Dynamic Model Based Malicious Collaborator Detection in Cooperative Tracking

Wang Pi[1,2], Pengtao Yang[1], Dongliang Duan[3], Chen Chen[1], Xiang Cheng[1,2], and Liuqing Yang[4]
1. State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronics, School of Electronics Engineering and Computer Science, Peking University, Beijing China
2. Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, China
3. Department of Electrical and Computer Engineering, University of Wyoming, Laramie, WY, USA
4. Department of Electrical and Computer Engineering, Colorado State University, Fort Collins, CO, USA.

***Abstract*—The mobility status of vehicles play a crucial role in most tasks of Autonomous Vehicles (AVs) and Intelligent Transportation System (ITS). To operate securely, a precise, stable and robust mobility tracking system is essential. Compared with self-tracking that relies only on mobility observations from on-board sensors (e.g. Global Positioning System (GPS), Inertial Measurement Unit (IMU) and camera), cooperative tracking increases the precision and reliability of mobility data greatly by integrating observations from road side units and nearby vehicles through V2X communications. Nevertheless, cooperative tracking can be quite vulnerable if there are malicious collaborators sending bogus observations in the network. In this paper, we present a dynamic sequential detection algorithm, dynamic model based mean state detection (DMMSD), to exclude bogus mobility data. Simulations validate the effectiveness and robustness of the proposed algorithm as compared with existing approaches.**

I. Introduction

Autonomous vehicles (AVs) and intelligent transportation system (ITS) are expected to greatly improve the efficiency of transportation systems and reduce fatal accidents in the near future. In the past decade, both industry and academia have paid increasing attention to many fundamental issues for AVs and ITS. Among those issues, obtaining precise mobility status, such as location, velocity and acceleration, of the self and surrounding vehicles is one of the most essential.

In practice, current prevailing tracking techniques often rely exclusively on the on-board sensors, such as Global Positioning System (GPS), Inertial Measurement Unit (IMU) and Lighting Detection and Ranging (LIDAR) to conduct single-vehicle independent tracking. In [1], the state-of-the-art single-vehicle non-cooperative localization techniques are investigated and summarized. As the authors stated, though fusing data from on-board sensors could potentially achieve the required accuracy for autonomous vehicles, the cost of a single vehicle may be too high. In addition, the performance may be compromised in some extreme scenarios. Thus, cooperative localization and tracking methods (see e.g. [2]–[9]) were proposed to utilize off-board information from V2X communications (see e.g. [10]–[14]) to augment the precision and reliability. However, those works assume that the mobility information sent by other collaborators are always trustworthy, which might not be the case in many scenarios. It is true that V2X communications authentication and verification protocols such as those summarized in [15], [16] can prevent unauthenticated and unverified collaborators to inject bogus mobility data into the cooperative network to some extent. Malicious collaborators that can bypass those protection protocols may still exist. Therefore, it is desirable to add an additional level of defense against malicious collaborators in the cooperative mobility tracking process so that it could be robust against bogus mobility data.

Most related work in the literature fall into two categories: 1) mobility data verification; 2) secure localization. Mobility data verification (see e.g. [17]–[20]) seems to be similar with the problem of interest, while they differ in terms of main objective and trust assumptions. The main task of mobility data verification is to verify other vehicles' self-claimed mobility status using its own observations, while the main objective of cooperative mobility tracking is to enhance the precision and reliability of the mobility tracking with observations from cooperating vehicles. In data verification the observations made by the vehicle itself are assumed to be precise or some fully trustworthy collaborators are previously identified, while in cooperative mobility tracking the observations made by the vehicle itself are highly likely to be quite noisy or totally unavailable in some scenarios and none of the cooperating vehicles is fully trustworthy. Thus, the algorithms proposed for mobility data verification are not suitable for the problem of interest in this paper.

A more related topic covered in the literature would be the problem of secure localization in VANET and Wireless Sensor Network (WSN), which considers how to detect and remove the bogus data during the cooperative positioning process.

In the survey papers [21], [22], secure localization algorithms are classified into two categories: 1) filtering algorithms and 2) detection algorithms. Filtering algorithms select

This work was in part supported by the Ministry National Key Research and Development Project under Grant 2017YFE0121400, Guandong Key R&D Project under Grant 2019B010153003, the open research fund of Key Laboratory of Wireless Sensor Network & Communication under Grant 2017003, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, and the National Science Foundation under Grants CNS-1932413 and CNS-1932139.

978-1-7281-3106-1/20/$31.00 ©2020 IEEE

a possible subset of precise observations to form the final estimate, such as gridding and voting in [23], [24], or use some robust loss functions in the formulation of the location estimate to minimize the influences of bogus data, such the least median square (LMS) proposed in [25] and the minimum mean absolute error (MMAE) used in [26], [27]. In contrast, the goal of detection algorithms is to find out all bogus data and exclude them from the cooperative positioning process.

Early detection algorithms are mostly based on the minimum mean square error (MMSE) consistency check, which was first proposed in [24] as a part of the attack-resistant minimum mean square estimation (ARMMSE) algorithm. However, ARMMSE is sometimes regarded as a filtering algorithm since it only selects a subset of the benign data. Cluster-based minimum mean square estimation (CMMSE) in [28] utilizes the consistency check and extends it to a true detection algorithm. Recently, hypothesis testing based detection algorithms, such as generalized likelihood ratio test (GLRT) and malicious node detection algorithm (MNDC) are proposed in [29], [30].

However, the algorithms in WSN either work on the single snap-shot data at a particular time instant (e.g. LMS, ARMMSE,CMMSE) or are only applicable to static scenario (e.g. GLRT, MNDC). This means that previous algorithms aren't capable to utilize temporal correlations of the mobility data to improve the detection accuracy in dynamic cooperative tracking scenario. Thus, a dynamic sequential detection algorithm, Dynamic Model based Malicious Detection (DMMSD), is proposed in this paper to detect bogus data and corresponding malicious collaborators in cooperative tracking.

Though some previous works have simply applied detection approaches used in WSN to VANET and ITS, there is no existing work that concentrates on malicious collaborator detection from the point view of dynamic sequential analysis in the literature. So the major contributions in this paper are:

- We proposed a sequential detection algorithm, namely the dynamic model based mean state detection (DMMSD), to identify malicious collaborators more precisely by utilizing the temporal correlation of mobility data. And to the best of our knowledge, this is the first time sequential malicious user detection algorithm are proposed in cooperative mobility tracking.
- We proposed a secure cooperative mobility tracking process to integrate proposed detection algorithm with existing cooperative tracking algorithms.

The proposed algorithm is tested under the most threatening attacks, the coordinated trajectory attacks, and compared with the existing algorithms. Simulations validate the effectiveness and robustness of the proposed algorithm as compared with existing approaches.

II. System Model

In general, the physical motion of a vehicle can be modeled as a first-order hidden Markov model [31]:

$$\begin{aligned} \boldsymbol{s}[j] &= \boldsymbol{f}\left(\boldsymbol{s}[j-1], \boldsymbol{u}[j], \boldsymbol{w}[j]\right), \\ \boldsymbol{z}[j] &= \boldsymbol{g}\left(\boldsymbol{s}[j], \boldsymbol{v}[j]\right), \end{aligned} \tag{1}$$

where j is the discrete time index, $\boldsymbol{s}$ is the state of the vehicle which includes position and velocity, $\boldsymbol{u}$ is the command process or equivalently the driving input, and $\boldsymbol{w}$ is the state noise; $\boldsymbol{z}$ is the observations through measurement devices such as GPS, IMU, LIDAR etc. and $\boldsymbol{v}$ is the measurement noise; $\boldsymbol{f}$ and $\boldsymbol{g}$ are the state and measurement functions which can be obtained by the physical laws of the motion and the properties of the sensing devices, respectively.

We assume that all vehicles in cooperation are equipped with GPS, IMU, and the integrated sensing system which may include LIDAR, radar, camera and so on. Each vehicle obtains its own position estimate from GPS, its own velocity estimate from IMU and wheel encoders, and the relative position and velocity with respect to other vehicles through the sensing system. To develop the mobility tracking algorithm, here we develop the detailed observation and state transfer model as follows:

A. System State Transfer Model

For a vehicle V_i, we can describe its mobility in a system state transfer equation [31]:

$$\boldsymbol{s}_i[j] = \boldsymbol{A}\boldsymbol{s}_i[j-1] + \boldsymbol{B_u}\boldsymbol{u}_i[j] + \boldsymbol{w}_i[j], \tag{2}$$

where

$$\boldsymbol{s}_i = \begin{pmatrix} x_i \\ \dot{x}_i \\ y_i \\ \dot{y}_i \end{pmatrix}, \boldsymbol{u}_i = \begin{pmatrix} F_{i,x} \\ F_{i,y} \end{pmatrix}, \boldsymbol{w}_i = \begin{pmatrix} w_{x_i} \\ w_{\dot{x}_i} \\ w_{y_i} \\ w_{\dot{y}_i} \end{pmatrix}, \tag{3}$$

$$\boldsymbol{A} = \begin{pmatrix} 1 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \boldsymbol{B_u} = \begin{pmatrix} \frac{(\Delta t)^2}{2} & 0 \\ \Delta t & 0 \\ 0 & \frac{(\Delta t)^2}{2} \\ 0 & \Delta t \end{pmatrix}, \tag{4}$$

x_i, y_i are the Cartesian coordinates of V_i, $\dot{x}_i, \dot{y}_i$ are the velocity of V_i; $F_{i,x}$ and $F_{i,y}$ are the vehicle command process that provides acceleration, which can be provided by the IMU; $\boldsymbol{w}$ is the state noise which can be usually modeled as additive white Gaussian noise (AWGN); Δt is the discrete time step.

B. Observation Model

The observation at an arbitrary vehicle V_s is composed of two parts: 1) the observation of its own mobility status, such as those provided by GPS and IMU, denoted as $\boldsymbol{z}_s$; 2) the observation of the relative mobility status between another vehicle V_i and itself, such as those provided by the integrated sensing system, denoted as $\boldsymbol{z}_{i\to s}$. For $\boldsymbol{z}_s$, we have

$$\boldsymbol{z}_s[j] = \boldsymbol{H}_s\boldsymbol{s}_s[j] + \boldsymbol{v}_s[j], \tag{5}$$

where $\boldsymbol{H}_s$ is the measurement matrix and $\boldsymbol{v}_s$ is the measurement noise, both of which can be determined by the properties of the sensing devices. For $\boldsymbol{z}_{i\to s}$, we have

$$\boldsymbol{z}_{i\to s}[j] = \boldsymbol{H}_{i\to s}\boldsymbol{s}_{i\to s}[j] + \boldsymbol{v}_{i\to s}[j], \tag{6}$$

where $\boldsymbol{s}_{i\to s}[j] = \boldsymbol{s}_i[j] - \boldsymbol{s}_s[j]$ is the relative state between vehicles s and i. The detailed value of $\boldsymbol{H}_{i\to s}$ and the statistical property of $\boldsymbol{v}_{i\to s}$ depend on the sensing device and the way to extract the related information from the raw data. Without

loss of generality, in this paper we assume that in both cases, the sensing devices have direct measurement of the state and the measurement noise is AWGN with known variance.

C. Secure Cooperative Mobility Tracking Process

The cooperative tracking model used here is the integration of our previous model [7] and the proposed malicious collaborator detection algorithm. The vehicle observed by other vehicles is called the target vehicle and denoted as V_{T} and the collaborators are denoted as V_i $(i = 1, 2, \cdots, N)$, where N is the number of vehicles in cooperation. At each time instant, V_{T} feeds the received state observations from N vehicles to the proposed DMMSD algorithm. The current and previous $K-1$ observations of each vehicle form the observation sequence. Then DMMSD analyzes the sequence of all collaborators to detect potential malicious ones. At the same time, current observations are also sent to N independent Kalman filters on V_{T} to generate current state estimates of V_{T}. Finally, the detection results will decide the estimates from which Kalman filters will be trusted and hence used to form the fused global state estimate as the mobility tracking result.

D. Threat Model

The threat model adopted here is similar to the threat models in WSN and VANET. In general, malicious attacks can be classified into two categories: 1) uncoordinated attacks: there is no communication among malicious vehicles, and thus the bogus data from each malicious vehicle are independent; and 2) coordinated attacks: before reporting their own bogus data to the target vehicle, the malicious vehicles will first confirm a mutual bogus state that deviates from the true state of V_{T}. Then each vehicle randomly choose a state near the confirmed mutual state to manufacture its bogus data. In this paper, we will consider the much more threatening coordinated attacks.

Particularly, if the data reported by malicious vehicles during the attack can form a plausible state trajectory that is close to the true state trajectory of V_{T}, the precision and stability of the global mobility estimation of V_{T} could be greatly degraded. Here, we term it as the trajectory attack.

Combining the two most threatening attack pattern above together, we can obtain the *coordinated trajectory attack*:

$$\boldsymbol{z}_{\mathrm{m}i}[j] = \boldsymbol{s}_{(\mathrm{m\_traj})}[j] + \boldsymbol{\delta}_{\mathrm{m}i}[j], \quad (j \in T_{\mathrm{m}}) \,, \tag{7}$$

where $i \in M$ and M is the set of identities of malicious vehicles; $\boldsymbol{z}_{\mathrm{m}i}[j]$ is the state observations from the i-th malicious vehicle at discrete time $t_j = j\Delta t$; $T_{\mathrm{m}} = [t_{\mathrm{start}}, t_{\mathrm{end}}]$ is the duration of the coordinated trajectory attack; $\boldsymbol{s}_{(\mathrm{m\_traj})}$ is the mutual bogus state trajectory confirmed by all malicious vehicles; independent small noise $\boldsymbol{\delta}_{\mathrm{m}i}$ is added by each malicious vehicle to make the spatial distribution of the bogus data at each time instant not abnormally dense.

III. The Proposed Algorithm

Sequential algorithms are also recently proposed to improve the performance of secure localization in WSN, e.g. previously mentioned MNDC algorithm. It averages data received over a period of time to reduce the influence of measurement noise and increase the accuracy of detection. However, the static node and fixed position assumption of MNDC makes it inapplicable in the dynamic cooperative mobility tracking scenario where all vehicles are moving in most of time.

To address the dynamic property of vehicles and form our dynamic sequential detection algorithm DMMSD, we rely on the state transfer function (2) in the dynamic model which completely describes the theoretical trajectory of the target vehicle. DMMSD consists of three main steps: 1) prediction with dynamic model, 2) variance reduction with averaging, 3) detection with consistency check and clustering.

A. Prediction with Dynamic Model

The predication with dynamic model is motivated by the fact that acceleration of the target vehicle at each time instant can be measured by its own on-board IMU precisely and regarded as trustworthy. Therefore, once we know the mobility state observation of V_{T} at a specific time instant, we can predict the possible observation for any future time with acceleration measurements and the dynamic model.

For instance, consider any particular cooperating vehicle V_i observing V_{T}. In a period of time $\{t_1, t_2, \cdots t_K\}$ (t_K is the current time instant). V_{T} can use state observation $\boldsymbol{z}_{i1}$ received from V_i at t_1 and acceleration measurements $\{a_1, a_2, \cdots a_{K-1}\}$ from its IMU to predict the observation V_i may send at t_K. We denote this predication as $\hat{\boldsymbol{z}}_{i(1\to K)}$. Note that we write the state observation sent by V_i at time t_j as $\boldsymbol{z}_{ij}$ instead of $\boldsymbol{z}_{\mathrm{T}\to i}[j] + \boldsymbol{z}_i[j]$ for simplicity. Similarly, other state predictions $\{\hat{\boldsymbol{z}}_{i(2\to K)}, \hat{\boldsymbol{z}}_{i(3\to K)}, \cdots \hat{\boldsymbol{z}}_{i(K\to K)}\}$ can also be obtained from $\{\boldsymbol{z}_{i2}, \boldsymbol{z}_{i3}, \cdots \boldsymbol{z}_{iK}\}$. Note that $\hat{\boldsymbol{z}}_{i(K\to K)} = \boldsymbol{z}_{iK}$.

After prediction, state observations from V_i at different time instants are converted into state predictions at the same time instant, which eliminates the influence of the motion of V_{T} and turns the dynamic sequential analysis problem into a static problem. Therefore, averaging strategy can be subsequently utilized to process those predictions.

B. Variance Reduction with the Averaging

The core idea of DMMSD is using correlated observation sequence to reduce the measurement noise and improve the detection accuracy. Thus, after converting state observations into state predictions, the second step is to use averaging strategy on multiple predictions to reduce the measurement noise. The mean of the state predictions of V_i, or equivalently the mean state, in this period is written as $\bar{\boldsymbol{z}}_{iK}$:

$$\bar{\boldsymbol{z}}_{iK} = \frac{\hat{\boldsymbol{z}}_{i(1\to K)} + \hat{\boldsymbol{z}}_{i(2\to K)} + \cdots + \hat{\boldsymbol{z}}_{i(K\to K)}}{K} \,. \tag{8}$$

Iteratively, V_{T} will compute the mean of state predictions of all cooperating vehicle and store them in the mean state vector

$$\bar{\boldsymbol{Z}} = \begin{pmatrix} \bar{\boldsymbol{z}}_{1K} & \bar{\boldsymbol{z}}_{2K} & \cdots & \bar{\boldsymbol{z}}_{NK} \end{pmatrix}^{\mathrm{T}} \,, \tag{9}$$

which will be analyzed in the third step of detection. Qualitatively speaking, the variance of $\bar{\boldsymbol{z}}_{iK}$ is surely much smaller than variance of any single prediction $\hat{\boldsymbol{z}}_{i(j\to K)}$ or single observation $\boldsymbol{z}_{ij}$. However, to determine the optimal sequence length K that achieves the maximum variance reduction, one needs to obtain the quantitative relation between the variance of $\boldsymbol{z}_{ij}$, the variance of $\bar{\boldsymbol{z}}_{iK}$ and the sequence length K. The relation is presented as the following theorem:

Theorem 1: Considering the accumulative noise brought in by the prediction, the variance of mean of state predictions given by a specific cooperating vehicle is approximately:

$$D(\bar{\boldsymbol{z}}_K)=\begin{pmatrix} D(\bar{x}_K) \\ D(\bar{v}_K) \end{pmatrix} \approx \frac{1}{K^2}\begin{pmatrix} K\sigma_x^2+(\Delta t)^2\sigma_v^2\sum_{j=1}^{K-1} j^2 \\ K\sigma_v^2+(\Delta t)^2\sigma_a^2\sum_{j=1}^{K-1} j^2 \end{pmatrix}, \tag{10}$$

where $D(\bar{x}_K), D(\bar{v}_K)$ are variance of mean position and velocity predictions, σ_x^2, σ_v^2 are the variance of single position, velocity measurement of cooperating vehicle and σ_a^2 is the variance of single acceleration measurement.

Proof 1: See Appendix A.

To get a clear vision of the amount of reduction in variance, we adopt a practical observation interval $\Delta t = 0.1\text{s}$ and assume that $\sigma_x^2 = \sigma_v^2 = \sigma^2$ and in practice, $\sigma^2 \gg \sigma_a^2$. Accordingly

$$\frac{D(\bar{\boldsymbol{z}}_K)}{\sigma^2} \approx \frac{1}{600K}\begin{pmatrix} 600+(K-1)(2K-1) \\ 600 \end{pmatrix}. \tag{11}$$

We can see that $D(\bar{v}_K)/\sigma^2$ keeps decreasing as K increases, while $D(\bar{x}_K)/\sigma^2$ has a minimum value due to accumulative noise brought by prediction process. Therefore, under the assumptions above, $K = 16$ is the optimal sequence length to minimize $D(\bar{x}_K)/\sigma^2$.

C. Detection Using the Consistency Check and Clustering

First two steps enlarge the difference among the bogus and normal observations by reducing the variance of the observations. However, we are yet to set a criteria to determine whether there are bogus observations and a tool to separate the bogus and normal observations. For this task, we propose the following two-step procedure: 1) Consistency Check: determine whether there are bogus observations by analyzing the distribution of the mean states of all cooperative vehicles; and 2) Clustering: if the step above indicates the existence of bogus data, then we apply a clustering algorithm to classify the mean states into two clusters.

In the consistency check, the mean square error (MSE) consistency which was firstly proposed in [24] is adopted. Its core idea is concisely explained here, while the detailed derivation can be found in the original paper: since normal observations are the sum of the true target state and zero-mean Gaussian noise, MSE of mean state vector $\bar{\boldsymbol{Z}}$ should satisfy $P\{\text{MSE} < \tau^2\} \to 1$ if all collaborators are benign and the normalized threshold τ^2 is properly selected. However, if there are bogus observations, the MSE would be very likely to exceed τ^2. Thus, the MSE of $\bar{\boldsymbol{Z}}$ is computed to determine whether observations from cooperating vehicles are consistent with each other.

If the consistency check indicates the existence of bogus data, clustering algorithm will be conducted on $\bar{\boldsymbol{Z}}$. If not, all observations will be regarded as normal. The goal of clustering is to distinguish normal and bogus mean states, then identify benign and malicious vehicles, so the number of cluster is always two. In this case, K-means clustering is a very effective algorithm and adopted here. However, any other clustering algorithms are also fully compatible with this framework.

The vehicles in the larger cluster are regarded as benign, and those in the smaller one are marked as malicious. This means that, like all other algorithms which assume "No one is absolutely trustworthy", DMMSD only handles the scenario where ratio of malicious users is less than 0.5. The final result of Consistency Check and Clustering are concluded as a boolean vector, or equivalently a trust table, which describes each vehicle as benign or malicious.

IV. Performance Evaluation

In this section, we evaluate DMMSD by comparing its performance with popular secure localization algorithms in WSN. Algorithms selected here include a detection algorithm, the SeqMMSE, an enhanced sequential version of CMMSE from [28] and two filtering algorithms, LMS from [25] and the MMAE used in [26], [27]. Though recently proposed MNDC algorithm in WSN can achieve high detection accuracy in static scenario, it's inherently inapplicable to dynamic scenario like cooperative tracking, thus, not adopted here.

Since previous and proposed algorithm all process position and velocity information in the state vector separately, without loss of generality, in the evaluation we assume bogus observations only exist in the position information for better result visualization. The true trajectory of the target vehicle can be seen as the blue line in Fig 2a, which is a typical lane changing action. Parameters of our simulation are listed in Table I.

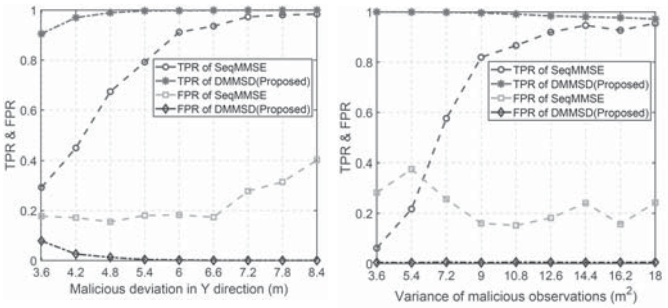
TABLE I: Simulation Parameters

Simulation Parameters	Value
Discrete time step	0.1 [s]
Duration of simulation	20 [s]
Length of sequence for analyzing	16
Malicious deviation	5 [m] in Fig. 1b, 2 3.6-8.4 [m] in Fig. 1a
Number of total collaborators	20
Number of malicious collaborators	8 in Fig. 1,2a 0-9 in Fig. 2b
Variance of single normal observation	9 [m^2]
Variance of single bogus observation	9 [m^2] in Fig. 2, 2 3.6-18 [m^2] in Fig. 1b

In the coordinated trajectory attack, the malicious trajectory $y_{\text{m}}[j]$ is assumed to be obtained by adding a constant deviation, ϵ_{m}, to the true trajectory $y_{\text{t}}[j]$ of the target vehicle in Y direction, i.e., $y_{\text{m}}[j] = y_{\text{t}}[j] + \epsilon_{\text{m}}$.

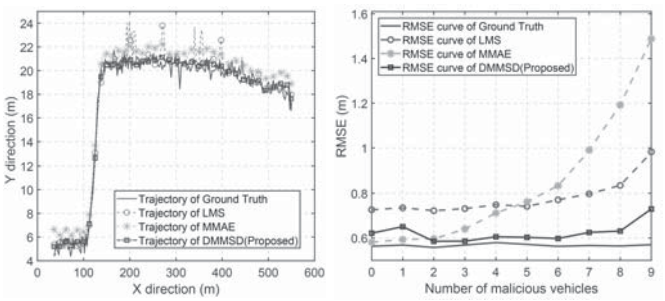
True positive rate (TPR) and false positive rate (FPR) are essential indicators to evaluate the performance of detection algorithms. Thus, we firstly compare the TPR and FPR of SeqMMSE and DMMSD with varying malicious deviation ϵ_{m} and variance of bogus data σ_{m}^2 in Fig. 1. As we can see, DMMSD significantly outperform SeqMMSE with better and more robust TPR and FPR.

To compare DMMSD with filtering algorithms, trajectory estimates and the root mean square error (RMSE) of estimates are used for evaluation. Trajectory estimates of different algorithms in Fig. 2a clearly demonstrates that the estimate of DMMSD is more stable and closer to the ground truth than LMS and MMAE. The estimate from LMS is not stable enough and the estimate from MMAE has an observable deviation in the Y direction due to the malicious attack. The



(a) With varying deviation. (b) With varying variance.

Fig. 1: TPR and FPR under coordinated trajectory attacks.



(a) Trajectory estimates. (b) RMSEs.

Fig. 2: Performance under coordinated trajectory attacks.

advantages of DMMSE are further verified in comparison of RMSE of estimates when number of malicious vehicles varies.

In Fig. 2b, the RMSE of DMMSD is always lower than that of LMS and stays much closer to the ground truth until the ratio of malicious vehicle approaches 0.5 where all algorithm has a larger increase in RMSE. As compared with MMAE, DMMSD has substantial advantage in most ratios. Though it's noticed that the RMSE of DMMSD is slightly higher than that of MMAE when the ratio of malicious users is very low, that is actually a reasonable result caused by balanced detection nature of DMMSD. A very brief explanation is: to make DMMSD more generalized and resistant to different types of attack, it is desirable to make the detection rate more balanced,i.e., make the TPR slightly smaller than 1 and FPR slightly larger than 0, instead of pushing one of them to the best. Therefore, when the ratio of malicious users is low, few malicious users may be classified as benign and some benign ones may be regarded as malicious. Consequently, RMSE of the DMMSD is slightly higher than MMAE. Though one is able to increase TPR or decrease FPR by fine-tuning parameters in the Consistency Check step, it often comes with the price of significant increase in FPR or decrease TPR according to our test. Thus, to get a balanced performance in all malicious ratio, a little bit higher RMSE in the low malicious ratio case is completely acceptable.

Quantitatively, RMSE of DMMSD is at least 11.5% and at most 25.8% lower than RMSE of LMS. As compared with MMAE, it's at most 10% higher in the low malicious ratio, while it can be 51% lower than MMAE when the malicious ratio approaches 0.5. Considering the mobility tracking has a fundamental impact on the safety and reliability of AVs and ITS, more robust and precise DMMSD is apparently better candidate for securing the cooperative tracking.

V. Conclusions

In this paper, we presented a dynamic sequential detection algorithm termed as DMMSD. Dynamic model based prediction and averaging strategies are introduced to utilize the temporal correlation of observations to increase the detection accuracy. Compared with sequential version of classical detection algorithms, DMMSD has much better TPR and FPR performance. Compared with the filtering algorithms used in WSN, DMMSD is much more robust under coordinated trajectory attack. Possible improvements in the future may include: 1) the integration of filtering algorithm and DMMSD by adding an adaptive switching module, which can utilize the low RMSE advantage of filtering algorithm in low malicious ratio scenario and robustness of DMMSD in high malicious ratio; and 2) the utilization of the correlation among acceleration, velocity and position to conduct hierarchical joint detection.

Appendix A
Proof of Theorem 1

The four dimensions of $\boldsymbol{s}$ and $\boldsymbol{z}$ are: position and velocity in X direction, position and velocity in Y direction as introduced in (3),(5),(6). Without loss of generality, we assume the motions in X and Y direction are independent, so we only consider X direction in the following derivations.

Firstly, the variance of single prediction $\hat{\boldsymbol{z}}_{(j\to K)}$ from any particular cooperating vehicle is derived. For simplicity, we use scalar x, v, a as the position, velocity observation from cooperating vehicle and acceleration observation from IMU of V_{T}. According to the state transfer function (2) we have:

$$x_{j+1} = x_j + v_j\Delta t + \frac{1}{2}a_j(\Delta t)^2 \tag{12}$$

$$v_{j+1} = v_j + a_j\Delta t \tag{13}$$

Then we can get position and velocity prediction at t_K from the observation at t_1:

$$\hat{x}_{1\to K} = x_1 + \Delta t\sum_{j=1}^{K-1} v_j + \frac{1}{2}(\Delta t)^2\sum_{j=1}^{K-1} a_j \tag{14}$$

$$\hat{v}_{1\to K} = v_1 + \Delta t\sum_{j=1}^{K-1} a_j \tag{15}$$

Considering that we only have the velocity at t_1, we need to write $\hat{x}_{1\to K}$ as:

$$\hat{x}_{1\to K}=x_1+\Delta t\sum_{j=1}^{K-1}v_1+(\Delta t)^2\sum_{j=1}^{K-1}\sum_{k=1}^{j-1}a_k+\frac{1}{2}(\Delta t)^2\sum_{j=1}^{K-1}a_j \tag{16}$$

All noises of x, v, a in (15),(16) are assumed to be AWGN with known variance as mentioned in Section II-B. Use $\sigma_x^2, \sigma_v^2, \sigma_a^2$ to represent their variances. Thus, the variances of $\hat{x}_{1\to K}$ and $\hat{v}_{1\to K}$ can be derived as:

$$D(\hat{x}_{1\to K}) = D(x_1) + (\Delta t)^2 D(\sum_{j=1}^{K-1} v_1) + \frac{1}{4}(\Delta t)^4 D(\sum_{j=1}^{K-1} a_j) + (\Delta t)^4 D(\sum_{j=1}^{K-1}\sum_{k=1}^{j-1} a_k) \tag{17a}$$

$$D(\hat{v}_{1\to K}) = D(v_1) + (\Delta t)^2 D(\sum_{j=1}^{K-1} a_j) \tag{17b}$$

With further simplifications,

$$D(\hat{x}_{1\to K}) = \sigma_x^2 + (K-1)^2(\Delta t)^2\sigma_v^2 + \frac{1}{4}(\Delta t)^4(K-1)\sigma_a^2 + (\Delta t)^4\sigma_a^2[1^2+2^2+...+(K-2)^2] \quad (18a)$$

$$D(\hat{v}_{1\to K}) = \sigma_v^2 + (K-1)^2(\Delta t)^2\sigma_a^2 \quad (18b)$$

A practical observation interval $\Delta t = 0.1$s is used in our assumption. The variance of the observations of IMU is quite small and the length of sequence K won't be larger than 30. Therefore, the last two terms in (18a) are high-order small amount and can be neglected. Then the approximation of $D(\hat{x}_{1\to K})$ have the same form as $D(\hat{v}_{1\to K})$, so we can use state vector to integrate them and simplify the expression.

$$D(\hat{\boldsymbol{z}}_{1\to K}) = \begin{pmatrix} D(\hat{x}_{1\to K}) \\ D(\hat{v}_{1\to K}) \end{pmatrix} \approx \begin{pmatrix} \sigma_x^2 + (K-1)^2(\Delta t)^2\sigma_v^2 \\ \sigma_v^2 + (K-1)^2(\Delta t)^2\sigma_a^2 \end{pmatrix} \quad (19)$$

The form of variance of other prediction $D(\hat{\boldsymbol{z}}_{j\to K})$ is similar:

$$D(\hat{\boldsymbol{z}}_{j\to K}) \approx \begin{pmatrix} \sigma_x^2 + (K-j)^2(\Delta t)^2\sigma_v^2 \\ \sigma_v^2 + (K-j)^2(\Delta t)^2\sigma_a^2 \end{pmatrix}. \quad (20)$$

Eventually, the variance of the mean of state predictions $D(\bar{\boldsymbol{z}}_K)$ can be obtained:

$$D(\bar{\boldsymbol{z}}_K) = \frac{D(\hat{\boldsymbol{z}}_{1\to K}) + D(\hat{\boldsymbol{z}}_{2\to K}) + ... + D(\hat{\boldsymbol{z}}_{K\to K}))}{K^2} \approx \frac{1}{K^2}\begin{pmatrix} K\sigma_x^2 + (\Delta t)^2\sigma_v^2(\sum_{j=1}^{K-1} j^2) \\ K\sigma_v^2 + (\Delta t)^2\sigma_a^2(\sum_{j=1}^{K-1} j^2) \end{pmatrix}.$$

REFERENCES

[1] S. Kuutti, S. Fallah, K. Katsaros, M. Dianati, F. Mccullough, and A. Mouzakitis, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 829–846, 2018.

[2] S. Fujii, A. Fujita, T. Umedu, S. Kaneda, H. Yamaguchi, T. Higashino, and M. Takai, "Cooperative vehicle positioning via v2v communications and onboard sensors," in *2011 IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–5, IEEE, 2011.

[3] M. Rohani, D. Gingras, V. Vigneron, and D. Gruyer, "A new decentralized bayesian approach for cooperative vehicle localization based on fusion of gps and inter-vehicle distance measurements," in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, pp. 473–479, IEEE, 2013.

[4] L. Altoaimy and I. Mahgoub, "Fuzzy logic based localization for vehicular ad hoc networks," in *2014 IEEE Symposium on Computational Intelligence in Vehicles and Transportation Systems (CIVTS)*, pp. 121–128, IEEE, 2014.

[5] C.-H. Chen, C.-A. Lee, and C.-C. Lo, "Vehicle localization and velocity estimation based on mobile phone sensing," *Ieee Access*, vol. 4, pp. 803–817, 2016.

[6] L. Conde, R. Chelim, and U. Nunes, "Collaborative vehicle self-localization using multi-gnss receivers and v2v/v2i communications," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, pp. 2525–2532, IEEE, 2015.

[7] P. Yang, D. Duan, C. Chen, X. Cheng, and L. Yang, "Optimal multi-sensor multi-vehicle (msmv) localization and mobility tracking," in *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 1223–1227, IEEE, 2018.

[8] X. Cheng, D. Duan, L. Yang, and N. Zheng, "Cooperative intelligence for autonomous driving," *ZTE Communications*, 2019.

[9] Y. Li, D. Duan, C. Chen, X. Cheng, and L. Yang, "Occupancy grid map formation and fusion in cooperative autonomous vehicle sensing," in *2018 IEEE International Conference on Communication Systems (ICCS)*, (Chengdu, China), pp. 204–209, IEEE, December 19-21, 2018.

[10] X. Cheng, R. Zhang, and L. Yang *5G-enabled vehicular communications and networking,* Springer, Cham, Switzerland, 2018.

[11] X. Cheng, R. Zhang, and L. Yang, "Wireless toward the era of intelligent vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 188–202, 2019.

[12] X. Cheng, C. Chen, W. Zhang, and Y. Yang, "5G-enabled cooperative intelligent vehicular (5GenIV) framework: When Benz meets Marconi," *IEEE Intelligent Systems*, vol. 32, pp. 53–59, May/June 2017.

[13] B. Hu, L. Fang, X. Cheng, and L. Yang, "Vehicle-to-vehicle distributed storage in vehicular networks," in *2018 IEEE International Conference on Communications (ICC)*, (Kansas City, MO), May 20-24, 2018.

[14] B. Hu, L. Fang, X. Cheng, and L. Yang, "In-vehicle caching (IV-Cache) via dynamic distributed storage relay (d^2sr) in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 68, pp. 843–855, January 2019.

[15] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted v2x communication," *Vehicular Communications*, vol. 12, pp. 50–65, 2018.

[16] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for v2x communications: A survey," *Computer Networks*, vol. 151, pp. 52–67, 2019.

[17] A. Jaeger, N. Bißmeyer, H. Stübing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *International Journal of Intelligent Transportation Systems Research*, vol. 10, no. 1, pp. 11–21, 2012.

[18] M. Schäfer, V. Lenders, and J. Schmitt, "Secure track verification," in *2015 IEEE Symposium on Security and Privacy*, pp. 199–213, IEEE, 2015.

[19] L. Altoaimy and I. Mahgoub, "Mobility data verification for vehicle localization in vehicular ad hoc networks," in *2016 IEEE Wireless Communications and Networking Conference*, pp. 1–6, IEEE, 2016.

[20] M. Sun, M. Li, and R. Gerdes, "A data trust framework for vanets enabling false data detection and secure vehicle tracking," in *2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, IEEE, 2017.

[21] H. Wang, Y. Wen, Y. Lu, D. Zhao, and C. Ji, "Secure localization algorithms in wireless sensor networks: a review," in *Advances in Computer Communication and Computational Sciences*, pp. 543–553, Springer, 2019.

[22] Y. Zeng, J. Cao, J. Hong, S. Zhang, and L. Xie, "Secure localization and location verification in wireless sensor networks: a survey," *The Journal of Supercomputing*, vol. 64, no. 3, pp. 685–701, 2013.

[23] G. Yan, X. Chen, and S. Olariu, "Providing vanet position integrity through filtering," in *2009 12th International IEEE Conference on Intelligent Transportation Systems*, pp. 1–6, IEEE, 2009.

[24] D. Liu, P. Ning, and W. K. Du, "Attack-resistant location estimation in sensor networks," in *Proceedings of the 4th international symposium on Information processing in sensor networks*, p. 13, IEEE Press, 2005.

[25] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proceedings of the 4th international symposium on Information processing in sensor networks*, p. 12, IEEE Press, 2005.

[26] D. Wang, J. Wan, M. Wang, and Q. Zhang, "An mef-based localization algorithm against outliers in wireless sensor networks," *Sensors*, vol. 16, no. 7, p. 1041, 2016.

[27] M. Shanthi and D. K. Anvekar, "Secure localization for underwater wireless sensor networks based on probabilistic approach," in *2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, pp. 1–6, IEEE, 2018.

[28] C. Wang, A. Liu, and P. Ning, "Cluster-based minimum mean square estimation for secure and resilient localization in wireless sensor networks," in *International Conference on Wireless Algorithms, Systems and Applications (WASA 2007)*, pp. 29–37, IEEE, 2007.

[29] S. A. AlRoomi, I. Ahmad, and T. Dimitriou, "Secure localization using hypothesis testing in wireless networks," *Ad Hoc Networks*, vol. 74, pp. 47–56, 2018.

[30] X. Liu, S. Su, F. Han, Y. Liu, and Z. Pan, "A range-based secure localization algorithm for wireless sensor networks," *IEEE Sensors Journal*, vol. 19, no. 2, pp. 785–796, 2018.

[31] L. Mihaylova, D. Angelova, S. Honary, D. R. Bull, C. N. Canagarajah, and B. Ristic, "Mobility tracking in cellular networks using particle filtering," *IEEE Transactions on Wireless Communications*, vol. 6, no. 10, pp. 3589–3599, 2007.