Detecting Location Spoofing Attacks using Multiple Angle of Signal Arrivals in MM-Wave Vehicular Networks

Chandana Sai Thondebhavi Shanthakumar
Department of Electrical & Electronic Engineering
California State University, Sacramento
California, USA
chandanasaitsthonde@csus.edu

Aishwarya Chawariya
Intel Corporation
Folsom, California, USA
aishwarya.chawariya@gmail.com

Yuan Cheng
School of Computing
Grand Valley State University
Allendale, Michigan, USA
chengy@gvsu.edu

Mohammed E. Eltayeb
Department of Electrical & Electronic Engineering
California State University, Sacramento
California, USA
mohammed.eltayeb@csus.edu

2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring) | 979-8-3503-8741-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/VTC2024-SPRING62846.2024.10683294

***Abstract*—Millimeter-wave (mm-wave) vehicular communication networks are expected to revolutionize intelligent transportation systems by enabling ultra-reliable, low-latency, and high-speed data exchange. A major challenge that needs to be addressed in these networks is the presence of malicious user activity that can disrupt the network through various means. These malicious activities include manipulating safety messages or launching location spoofing attacks. To tackle this challenge, a physical-layer-based location spoofing attack detection technique for mm-wave vehicular networks is proposed in this paper. The proposed technique makes use of the additional channel measurements available in systems with hybrid antenna architectures to enable joint beamforming and channel sensing. Spoofing attack detection is achieved by verifying a cluster of estimated angles of arrivals with the reported location information. The numerical results show that the proposed technique is highly accurate in detecting location spoofing attacks using just a few communication packets at the receiver without the need for a dedicated channel sensing stage or extra communication overhead.**

***Index Terms*—Millimeter-wave, physical-layer security, joint beamforming and sensing, spoofing, position falsification.**

I. Introduction

Millimeter-wave (mm-wave) vehicular communications are expected to enable a plethora of applications for safety, traffic efficiency, and driver assistance, and support future intelligent transportation systems (ITS) [1], [2]. The intricate interplay between connected and autonomous vehicles (CAVs), public safety, and infrastructures means that security is crucial, especially for next-generation mm-wave networks [3]. CAVs continuously exchange safety messages with other vehicles and infrastructures, including speed, GPS location, time, and other sensory data. Ensuring the accuracy and authenticity of this data is vital for the design of ITS, as attackers may attempt to falsify data during communication [4]. This type of attack, known as spoofing, has emerged as a significant threat to ITS as it can mislead other vehicles and infrastructures and cause hazardous road conditions.

Several approaches have been proposed in the literature to detect spoofing attacks in CAVs. These approaches can be broadly classified as node-centric and data-centric [5]. Node-centric approaches typically rely on the interaction between multiple entities for message authentication [6], while data-centric approaches assess the validity of received messages based on their contents [7], [8]. Although these techniques are effective, they usually rely on costly public-key cryptography, which can result in significant overhead and delayed responses, especially in real-time gigabit-per-second mm-wave environments. Furthermore, these methods do not eliminate the possibility of masquerading attacks, message replay attacks, and sybil attacks [3], [5], [9]. To address these issues, physical-layer-based security techniques that obtain independent measurements to complement existing upper-layer authentication protocols have emerged [9]–[12]. These techniques primarily monitor a wireless channel parameter, such as the received signal strength or the channel state information, to detect malicious activities such as spoofing. Nonetheless, the success of these techniques is contingent on prior channel knowledge, which is challenging to obtain in mm-wave environments and requires a significantly long coherence interval.

In this paper, we propose a physical-layer-based location spoofing attack detection technique for next-generation mm-wave vehicular networks. This technique makes use of the excess antennas on modern roadside units (RSUs) to estimate and verify a set of angle-of-arrivals (AoAs) associated with a legitimate transmitter using multiple receive communication packets. This is achieved without the need for a dedicated beam training phase as required by compressed channel esti-

mation solutions [13]. The proposed solution is different from the one presented in [9], which also adopts AoA verification for location spoofing detection. The technique proposed in [9] requires the use of a digital antenna architecture at the receiver and high receive signal-to-noise (SNR) for AoA and spoofing detection. Due to the high mm-wave channel path loss and hardware constraints, the approach presented in [9] is not suited for mm-wave systems. In this paper, we (i) develop a new framework for channel sensing with a fixed communication beam that makes use of the existing structure of mm-wave hybrid analog/digital antennas; (ii) propose a location spoofing detection technique that is tailored to next-generation vehicular mm-wave networks and low SNR regimes; and (iii) show, via simulations, that there is a trade-off between a fixed communication beamwidth and the AoA detection accuracy.

II. Attack and System Models

We consider a scenario where a vehicle (attacker) attempts to transmit false location information to a roadside unit and neighboring vehicles, as shown in Fig. 1. The attacker may also utilize one or more stolen identities to purposefully falsify their location or replay a legitimate GPS message with the intent to commit fraudulent activity or gain an advantage. All vehicles and the RSU communicate via a single data stream over a line-of-sight (LoS) mm-wave communication channel. The attacking vehicle is equipped with $N_{\mathrm{T}} > 1$ antennas, while the RSU is equipped with N antennas and $K \ll N$ RF-chains (hybrid antenna architecture). The attacker uses a precoder $\mathbf{f}$ (of size $N_{\mathrm{T}} \times 1$) to transmit an information symbols s, where $\mathbb{E}[|s|^2] = 1$, to the RSU. At the RSU, the received signals on all N antennas are combined to obtain

$$y_r = \mathbf{w}_{\mathrm{BB}}^* \mathbf{W}_{\mathrm{RF}}^* \mathbf{H} \mathbf{f} s + \mathbf{w}_{\mathrm{BB}}^* \mathbf{W}_{\mathrm{RF}}^* \mathbf{e}, \tag{1}$$

where $\mathbf{W}_{\mathrm{RF}}$ is an $N \times K$ RF combing matrix, $\mathbf{w}_{\mathrm{BB}}$ is a $K \times 1$ digital combing vector, $\mathbf{H}$ is the $N \times N_{\mathrm{T}}$ matrix that represents the mm-wave channel between the RSU and vehicle, $\mathbf{e} \sim \mathcal{CN}(0, \sigma^2)$ is the additive white Gaussian noise vector with a complex normal distribution. The optimum vector $\mathbf{w}_{\mathrm{BB}}$ and matrix $\mathbf{W}_{\mathrm{RF}}$ are selected from a predetermined codebook as outlined in Section III-A. Adopting a narrow-band geometric channel model [2], [13]–[16], the channel can be expressed as $\mathbf{H} = \mathbf{H}^{\mathrm{los}} + \mathbf{H}^{\mathrm{nlos}}$, with $\mathbf{H}^{\mathrm{los}}$ and $\mathbf{H}^{\mathrm{nlos}}$ representing the LoS and NLoS channel components. Furthermore, the channels matrices $\mathbf{H}^{\mathrm{los}}$ and $\mathbf{H}^{\mathrm{nlos}}$ can be expressed as

$$\mathbf{H}^{\mathrm{los}} = \sqrt{1/\zeta}\alpha_1 \mathbf{a}_{\mathrm{RSU}}(\theta_1)\mathbf{a}_{\mathrm{V}}^*(\phi_1) \tag{2}$$

$$\mathbf{H}^{\mathrm{nlos}} = \sqrt{1/\zeta}\sum_{\ell=2}^{L} \alpha_\ell \mathbf{a}_{\mathrm{RSU}}(\theta_\ell)\mathbf{a}_{\mathrm{V}}^*(\phi_\ell), \tag{3}$$

where ζ is the average path loss between the RSU and the transmitter and L is the total number of channel paths. The angles $\theta_\ell \in [0, 2\pi]$ and $\phi_\ell \in [0, 2\pi]$ represent the ℓth path's azimuth angles of departure or arrival (AoD/AoA) of the communicating vehicle and the RSU respectively, and α_ℓ is the ℓth path gain. The vector $\mathbf{a}_{\mathrm{V}}(\phi)$ represents the vehicle's array response while the vector $\mathbf{a}_{\mathrm{RSU}}(\theta)$ represents the RSU's array response [13]. While the proposed techniques can be generalized to arbitrary antenna architectures, for ease of exposition, the fully-connected hybrid architecture with uniform linear arrays (ULAs) and LoS point-to-point channels will be assumed throughout this paper. The impact of multi-path will be examined in Section IV.

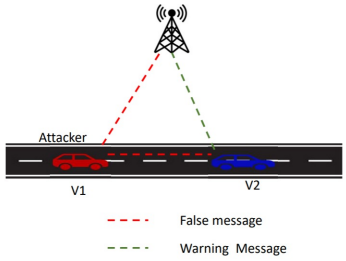

Fig. 1. An illustration of the proposed spoofing detection technique showing V1 transmitting a message to V2 with spoofed GPS location. The RSU estimates a series of AoAs using the V1 signal and compares them with the reported location. The RSU declares a spoofing attack and sends out a warning to V2.

III. Joint Beamforming and Malicious User Detection

In this section, we first demonstrate how hybrid communication beams can be utilized for AoA estimation (or channel sensing) and then formulate the spoofing detection problem.

A. Leveraging Hybrid Analog/Digital Codebooks for Sensing

To create near-ideal communication beams, hybrid antenna architectures divide the combining (or precoding) stage between the analog RF and digital baseband domains [13]-[17]. This is achieved by the use of hybrid codebooks that approximate unconstrained digital beams by selecting a combination of low-resolution analog steering vectors and digitally combining them at baseband as follows [13]

$$\begin{aligned} &(\mathbf{W}_{\mathrm{RF}}^{\mathrm{opt}}, \mathbf{w}_{\mathrm{BB}}^{\mathrm{opt}}) = \arg\min \|\mathbf{W}_{\mathrm{opt}}^{\star} - \mathbf{W}_{\mathrm{RF}}\mathbf{w}_{\mathrm{BB}}\|_F, \\ &\text{s.t.} \quad [\mathbf{W}_{\mathrm{RF}}]_{:,i} \in [\mathbf{A}_{\mathrm{can}}]_{:,\ell} | 1 \le \ell \le N_{\mathrm{can}}, i = 1, ..., K \\ &\quad \|\mathbf{W}_{\mathrm{RF}}\mathbf{w}_{\mathrm{BB}}\|_F^2 = 1, \end{aligned} \tag{4}$$

where $\mathbf{W}_{\mathrm{RF}}$ is the $N \times K$ the constrained analog RF combining matrix, $\mathbf{w}_{\mathrm{BB}}$ is the $K \times 1$ baseband digital combing matrix, and $\mathbf{W}_{\mathrm{RF}}^{\mathrm{opt}}$ and $\mathbf{w}_{\mathrm{BB}}^{\mathrm{opt}}$ are the optimum hybrid combiners. The matrix $\mathbf{W}_{\mathrm{opt}}^{\star}$ is a digital unconstrained combiner, $\mathbf{A}_{\mathrm{can}}$ represents an $N \times N_{\mathrm{can}}$ matrix that carries a finite set of quantized analog steering vectors, and N_{can} is the number of possible steering vectors due to the quantized phase-shifters. Consequently, the hybrid combining vector becomes

$$\mathbf{w}_{\mathrm{H}} = \mathbf{W}_{\mathrm{RF}}^{\mathrm{opt}} \mathbf{w}_{\mathrm{BB}}^{\mathrm{opt}}. \tag{5}$$

In this paper, we utilize the received signal at each RF chain (using $\mathbf{W}_{\mathrm{RF}}^{\mathrm{opt}}$), prior to digital processing, for channel sensing. In Fig. 2, an example is demonstrated where the hybrid beamforming vector $\mathbf{w}_{\mathrm{H}}$ is fixed, and the resulting

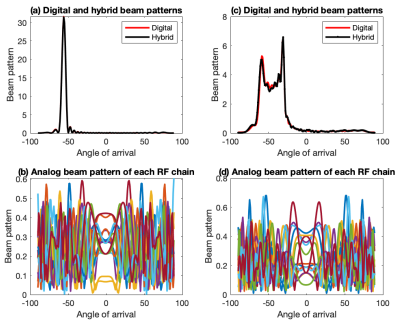

Fig. 2. Comparison of the resulting hybrid, digital, and analog beam patterns for a ULA with 32 antennas, 14 RF chains, and 2-bit phase-shifters at AoAs -55^o (sub-figures a and b) and -30^o to -60^o (sub-figures c and d). Systems with hybrid antenna architectures can utilize unprocessed analog beamforming for channel sensing.

beam pattern of the analog unprocessed beams is shown when the communication beam is fixed and steered towards -55^o (subfigures a-b), and the AoA range -30^o to -60^o (subfigures c-d). For both sector sizes, we observe that each analog unprocessed beam (when using beam steering vectors from $\mathbf{W}_{\text{RF}}^{\text{opt}}$) yields a unique beam pattern in the angular domain. Given $K = 14$ RF chains, we obtain 14 unique beam patterns which we exploit for sensing in this paper. This randomized beam pattern is achieved without the need for antenna switching as done in [18], [19], and hence can be readily exploited for PHY-layer assisted authentication in existing systems with hybrid antenna architectures.

B. Reliable Detection of Location Spoofing and Attacks using Consecutive Communication Packets

For location spoofing and attack detection, we estimate the AoA of the transmitting vehicle at the RSU using the analog unprocessed channel measurements each RF chain provides when receiving communication packets. Each received communication packet is assumed to consist of a channel estimation (gain) and synchronization preamble block, a header, communication data blocks (beacon safety message), and optional beam training fields [19]. Unlike conventional mm-wave channel estimation techniques that utilize the beam training field for AoA estimation, we reuse the channel estimation preamble block for AoA estimation under a fixed hybrid communication beam. Before we introduce the proposed attack detection technique, we first lay the following assumptions: (i) all GPS location data is accurate and is received error-free, and (ii) each communication packet is received at the RSU from an independent AoA.

1) Formulation of the AoA estimation problem: After decoding the mth communication packet using a fixed hybrid combining vector $\mathbf{w}_{\text{H}}$, the output of the analog stage prior to digital combining can be written as

$$\mathbf{y}_m = (\mathbf{W}_{\text{RF}}^{\text{opt}})^* \mathbf{h}_m + (\mathbf{W}_{\text{RF}}^{\text{opt}})^* \mathbf{e}_m, \tag{6}$$

where $\mathbf{y}_m \in \mathcal{C}^{K\times 1}$, $m = 1, 2, ..., M$ is the received packet index, the channel $\mathbf{h}_m = \mathbf{H}_m \mathbf{f}_m c$ is dependent on the transmitting vehicle's location at the mth time instant, and c is a known preamble symbol for channel estimation and synchronization (not for beam training). Assuming all AoAs are quantized and taken from a uniform grid of N points, and neglecting discretization errors, (6) can be written as follows [16]

$$\mathbf{y}_m = \underbrace{(\mathbf{W}_{\text{RF}}^{\text{opt}})^* \mathbf{A}}_{\mathbf{Q}} \underbrace{\mathbf{x}_m}_{m\text{th AoA}} + \underbrace{(\mathbf{W}_{\text{RF}}^{\text{opt}})^* \mathbf{e}_m}_{\text{noise}}, \tag{7}$$

where $\mathbf{A}$ is the $N \times N$ dictionary matrix that consists of RSU's antenna array response vector corresponding to each quantized AoA θ_q taken from the uniform grid. The matrix $\mathbf{Q}$ is a $K \times N$ channel sensing matrix and $\mathbf{x}_m \in \mathcal{C}^{N\times 1}$ is a time-varying sparse AoA vector with the nth non-zero entry representing the product of the training symbol c and the complex channel gain corresponding to the nth quantized AoA at the mth time instant. Intuitively, one may apply sparse signal recovery algorithms, see example [20], [21], to recover the entries of $\mathbf{x}_1$, i.e. using only one received communication packet, without the need for additional measurements by solving the following optimization problem: $\min_{\mathbf{x}_1} \|\mathbf{x}_1\|_0 \;\; \text{s.t.} \;\; \|\mathbf{y}_1 - \mathbf{Q}\mathbf{x}_1\|_2 \leq \xi$. Nonetheless, as we will show in the next section, this requires high receive SNR and the use of a large number of RF chains at the RSU, both of which may not be practical in mm-wave vehicular networks. In this paper, we propose the accumulation of M communication packets for AoA recovery instead.

2) Sensing matrix design: When M communication packets are received, we vertically stack the received measurement vectors $\mathbf{y}_m$ to obtain

$$\mathbf{y} = [\mathbf{y}_1^T \quad \mathbf{y}_2^T \quad \dots \quad \mathbf{y}_M^T]^T = \Big(\mathbf{I}_M \otimes \mathbf{Q}\Big)\mathbf{x} + \mathbf{e}, \tag{8}$$

where $\mathbf{I}_M$ is the identity matrix, $(.)^T$ is the transpose operator, $\otimes$ is the Kronecker product operator, $\mathbf{x} = [\mathbf{x}_1^T \quad \mathbf{x}_2^T \quad \dots \quad \mathbf{x}_M^T]^T$ is the received vector that consists of M sparse channel gains, and $\mathbf{e} = [((\mathbf{W}_{\text{RF}}^{\text{opt}})^* \mathbf{e}_1)^T \quad \dots \quad ((\mathbf{W}_{\text{RF}}^{\text{opt}})^* \mathbf{e}_M)^T]^T$, is the stacked noise vector. Given that the number of measurements in (8) has increased by M, using sparse recovery to detect the AoAs is still inefficient since the channel sparsity increased by at least that factor as well.

One way to optimize AoA recovery is to make use of the following prior information: (i) the vectors $\mathbf{x}_m$ have the same number of non-zero entries as the AoAs of the received communication packets are consecutive along the direction of travel, and (ii) a vehicle can not be at the same location at different time instances, e.g., having the third entry in $\mathbf{x}_1$ and $\mathbf{x}_2$ to be non-zero is not possible since the LoS AoA is changing with every received packet. Using this information, we reformulate the sparse detection problem by grouping M consecutive AoAs and eliminating outcomes that are not expected to occur. This reformulation has two immediate benefits. First, it reduces the dimension of the block diagonal matrix in (8). Second, it improves the received SNR by accumulating measurements over time.

To permit AoA group selection, we group all the indices of the N quantized AoAs into subsets such that the difference

between the elements within each subset is at most $M-1$. This ensures that the AoAs within each group are consecutive, e.g., if $N=6$ and $M=4$, the resulting subsets are $\{1,2,3,4\},\{2,3,4,5\},\{3,4,5,6\}$. Based on this arrangement, the number of subsets becomes $N-M+1$. Following that, we need to rearrange the columns of the sensing matrix $\mathbf{Q}$ to enable group detection. To achieve this, let the matrix $\tilde{\mathbf{Q}}^{(i,j)}$, of size $K \times (N-M+1)$, represent the matrix $\mathbf{Q}$ that is circularly shifted column-wise to the left by i and the last $j=(M-1)$ columns are pruned. Similarly, let the vector $\tilde{\mathbf{x}}_m^{(i,j)}$, of size $(N-M+1)\times 1$, represent vector $\mathbf{x}$ circularly shifted upwards by i and the last $j=(M-1)$ elements removed. We can then rewrite $\mathbf{y}_m$ in (7) as

$$\mathbf{y}_m = \tilde{\mathbf{Q}}^{(m-1,M-1)}\tilde{\mathbf{x}}_m^{(m-1,M-1)} + (\mathbf{W}_{\text{RF}}^{\text{opt}})^*\mathbf{e}_m. \tag{9}$$

Observe in (9) the vectors $\tilde{\mathbf{x}}_m^{(m-1,M-1)}$ (corresponding to the LoS AoAs) share common sparse support for all values of m. This results due to the circular shift and pruning applied to the vectors $\mathbf{x}_m$ and the sensing matrix $\mathbf{Q}$ which forces the non-zero entries of $\mathbf{x}_m, \forall m$ to have a common index. Define the vector $\mathbf{z} = \sum_{m=1}^{M} = \tilde{\mathbf{x}}_m^{(m-1,M-1)}\alpha_{1,m}^{-1}$, where $\alpha_{1,m}^{-1}$ is the inverse channel gain of the mth LoS AoA, be an $(N-M+1)\times 1$ sparse vector with the non-zero entries representing the index of the active AoA group. Then the group detection problem can be reformulated by rewriting (8) as

$$\underbrace{\begin{bmatrix}\tilde{\mathbf{y}}_1\\ \tilde{\mathbf{y}}_2\\ \vdots\\ \tilde{\mathbf{y}}_M\end{bmatrix}}_{\tilde{\mathbf{y}}} = \underbrace{\begin{bmatrix}\tilde{\mathbf{Q}}^{(0,M-1)}\\ \tilde{\mathbf{Q}}^{(1,M-1)}\\ \vdots\\ \tilde{\mathbf{Q}}^{(M-1,M-1)}\end{bmatrix}}_{\mathbf{\Phi}\in\mathcal{C}^{MK\times(N-M+1)}}\mathbf{z} + \underbrace{\begin{bmatrix}(\mathbf{W}_{\text{RF}}^{\text{opt}})^*\tilde{\mathbf{e}}_1\\ (\mathbf{W}_{\text{RF}}^{\text{opt}})^*\tilde{\mathbf{e}}_2\\ \vdots\\ (\mathbf{W}_{\text{RF}}^{\text{opt}})^*\tilde{\mathbf{e}}_M\end{bmatrix}}_{\tilde{\mathbf{e}}}, \tag{10}$$

where $\tilde{\mathbf{y}}_m$ and $\tilde{\mathbf{e}}_m$ are the vectors $\mathbf{y}_m$ and $\mathbf{e}_m$ normalized by the mth AoA channel gain, and the matrix $\mathbf{\Phi}$ is the equivalent sensing matrix. When $M=1$, (10) reduces to the classical sparse AoA recovery problem in (7).

3) AoA group recovery: Given $\tilde{\mathbf{y}}$ and $\mathbf{\Phi}$, the sparse vector $\mathbf{z}$ can be easily recovered using sparse recovery algorithms such as the orthogonal matching pursuit as outlined in [20]. Since we are only interested in recovering a single AoA group, we apply the maximum correlation for simplicity, and the recovered group index is obtained as follows [20]

$$g^\star = \arg\max_{g=1,2,\ldots,G} |\mathbf{y}^*\mathbf{\Phi}_{:,g}|,$$

where $G = N-M+1$ is the number of AoA groups along the direction of travel.

4) Attack detection: Once the AoA group of the communicating vehicle $g^\star$ is estimated, the RSU compares the declared AoA group index g_{D} (location obtained via communication) and compares it with the estimated group index $g^\star$. A spoof attack is declared if $|g^\star - g_{\text{D}}| > \epsilon$, where ϵ is a small threshold.

C. Performance Analysis

We assess the performance of the proposed spoofing detection technique using the probability of correct detection, P_{D}, and the probability of false alarm P_{F} metrics. The probability of correct detection, P_{D} is defined as the probability of accepting communication packets corresponding to transmission originating from a legitimate transmitter. The probability of false alarm P_{F} is defined as the probability of accepting communication packets originating from an illegitimate transmitter. Let $\mathcal{H}_0$ represent the event that a legitimate vehicle is communicating from the declared AoA location, and $\mathcal{H}_1$ represent the event that a malicious vehicle is communicating from a location that does not correspond to its declared AoA location. Based on this, we express the probability of correct detection and the probability of false alarm as $P_{\text{D}} = P(|g^\star - g_{\text{D}}| < \epsilon|\mathcal{H}_0)$, and $P_{\text{F}} = P(|g^\star - g_{\text{D}}| < \epsilon|\mathcal{H}_1)$.

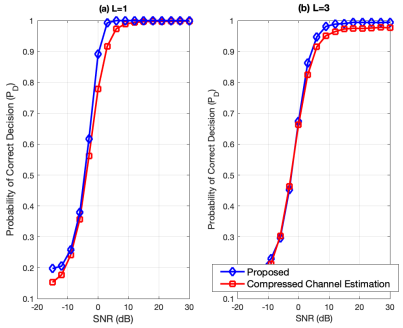

Fig. 3. P_{D} versus the SNR per antenna for $L=1$ and $L=3$ channel paths; $\theta_{\text{T}} = -55^o$, $K=14$, $\epsilon = 0.12$, and the receive communication beam sector size is $30^o(-30^o$ to $-59^o)$. P_{D} increases with higher receive SNR ρ.

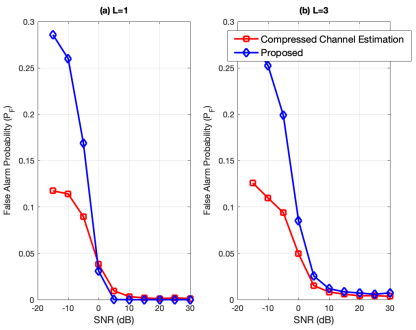

Fig. 4. P_{F} versus the SNR per antenna for $L=1$ and $L=3$ channel paths; $\theta_{\text{T}} = -55^o$, $\theta_{\text{R}} = -25^o$, $K=14$, $\epsilon = 0.12$, and the communication beam sector size is $30^o(-30^o$ to $-59^o)$. P_{F} decreases with higher receive SNR ρ.

IV. Numerical Results

In this section, we perform numerical simulations to evaluate the performance of the proposed location spoofing attack detection technique. We assume that at any moment, the RSU receives error-free and accurate GPS location reporting from the transmitting vehicle and the vehicle direction of travel is from -90^o to 90^o with respect to the RSU. Unless otherwise specified, the RSU is equipped with $N=32$ antennas each with 2-bit phase shifters, the average receive SNR per antenna is $\rho = \frac{\sum_l \alpha_l^2}{\zeta\sigma^2}$, and the decision threshold is $\epsilon = 0.5$. Using the hybrid combining vector in (5), the

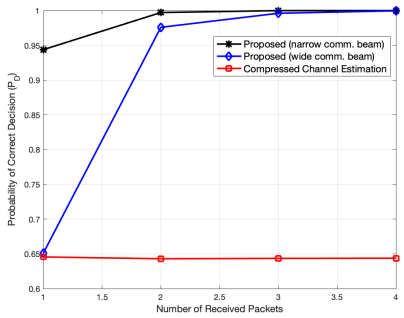

Fig. 5. $P_{\rm D}$ versus the number of received packets M. $\rho = 0$ dB, $L = 3$, $\theta_{\rm T} \in \{-43.4^o, -38.7^o, -34.2^o, -30^o\}$, and $K = 14$. $P_{\rm D}$ increases with the number of received packets and narrower communication beams.

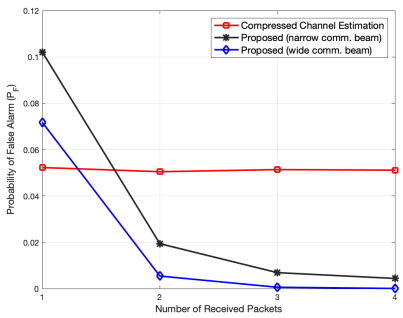

Fig. 6. $P_{\rm F}$ versus the number of received packets M. $\rho = 0$ dB, $L = 3$, $\theta_{\rm T} \in \{-43.4^o, -38.7^o, -34.2^o, -30^o\}$, $\theta_{\rm R} \in \{0^o$ - $90^o\}$, and $K = 14$, $P_{\rm F}$ decreases with the number of packets and wider communication beams.

receive communication beam is fixed and steered towards the AoA range -30^o to -59^o (defined as a wide communication beam) or towards the AoA range -30^o to -44^o (defined as a narrow communication beam). The matrix $\mathbf{A}$ in (7) is composed of steering vectors corresponding to 32 quantized AoAs (-90^o to 90^o) and the entries of the matrix $\mathbf{A}_{\rm can}$ in (4) are selected from the set $\{\pm 1, \pm j\}$. The performance of the proposed technique is evaluated considering $L = 1$ and $L = 3$ channel paths. For $L = 3$, the gain of the LoS path is set to $\alpha_1^2/\zeta = 0.7$, and AoAs of the NLoS paths are randomly selected from the set $\{-90^o, 90^o\}$ with $\alpha_\ell^2/\zeta = 0.15$. To provide some context, we also plot the performance of the AoA-based authentication technique proposed in [9] using mm-wave system-suitable compressed channel estimation techniques as outlined in [13]. It is important to note that compressed channel estimation requires a dedicated beam training phase for AoA estimation, whereas the proposed technique utilizes the existing communication beam for AoA estimation.

In Figs. 3 and 4, we analyze the performance of the proposed spoofing detection technique in terms of the probability of correct decision and false alarm probability for a legitimate vehicle located at the non-quantized AoA $\theta_{\rm T} = -55^o$. We set the number of RF-chains to 14 and use $M = 1$ communication packet for AoA estimation. For both $L = 1$ and $L = 3$ cases, Fig. 3 shows that the probability of correct decision increases with the received SNR. It also shows that the probability of a correct decision is comparable to that achieved by the AoA-based authentication technique proposed in [9] (red plot) when using compressed-sensing-based channel estimation that requires the use of random beams for channel sensing. The proposed technique can achieve similar performance by utilizing the excess channel measurements (analog) available at the receiver, prior to digital combing, to successfully detect attacks without requiring a dedicated channel estimation phase.

To assess the false alarm probability, we consider a malicious vehicle located at AoA $\theta_{\rm R} = -25^o$ claiming to be located at AoA $\theta_{\rm T} = -55^o$. For both $L = 1$ and $L = 3$ paths, Fig. 4 shows that in the high SNR case, both spoofing detection techniques exhibit similar false alarm rates. However, at low SNR, the false alarm probability of the proposed technique is higher. Furthermore, Figs. 3 and 4 indicate successful spoofing detection at high SNR only, with both methods failing at low SNR in spite of the high number of RF chains.

In Figs. 5 and 6, we evaluate the performance of the proposed technique in the low SNR regime when using multiple received communication packets. When using a wide communication beam, Fig. 5 shows that the probability of correct decision approaches 1 with just three communication packets while the performance of the AoA-based authentication technique using compressed channel estimation remains constant. The reason for this is that the proposed formulation permits the receiver to accumulate time varying measurements for detecting an AoA cluster. Compressed channel estimation-based techniques fail here since the AoA changes at each location and hence, measurements can not be readily accumulated for AoA estimation. To gain some insights into the influence of the receiver's communication beam width on the detection performance, we also plot the probability of correct decision when using a fixed narrow hybrid communication beam for detection. The figure shows that narrow communication beams improve the probability of correct decision $P_{\rm D}$ when compared to wider beams. This improvement is due to the inherit design of the analog antenna weights that contain entries that are correlated with the legitimate vehicle's communication channel. This correlation results in higher detection probability at the cost of a slight increase in false alarm probability as shown in Fig. 6, where we considered a malicious vehicle located at AoAs randomly selected from the set $\theta_{\rm R} \in \{0^o, 90^o\}$ with 3.6^o angle separation claiming to at AoAs $\theta_{\rm T} = -43.4^o, -38.7^o, -34.2^o, -30^o$.

Finally, in Figs. 7 and 8, we evaluate the performance of the proposed spoofing detection technique using $K = 6$ RF-chains and in low SNR regime. The results show that, for a limited number of RF-chains and low SNR, the proposed spoofing detection technique yields correct detection of the legitimate vehicle with a diminishing false alarm probability using just a few number of received packets. However, in Fig. 8, we observe a slightly higher false alarm probability for the narrow communication beam case. This is mainly due to the dependency of the detection matrix $\tilde{\mathbf{Q}}$ on the choice of

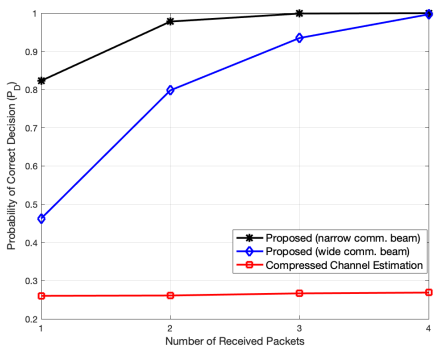

Fig. 7. P_{D} versus M when utilizing a wide communication beam. $\rho = 0$ dB, $K = 6$, $L = 3$, $\theta_{\mathrm{T}} \in \{133.4^o, 128.6^o, 124.2^o, 120^o\}$, and $\theta_{\mathrm{R}} \in \{0^o - 90^o\}$.

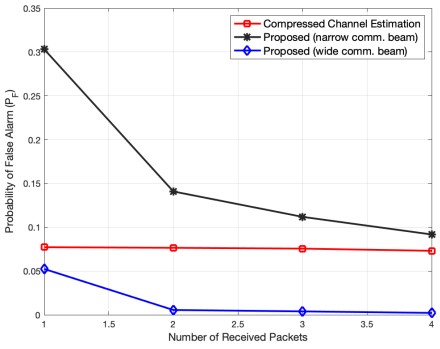

Fig. 8. P_{F} versus M when utilizing a wide communication beam. $\rho = 0$ dB, $K = 6$, $L = 3$, $\theta_{\mathrm{T}} \in \{133.4^o, 128.6^o, 124.2^o, 120^o\}$, and $\theta_{\mathrm{R}} \in \{0^o - 90^o\}$.

the selected analog steering vectors from $\mathbf{A}_{\text{can}}$ in (4), which are correlated to the communication beam by design. These steering vectors produce correlated beam patterns and result in a detection performance hit. Therefore, there is a trade-off between the communication beam width and the probability of malicious vehicle detection.

V. Conclusion

In this paper, we presented a novel technique for detecting location spoofing in mm-wave vehicular networks. By leveraging mm-wave hybrid analog/digital antenna architectures, we demonstrated that the received analog RF signals, prior to digital combining, can be utilized for joint communication and sensing. The proposed technique estimates a cluster of AoAs from a few messages using a fixed communication beam. Spoofing detection is achieved by comparing the estimated AoA cluster with the reported AoAs. The numerical results confirmed the efficacy of our technique, showing that it can detect spoofing attacks with high accuracy using just a few communication packets.

Acknowledgment

This material is based upon work supported in part by Sacramento State Research and Creative Activity Faculty Awards Program and by the National Science Foundation under grant No. NSF-ECCS-2243089.

References

[1] M. Ahmed et al., "Vehicular communication Network Enabled CAV Data Offloading: A Review," in *IEEE Trans. Intell. Transp. Syst.,* vol. 24, no. 8, pp. 7869-7897, Aug. 2023.

[2] J. Choi, N. G.-Prelcic, R. Daniels, C. Bhat, and R. Heath, "Millimeter Wave Vehicular Communication to Support Massive Automotive Sensing," *IEEE Commun. Mag.,* vol. 54, no. 12, pp. 160-167, Dec. 2016.

[3] D. Hahn, A. Munir and V. Behzadan, "Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges," in *IEEE Intell. Transp. Syst. Mag.,* vol. 13, no. 1, pp. 181-196, Spring 2021.

[4] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A Survey on the Current Security Landscape of Intelligent Transportation Systems," in *IEEE Access,* vol. 9, pp. 9180-9208, 2021.

[5] R. Heijden, S. Dietzel, T. Leinmüller and F. Kargl, "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems," in *IEEE Commun. Surv. Tutor.,* vol. 21, no. 1, pp. 779-811, 2019.

[6] S. Ly, and Y. Cheng. "A Data-based Protocol for One-way Trust in Inter-vehicular Communication," in *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems,* pp. 69-74. 2021.

[7] C. Kim, SY. Chang, D. Lee, J. Kim, K. Park, and J. Kim, "Reliable Detection of Location Spoofing and Variation Attacks," in *IEEE Access* 11, pp.10813-10825, 2023 Jan 31.

[8] A. Sharma and A. Jaekel, "Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach," in *IEEE Open J. Veh. Technol.,* vol. 3, pp. 1-14, 2022.

[9] A. Abdelaziz, R. Burton, F. Barickman, J. Martin, J. Weston and C. E. Koksal, "Enhanced Authentication Based on Angle of Signal Arrivals," in *IEEE Trans. Veh. Technol.,* vol. 68, no. 5, pp. 4602-4614, May 2019.

[10] W. Li, N. Wang, L. Jiao and K. Zeng, "Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks," in *IEEE Access,* vol. 9, pp. 60419-60432, 2021.

[11] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, "Practical User Authentication Leveraging Channel State Information (CSI)," in *Proc. ACM Symp. Inf., Comput. Commun. Security,* 2014, pp. 389 400.

[12] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Commun.,* vol. 17, no. 5, pp. 56–62, Oct. 2010.

[13] A. Alkhateeb, O. El Ayach, G. Leus and R. W. Heath, "Channel Estimation and Hybrid Precoding for Millimeter Wave Cellular systems," in *IEEE J. Sel. Topics Signal Process,* vol. 8, pp. 831-846, Oct. 2014.

[14] M. Akdeniz, Y. Liu, M. Samimi, S. Sun, S. Rangan, T. Rappaport, and E. Erkip, "Millimeter Wave Channel Modeling and Cellular Capacity Evaluation," *IEEE J. on Selected Areas in Commun.,* vol. 32, no. 6, pp. 1164-1179, June 2014.

[15] V. Va, J. Choi and R. W. Heath, "The Impact of Beamwidth on Temporal Channel Variation in Vehicular Channels and Its Implications," in *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5014-5029, June 2017.

[16] R. W. Heath, N. Gonzalez-Prelcic, S. Rangan, W. Roh, and A. M. Sayeed, "An Overview of Signal Processing Techniques for Millimeter Wave MIMO Systems," *IEEE J. Sel. Topics Signal Process.,* vol. 10, no. 3, pp. 436–453, 2016.

[17] M. E. Eltayeb, A. Alkhateeb, R. W. Heath and T. Y. Al-Naffouri, "Opportunistic Beam Training with Hybrid Analog/Digital Codebooks for mmWave Systems," *in the 2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP),* 2015, pp. 315-319.

[18] N. Valliappan, A. Lozano and R. W. Heath, "Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication," in *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231-3245, August 2013.

[19] P. Kumari, M. E. Eltayeb and R. W. Heath, "Sparsity-Aware Adaptive Beamforming Design for IEEE 802.11ad-Based Joint Communication-Radar," in *2018 IEEE Radar Conference,* Oklahoma City, OK, USA, 2018, pp. 0923-0928.

[20] A. K. Fletcher, S. Rangan, and V. K. Goyal, "Necessary and Sufficient Conditions for Sparsity Pattern Recovery," in *IEEE Trans. Inf. Theory* vol. 55, no. 12, pp. 5758–5772, Dec 2009.

[21] M. E. Eltayeb, T. Y. Al-Naffouri and H. R. Bahrami, "Compressive sensing for feedback reduction in MIMO broadcast channels, " in *IEEE Trans. Commun.,* vol. 62, no. 9, pp. 3209-3222, Sept. 2014.