# Poster: Position Verification in Vehicular Platoons Using a Euclidean Distance Matrix

Tasnuva Tithi, Ryan Gerdes, Chris Winstead
Department of ECE, Utah State University
Logan, UT 84322-4120
tasnuvatithi@aggiemail.usu.edu, ryan.gerdes@usu.edu, chris.winstead@usu.edu

***Abstract*—This work presents a novel method for detecting false position claims in vehicle platoons based on the Euclidean Distance Matrix (EDM). Analytical and simulation results show that the EDM analysis is resistant to terrorist-fraud attacks and can identify an attacker in 100% cases if aided by a single colluder and 83.33% cases if aided by two colluders.**

## I. Introduction

In a vehicle platoon a group of vehicles act as single unit through coordination of movements. Platooning is expected to increase safety, roadway capacity, and efficiency. Accurate and timely vehicle position information, however, is critical in platooning operations [1]; in addition, inaccurate or unavailable position information can be leveraged by malicious individuals to decrease efficiency [2] or cause accidents [3], [4].

Existing secure localization approaches [5]–[7] are vulnerable to attack in the presence of multiple, colluding attackers. This work presents a method based on Euclidean Distance Matrix (EDM) analysis to detect two distance attacks. The method relies on only self-localization (e.g. through GPS) and adjacent neighbor distance measurements (e.g. using radar). Under the assumption that these measurements are reliable, EDM analysis is able to discover attackers in the majority of cases for the attack types considered.

## II. Assumptions and Attack model

Let us consider a platoon consisting of $n$ vehicles ideally spaced at a distance of $d^*$ from each other. We assume that vehicles move in a straight line and only the $x$ coordinates of their positions are relevant. Each vehicle is able to localize itself and measures the distances to its adjacent neighbors via local sensors. Vehicles are required to broadcast their sensor measurements along with their position. The vehicle in the front of the platoon, the *leader* $v_L$, is in charge of detecting false position claims and identifying the attacker. We assume that the leader is honest and all measurements are noise free.

We denote the vehicle in the $i^{\text{th}}$ position as $v_i$. The true position of $v_i$ is $p_i$, and the reported position is $y_i$. The sensor measurement of $v_i$ to adjacent neighbor $v_j$ is denoted by $s_{ij}$, where $j = i \pm 1$. In general, the physical distance between $v_i$ and $v_j$ is denoted by $d_{ij}$. If $v_i$ and $v_j$ are adjacent neighbors, we expect $d_{ij} = s_{ij} = s_{ji} = d_{ji}$. We assume that all vehicles report true position and sensor measurements, except those which are attackers or colluders. In this work, any vehicle that reports a false position and false sensor measurements is considered an attacker, and any vehicle that reports a true position but false sensor measurements to support the attacker is considered a colluder.

### A. Attack type I

We first consider an attack executed by an attacker with a single colluder (Fig. 1a). Let an attacker $v_a$ deviate by an amount $\delta$ from its reported position $y_a$. One of the adjacent vehicles to $v_a$ is the colluder $v_c$, and the other adjacent vehicle is referred to as the target vehicle $v_t$. To cover the deviation, the attacker falsifies the sensor measurements such that

$$s_{at} = |y_a - y_t| = d^* \tag{1}$$

Colluder $v_c$ supports $v_a$ by tampering with $s_{ca}$ such that $s_{ca} = |y_c - y_a| = d^* = s_{ac}$. The target $v_t$ reports the true sensor measurement,

$$s_{ta} = |p_t - p_a| = |y_t - y_a| - \delta = d^* - \delta \tag{2}$$

where $\delta$ is positive if $v_a$ is moving toward $v_t$. All reports from $v_c$ except for $s_{ca}$ are truthful.

### B. Attack type II

In this attack it is assumed that $v_a$ is supported by two colluders $v_{c1}$ and $v_{c2}$ as illustrated in (Fig. 1b). The purpose of this attack is to frame $v_t$ as an attacker.

Case (*i*): $v_a$ moving closer to $v_t$. To execute this attack, $v_a$ deviates $\delta$ from reported position $y_a$ to move towards $v_t$ as shown in (Fig. 1 b). The deviation $\delta$ is positive if $v_a$ is behind $v_t$; $\delta$ is negative otherwise. Unlike attack type I, in this attack, $v_a$ reports the true distance to $v_t$ as $s_{at} = |p_a - p_t| = |y_a - y_t| - |\delta|$ to indicate it is $v_t$ which has deviated by $\delta$ from $y_t$ and came closer to $v_a$.

Colluder $v_{c1}$ supports $v_a$ by tampering with its sensor measurement to $v_a$ such that $s_{c1a} = s_{ac1} = |y_a - y_{c1}|$. Colluder $v_{c2}$ supports $v_a$ by tampering with its sensor measurement to $v_t$ such that $d_{c2a} = d_{ac2} = s_{c2t} + s_{ta} = |y_{c2} - y_a| = 2d^*$. Therefore,

$$s_{ta} = |p_t - p_a| = |y_t - y_a| - |\delta| = d^* - |\delta| = s_{at} \tag{3}$$

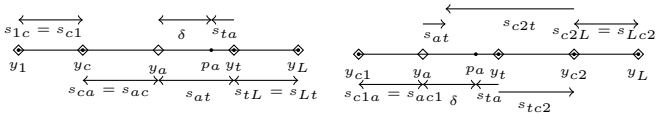
$$s_{c2t} = 2d^* - s_{ta} = 2d^* - d^* + |\delta| = d^* + |\delta|; \tag{4}$$

$s_{c2t}$ indicates that $v_t$ is further than expectation and closer to $v_a$, supporting $v_a$'s claims. All other reports from $v_{c1}$ and $v_{c2}$ are true (except for $s_{c1a}$ and $s_{c2t}$).

Case (*ii*): $v_a$ moving away from $v_t$. If $v_a$ is deviating by $\delta$ from $y_a$ to move further away from $v_t$, we have

$$s_{ta} = |p_t - p_a| = |y_t - y_a| + |\delta| = d^* + |\delta| = s_{at} \tag{5}$$

$$s_{c2t} = 2d^* - s_{ta} = 2d^* - d^* - |\delta| = d^* - |\delta|; \tag{6}$$




(a) Attack type I

(b) Attack type II

Figure 1: Fraudulent position claims for a five vehicle platoon: true position $p_i$ of the $i^{\text{th}}$ vehicle $v_i$ is indicated by "$\cdot$" and reported position $y_i$ is indicated by the "$\diamond$" symbol.

$\delta$ is positive if $v_a$ is in front of $v_t$ , and negative otherwise.

In each attack case, distance bounding by the leader would be insufficient to identify the attacker due to the presence of the colluding attackers. The proposed EDM analysis can successfully detect these attacks and identify the attacker as well.

## III. Euclidean distance matrix (EDM)

An EDM is a matrix $D$ containing an exhaustive table of squared distances $d_{ij}^2$ between points taken by pair from a list of $n$ points. The rank of $D$ is a function of the embedding dimension ($r$) and does not depend upon the number of data points ($n$). Therefore, $D$ is a low rank matrix, given $n > r + 2$. In our approach, we make use of the low rank property of EDM. An EDM constructed for an $n$ vehicle platoon with embedding dimension of 1 will always have a rank of $r + 2 = 3$. We construct two matrices from the available information. Let $Y = \{y_1, ..., y_n\}^T$ be a column vector of positions reported by all the vehicles in the platoon, and $S = \{s_{12}, s_{21}, s_{23}, ..., s_{n(n-1)}\}$ be the vector of sensor measurements from the vehicles. We construct an EDM $D_Y$ from $Y$

$$D_Y = \text{diag}(YY^T)\mathbf{1}^T + \mathbf{1}\ \text{diag}(YY^T)^T - 2(YY^T) \qquad (7)$$

where the matrix $YY^T$ is called the Gramian of the vector $Y$, and the vector $\mathbf{1}$ is a column vector of 1s of dimension $n$. $D_Y$ is a rank 3 matrix. We denote the $i$,j$^{\text{th}}$ element of $D_Y$ as $d_{ij}^2$. It is expected that for $v_i$, $d_{ij} = s_{ij} = d_{ji} = s_{ji}$, where $v_j$ is adjacent to $v_i$, i.e.; $j = i \pm 1$. We construct another matrix $D$ from $D_Y$ and $S$ by replacing all $d_{ij}^2$ in $D_Y$ by $s_{ij}^2$ for $j = i \pm 1$, i.e.; replacing distances to adjacent neighbors for each vehicle by the sensor measurements. $D$ looks as follows:

$$D = \begin{pmatrix} 0 & s_{12}^2 & d_{13}^2 & \dots & \dots \\ & \ddots & \ddots & & \\ \dots & s_{i(i-1)}^2 & 0 & s_{i(i+1)}^2 & \dots \\ & & \ddots & \ddots & \\ \dots & \dots & d_{n(n-2)}^2 & s_{n(n-1)}^2 & 0 \end{pmatrix}$$

## IV. Analysis of EDM for attack detection

The matrix $D$ is a rank 3 matrix if all the vehicles are honest and if there is no inconsistency in the sensor measurements. However, under an attack scenario described in Sec. II, $D$ will have a higher rank than 3 as an immediate result of the attack. We define an error matrix $E = D_Y - D$, to analyze the differences between $D$ and $D_Y$. We use a column sum of $E$ to determine the vehicle with most conflict. Let us consider a $n = 5$ vehicle platoon with $Y = \{1, 2, 3, 4, 5\}$, $d^* = 1$.

To demonstrate a case of Attack type I, assume $v_c = v_2$, $v_a = v_3$, $v_t = v_4$, $v_L = v_5$, and $v_a$ is moving toward $v_t$. Vehicle $v_1$ is a benign vehicle in the platoon. As described in Sec. II-A, $v_t$ reports $s_{ta} = d^* - \delta = 1 - \delta$. Therefore, $D_Y$, $D$, and $E$ have the structure as shown:

| $D_Y$ | $v_1$ | $v_c$ | $v_a$ | $v_t$ | $v_L$ |
|---|---|---|---|---|---|
| $v_1$ | 0 | 1 | 4 | 9 | 16 |
| $v_c$ | 1 | 0 | 1 | 4 | 9 |
| $v_a$ | 4 | 1 | 0 | 1 | 4 |
| $v_t$ | 9 | 4 | 1 | 0 | 1 |
| $v_L$ | 16 | 9 | 4 | 1 | 0 |

| $D$ | $v_1$ | $v_c$ | $v_a$ | $v_t$ | $v_L$ |
|---|---|---|---|---|---|
| $v_1$ | 0 | 1 | 4 | 9 | 16 |
| $v_c$ | 1 | 0 | 1 | 4 | 9 |
| $v_a$ | 4 | 1 | 0 | 1 | 4 |
| $v_t$ | 9 | 4 | $(1-\delta)^2$ | 0 | 1 |
| $v_L$ | 16 | 9 | 4 | 1 | 0 |

| $E$ | $v_1$ | $v_c$ | $v_a$ | $v_t$ | $v_L$ |
|---|---|---|---|---|---|
| $v_1$ | 0 | 0 | 0 | 0 | 0 |
| $v_c$ | 0 | 0 | 0 | 0 | 0 |
| $v_a$ | 0 | 0 | 0 | 0 | 0 |
| $v_t$ | 0 | 0 | $2\delta - \delta^2$ | 0 | 0 |
| $v_L$ | 0 | 0 | 0 | 0 | 0 |

A column sum of $E$ reveals an anomaly for $v_a$ of amount $2\delta - \delta^2$ for any value of $\delta$.

A similar analysis of Attack type II shows, to identify $v_a$ when it is deviating by an amount $\delta$ from $y_a$ towards $v_t$,

$$|\delta| < \frac{2}{3}d^* \qquad (8)$$

When $v_a$ when it is deviating by an amount $\delta$ from $y_a$ away from $v_t$

$$|\delta| < 2d^* \qquad (9)$$

Therefore, detection probability is $\frac{2}{3}$ when the attacker is coming nearer to the target, and 1 when the attacker is moving away from the target. The total detection probability is therefore

$$0.5 \times 1 + 0.5 \times \frac{2}{3} = 0.8333 \qquad (10)$$

which translates to 83.33% detection. Additionally, as the attacker cannot instantaneously achieve a distance of $\frac{2}{3}d^*$ to the target, the initiation of this attack could be detected by employing the EDM method at a fine grained time-scale. That is, using small intervals between position verification cycles allows for 100% detection.

## V. Conclusion

A position verification scheme for vehicular platooning that relies on only local measurements and their broadcast, and which is resistant to terrorist-fraud attacks, was presented.

## References


[1] X.-Y. Lu and S. E. Shladover, "Automated truck platoon control and field test," in *Road Vehicle Automation*. Springer, 2014, pp. 247–261.

[2] R. M. Gerdes, C. Winstead, and K. Heaslip, "Cps: an efficiency-motivated attack against autonomous vehicular transportation," in *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM, 2013, pp. 99–108.

[3] J. J. Haas, "The effects of wireless jamming on vehicle platooning," 2009, [Tech report; online; accessed 04-June-2014].

[4] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 2015.

[5] J. T. Chiang, J. J. Haas, and Y.-C. Hu, "Secure and precise location verification using distance bounding and simultaneous multilateration," in *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, pp. 181–192.

[6] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*, Nov 2005, pp. 7 pp.–840.

[7] T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 16–21, October 2006.