deviations in the motion claim, and can approximately track the vehicle within short ranges. We also discussed the applications of this work and ways to further enhance the verification performance. Future work will extend this scheme to verify and track UAVs movements in 3D.

ACKNOWLEDGEMENT

This work was partly supported by NSF grants CNS-1801402, CNS-1410000 and ARO grant W911NF-19-1-0050.

REFERENCES

[1] Giancarlo Alessandretti, Alberto Broggi, and Pietro Cerri. 2007. Vehicle and guard rail detection using radar and vision data fusion. *IEEE Transactions on Intelligent Transportation Systems* 8, 1 (2007), 95–105.

[2] Amazon. 2020. Prime Air Delivery. https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011.

[3] Harry R Anderson. 1993. A ray-tracing propagation model for digital broadcast systems in urban areas. *IEEE Transactions on Broadcasting* 39, 3 (1993), 309–317.

[4] Richard Baker and Ivan Martinovic. 2016. Secure location verification with a mobile receiver. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. 35–46.

[5] Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z Morley Mao. 2019. Adversarial sensor attack on lidar-based perception in autonomous driving. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2267–2281.

[6] Srdjan Capkun and J-P Hubaux. 2005. Secure positioning of wireless devices with application to sensor networks. In *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, Vol. 3. IEEE, 1917–1928.

[7] Srdjan Capkun and J-P Hubaux. 2006. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications* 24, 2 (2006), 221–232.

[8] Qi Alfred Chen, Yucheng Yin, Yiheng Feng, Z Morley Mao, and Henry X Liu. 2018. Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control.. In *NDSS*.

[9] Sushanta Das and Mounita Saha. 2015. Autonomous vehicle positioning system for misbehavior detection. US Patent 8,954,261.

[10] Bruce DeBruhl, Sean Weerakkody, Bruno Sinopoli, and Patrick Tague. 2015. Is your commute driving you crazy?: a study of misbehavior in vehicular platoons. In *Proceedings of the 8th ACM Wisec*. ACM, 22.

[11] Sylvie Delaët, Partha Sarathi Mandal, Mariusz A Rokicki, and Sébastien Tixeuil. 2011. Deterministic secure positioning in wireless sensor networks. *Theoretical Computer Science* 412, 35 (2011), 4471–4481.

[12] Changlai Du, Ruide Zhang, Wenjing Lou, and Y Thomas Hou. 2016. Mobtrack: Locating indoor interfering radios with a single device. In *IEEE INFOCOM 2016*. IEEE, 1–9.

[13] Song Fang, Yao Liu, Wenbo Shen, and Haojin Zhu. 2014. Where are you from? Confusing location distinction using virtual multipath camouflage. In *Proceedings of the 20th international conference on Mobile computing and networking*. 225–236.

[14] Shih-Hau Fang, Chung-Chih Chuang, and Chiapin Wang. 2012. Attack-resistant wireless localization using an inclusive disjunction model. *IEEE Transactions on Communications* 60, 5 (2012), 1209–1214.

[15] M Gasior and JL Gonzalez. 2004. Improving FFT frequency measurement resolution by parabolic and Gaussian spectrum interpolation. In *AIP Conference Proceedings*, Vol. 732. American Institute of Physics, 276–285.

[16] Nirnimesh Ghose and Loukas Lazos. 2015. Verifying ADS-B navigation information through Doppler shift measurements. In *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*. IEEE, 4A2–1.

[17] Shyamnath Gollakota and Dina Katabi. 2008. Zigzag decoding: combating hidden terminals in wireless networks. In *Proceedings of the ACM SIGCOMM 2008 conference on Data communication*. 159–170.

[18] Naveen S Gowdayyanadoddi, James T Curran, Ali Broumandan, and Gérard Lachapelle. 2015. A ray-tracing technique to characterize GPS multipath in the frequency domain. *International Journal of Navigation and Observation* 2015 (2015).

[19] Bogdan Groza and Pal-Stefan Murvay. 2018. Security solutions for the controller area network: Bringing authentication to in-vehicle networks. *ieee vehicular technology magazine* 13, 1 (2018), 40–47.

[20] Ismail Guvenc, Farshad Koohifar, Simran Singh, Mihail L Sichitiu, and David Matolak. 2018. Detection, tracking, and interdiction for amateur drones. *IEEE Communications Magazine* 56, 4 (2018), 75–81.

[21] Jun Han, Madhumitha Harishankar, Xiao Wang, Albert Jin Chung, and Patrick Tague. 2017. Convoy: Physical context verification for vehicle platoon admission. In *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*. 73–78.

[22] Loukas Lazos and Radha Poovendran. 2004. SeRLoc: Secure range-independent localization for wireless sensor networks. In *Proceedings of the 3rd ACM workshop on Wireless security*. 21–30.

[23] Bo Li, Tianlei Zhang, and Tian Xia. 2016. Vehicle detection from 3d lidar using fully convolutional network. *arXiv preprint arXiv:1608.07916* (2016).

[24] Yanmao Man, Ming Li, and Ryan Gerdes. 2020. GhostImage: Perception Domain Attacks against Vision-based Object Classification Systems. *arXiv preprint arXiv:2001.07792* (2020).

[25] David W Matolak. 2014. Modeling the vehicle-to-vehicle propagation channel: A review. *Radio Science* 49, 9 (2014), 721–736.

[26] Samuel Mitchell, Imran Sajjad, Ali Al-Hashimi, Soodeh Dadras, Ryan M Gerdes, and Rajnikant Sharma. 2017. Visual distance estimation for pure pursuit based platooning with a monocular camera. In *2017 American Control Conference (ACC)*. IEEE, 2327–2332.

[27] Nancy A Obuchowski. 2005. ROC analysis. *American Journal of Roentgenology* 184, 2 (2005), 364–372.

[28] Paolo Pivato, Luigi Palopoli, and Dario Petri. 2011. Accuracy of RSS-based centroid localization algorithms in an indoor environment. *IEEE Transactions on Instrumentation and Measurement* 60, 10 (2011), 3451–3460.

[29] Qifan Pu, Sidhant Gupta, Shyamnath Gollakota, and Shwetak Patel. 2013. Whole-home gesture recognition using wireless signals. In *Proceedings of the 19th annual international conference on Mobile computing & networking*. 27–38.

[30] SPEED RADAR. 2020. Radar Gun. https://www.radargunsales.com/product/traffic-enforcement-police-radar-guns/genesis-handheld-directional-2/.

[31] Matthias Schäfer, Vincent Lenders, and Jens Schmitt. 2015. Secure track verification. In *2015 IEEE Symposium on Security and Privacy*. IEEE, 199–213.

[32] Matthias Schäfer, Patrick Leu, Vincent Lenders, and Jens Schmitt. 2016. Secure Motion Verification Using the Doppler Effect. In *Proceedings of 9th ACM Wisec'*. ACM, USA, 135–145.

[33] Matthias Schäfer, Carolina Nogueira, Jens B Schmitt, and Vincent Lenders. 2019. Secure Location Verification: Why You Want Your Verifiers to be Mobile. In *Computer Security*. Springer, 419–437.

[34] Seong-Cheol Kim, B. J. Guarino, T. M. Willis, V. Erceg, S. J. Fortune, R. A. Valenzuela, L. W. Thomas, J. Ling, and J. D. Moore. 1999. Radio propagation measurements and prediction using three-dimensional ray tracing in urban environments at 908 MHz and 1.9 GHz. *IEEE Transactions on Vehicular Technology* 48, 3 (May 1999), 931–946. https://doi.org/10.1109/25.765022

[35] Xiufang Shi, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi, and Jiming Chen. 2018. Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Communications Magazine* 56, 4 (2018), 68–74.

[36] Steven So, Jonathan Petit, and David Starobinski. 2019. Physical layer plausibility checks for misbehavior detection in V2X networks. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 84–93.

[37] SPEEDlidar. 2020. https://store.dji.com/product/livox-horizon-lidar?vid=89181/.

[38] Mingshun Sun, Ming Li, and Ryan Gerdes. 2017. A data trust framework for vanets enabling false data detection and secure vehicle tracking. In *2017 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 1–9.

[39] Ian Tan, Wanbin Tang, Ken Laberteaux, and Ahmad Bahai. 2008. Measurement and analysis of wireless channel impairments in DSRC vehicular communications. In *2008 IEEE International Conference on Communications*. IEEE, 4882–4888.

[40] Tesla. 2020. Autopilot. https://www.tesla.com/autopilot.

[41] Michaela C Vanderveen, A-J Van der Veen, and Arogyaswami Paulraj. 1998. Estimation of multipath parameters in wireless communications. *IEEE Transactions on Signal Processing* 46, 3 (1998), 682–690.

[42] Deepak Vasisht, Swarun Kumar, and Dina Katabi. 2016. Decimeter-level localization with a single WiFi access point. In *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*. 165–178.

[43] Deepak Vasisht, Swarun Kumar, Hariharan Rahul, and Dina Katabi. 2016. Eliminating channel feedback in next-generation cellular networks. In *Proceedings of the 2016 ACM SIGCOMM Conference*. 398–411.

[44] Wantanee Viriyasitavat, Mate Boban, Hsin-Mu Tsai, and Athanasios Vasilakos. 2015. Vehicular communications: Survey and challenges of channel and propagation models. *IEEE Vehicular Technology Magazine* 10, 2 (2015), 55–66.

[45] Adnan Vora and Mikhail Nesterenko. 2006. Secure location verification using radio broadcast. *IEEE Transactions on Dependable and Secure Computing* 3, 4 (2006), 377–385.

[46] Teng Wei, Anfu Zhou, and Xinyu Zhang. 2017. Facilitating robust 60 ghz network deployment by sensing ambient reflectors. In *14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17)*. 213–226.

[47] Stefan Wender and Klaus Dietmayer. 2008. 3D vehicle detection using a laser scanner and a video camera. *IET Intelligent Transport Systems* 2, 2 (2008), 105–112.

[48] Michael G Wing et al. 2011. Consumer-grade GPS receiver measurement accuracy in varying forest conditions. *Res J For* 5, 2 (2011), 78–88.

[49] WIRED. 2015. Hackers Remotely Kill a Jeep on the Highway—With Me in It.

[50] Peter W Wolniansky, Gerard J Foschini, Glen D Golden, and Reinaldo A Valenzuela. 1998. V-BLAST: An architecture for realizing very high data rates over the rich-scattering wireless channel. In *1998 URSI international symposium on signals, systems, and electronics. Conference proceedings*. IEEE, 295–300.

[51] Xiufeng Xie, Eugene Chai, Xinyu Zhang, Karthikeyan Sundaresan, Amir Khojastepour, and Sampath Rangarajan. 2015. Hekaton: Efficient and practical large-scale MIMO. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. 304–316.

[52] Jie Xiong and Kyle Jamieson. 2013. Arraytrack: A fine-grained indoor location system. In *Presented as part of the 10th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 13)*. 71–84.

[53] Jie Xiong and Kyle Jamieson. 2013. SecureArray: Improving Wifi Security with Fine-grained Physical-layer Information. In *Mobicom*. ACM, New York, NY, USA, 441–452.

[54] Qing Xu, Tony Mak, Jeff Ko, and Raja Sengupta. 2004. Vehicle-to-vehicle safety messaging in DSRC. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 19–28.

[55] Gongjun Yan, Stephan Olariu, and Michele C Weigle. 2008. Providing VANET security through active position detection. *Computer communications* 31, 12 (2008), 2883–2897.

[56] Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou. 2017. Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 591–602.

[57] Sigen Ye, Rick S Blum, and Leonard J Cimini. 2006. Adaptive OFDM systems with imperfect channel state information. *IEEE Transactions on Wireless Communications* 5, 11 (2006), 3255–3265.

[58] Bo Yu, Cheng-Zhong Xu, and Bin Xiao. 2013. Detecting sybil attacks in VANETs. *J. Parallel and Distrib. Comput.* 73, 6 (2013), 746–756.

[59] Yong Zeng and Rui Zhang. 2017. Energy-efficient UAV communication with trajectory optimization. *IEEE Transactions on Wireless Communications* 16, 6 (2017), 3747–3760.

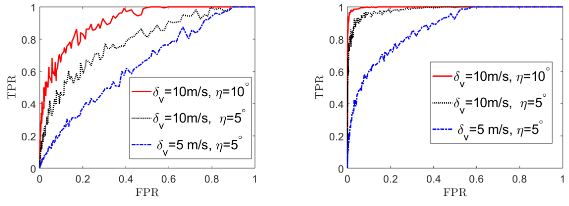
[60] Junxing Zhang, Mohammad H Firooz, Neal Patwari, and Sneha K Kasera. 2008. Advancing wireless link signatures for location distinction. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*. 26–37.

[61] Jianwei Zhao, Feifei Gao, Linling Kuang, Qihui Wu, and Weimin Jia. 2018. Channel tracking with flight control system for UAV mmWave MIMO communications. *IEEE Communications Letters* 22, 6 (2018), 1224–1227.

A APPENDIX

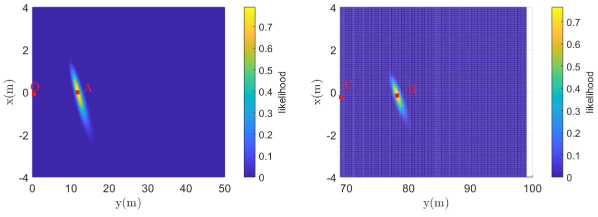
Algorithm 1: Position Claim Verification & Estimation

```
Input: $o$, $P_{\text{AoA}}(\phi)$ and all possible reflectors set $\mathcal{R}$
1: Determine the number of paths $M$ and search region $\mathcal{K}$
2: $\forall\ k \in \mathcal{K}$:
    Find most probable reflector of each path from $\mathcal{R}$ & $P_{\text{AoA}}(\phi)$
    Calculate the posterior likelihood of every path
    Combine above likelihood and get total likelihood of $k$
3: Find $k^*$ with the largest total likelihood
4: Compare $k^*$ with $p$, get distance $d = ||k^* - p||$
5: if $d \geq Q$
      Report Alarm
      Output: the estimated position $k^*$
   else
      Output: verified $p$, the inferred reflector of each path
```



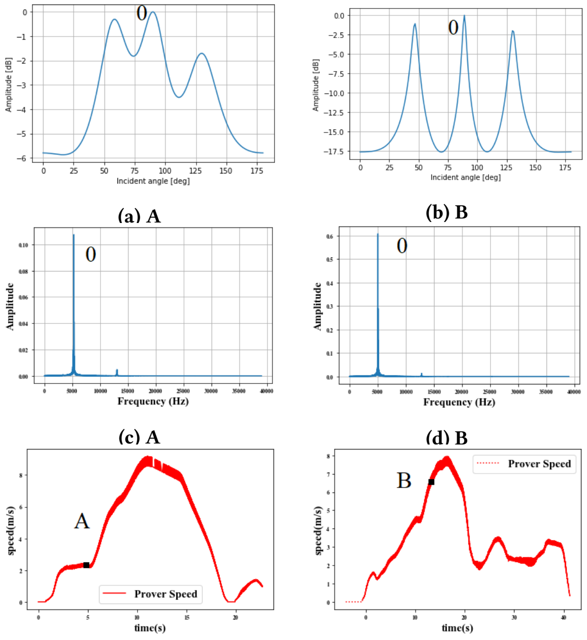
(a) Scenario One **(b) Scenario Two**

Figure 9: Velocity claim detection performance



(a) A **(b) B**

Figure 10: Position Likelihood of Possible Area

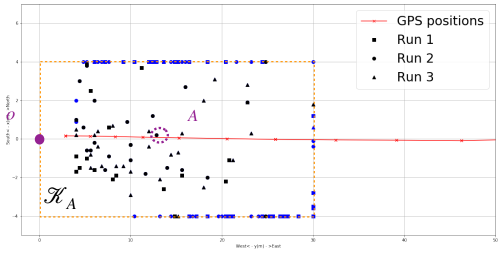


(a) A **(b) B**

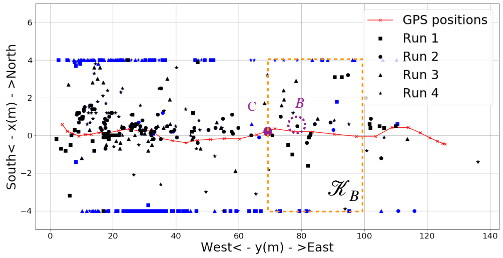
(c) A **(d) B**

(e) Scenario one **(f) Scenario two**

Figure 11: AOA (a,b), FOA (c,d) and speed (e,f) profile



(a) Scenario One



(b) Scenario Two

Figure 12: Position estimation results using all valid segments and after applying likelihood threshold $\mathcal{T}_l = 0.5$.