Proceedings of the ASME 2020
Dynamic Systems and Control Conference
DSCC2020
October 4-7, 2020, Pittsburgh, PA, USA

DSCC2020-3139

ATTACK-RESILIENT OBSERVER PRUNING FOR PATH-TRACKING CONTROL OF WHEELED MOBILE ROBOT

Yu Zheng, Olugbenga Moses Anubi
FAMU-FSU College of Engineering
Tallahassee, FL 32310, USA
Email: yz19b@fsu.edu, oanubi@fsu.edu

ABSTRACT

Path-tracking control of wheeled mobile robot (WMR) has gained a lot of research attention, primarily because of its wide applicability – for example intelligent wheelchairs, exploration-assistant remote WMR. Recent increase in remote and autonomous operations/requirements for WMR has led to more and more use of IoT devices within the control loop. Consequently, providing interfaces for malicious interactions through false data injection attacks (FDIA). Moreover, optimization-based FDIAs have been shown to cause catastrophic consequences in feedback control systems while by-passing any residual-based monitoring system. Since these attacks target system measurement process, this paper focuses on the problem of improving the resiliency of dynamical observers against FDIA. Specifically, we propose an attack-resilient pruning algorithm which attempts to exclude compromised channels from being processed by the observer. The proposed pruning algorithm improves attack-localization precision to 100% *with high probability, which correspondingly improves the resiliency of the underlying UKF to FDIA. The improvements due to the developed resilient pruning-based observer is validated through a numerical simulation of a two-layer path-tracking control platform of differential-driven wheeled mobile robot (DDWMR) under FDIA.*

NOMENCLATURE

The following notations and definitions are used throughout the whole paper: $\mathbb{R}, \mathbb{R}^n, \mathbb{R}^{n\times m}$ denote the space of real numbers, real vectors of length n and real matrices of n rows and m columns respectively. $\mathbb{R}_+$ denotes positive real numbers. Normal-face lower-case letters $(e.g.\ x \in \mathbb{R})$ are used to represent real scalar, bold-face lower-case letter $(e.g.\ \mathbf{x} \in \mathbb{R}^n)$ represents vectors, while normal-face upper case $(e.g.\ X \in \mathbb{R}^{n\times m})$ represents matrices. $\mathbb{1}$ represents all-ones vector. Let $\mathcal{T} \subseteq \{1,\dots,n\}$, then for a matrix $X \in \mathbb{R}^{n\times m}$, $X_{\mathcal{T}} \in \mathbb{R}^{|\mathcal{T}|\times m}$ is the sub-matrix obtained by extracting the rows of X corresponding to the indices in $\mathcal{T}$. $\mathcal{T}^c$ denotes the complement of a set $\mathcal{T}$ and the universal set on which it is defined will be clear from the context. The symbol $\circ$ denotes element-wise multiplication of two vectors and is defined as $\mathbf{z} = \mathbf{x} \circ \mathbf{y}$, where $\mathbf{z}_i = \mathbf{x}_i \cdot \mathbf{y}_i$. The symbol $*$ denotes the convolution operator for vectors. $\mathsf{supp}(\mathbf{x})$ donotes the support of the vector $\mathbf{x}$ given by the set $\mathcal{T} = \mathsf{supp}(\mathbf{x}) = \{i | \mathbf{x}_i \neq 0\}$. $\mathsf{argsort}\downarrow(\mathbf{x})$ denotes a function that returns the sorted indices of vector x in descending order. The space of all square integrable signals is denoted by $\mathcal{L}_2$. The space of all point-wise bounded signals is denoted by $\mathcal{L}_\infty$.

1 INTRODUCTION

Nonholonomic wheeled mobile robots (WMRs) have attracted much attention in the past two decades due to its great mobility and the broad range of applications [1]. Quite a lot of researchers have developed path-tracking controllers for wheeled mobile robots considering nonlinearities [2, 3, 4], robustness against model uncertainties [5,6], robustness against noise [7,8]. The control strategies depend on the measurements of the robots' velocities and/or location coordinates. However, due to the increasing dependence on IoT devices and wireless communica-

tion, the resulting tight coupling of computation, communication and physical components enables malicious agents to inject attacks via the sensors and actuators [9]. Consequently, controller would make decision based on attacked measurements or the vehicle would receive malicious control signals. One type of attacks, false data injection attacks (FDIAs), has been shown to be capable of fooling bad data detection (BDD) scheme to compromise the integrity of the state estimator, even with very sparse measurements corruption. This results in false operations of the whole system without any alarm [10, 11]. Therefore, it is necessary to develop an attack-resilient observer-based control scheme to mitigate the effect of those attacks.

Many authors [9, 12, 13] have proposed an ℓ_0-based resilient state estimators with different modifications or under different scenarios. These estimators have been validated using cruise control of autonomous ground vehicle, electrical power systems, industrial control systems. However, with the exception of [13], none of the estimators were validated against large percentage FDIA. Also, in [14], a robot intrusion detection system (RIDS) is designed by leveraging physical dynamics of mobile robots. However, the detection engine is a residual-based Chi-square scheme, which is known to be vulnerable to coordinated FDIAs considered in this paper.

Inspired by recent developments in estimation and compressive sensing, we propose a pruning algorithm to mitigate the effect of FDIA on UKF. Consider a linear measurement model under attack:

$$\mathbf{y} = H\mathbf{x} + \mathbf{e},$$

where, $H \in \mathbb{R}^{m\times n}$ is the linear measurement operator, $\mathbf{x} \in \mathbb{R}^n$ is the state vector, $\mathbf{y} \in \mathbb{R}^m$ is the attacked measurement corrupted by a sparse attack vector $\mathbf{e} \in \mathbb{R}^m$. Consequently, attack-resilient estimation is often formulated as a classical error correction problem [12, 15, 13, 9]:

$$\text{Minimize} : \|\mathbf{e}\|_{\ell_0} \quad \text{Subject to:} \ \ \mathbf{y} = F\mathbf{e},$$

where $F \in \mathbb{R}^{n\times m}$ is a coding matrix with $n \ll m$ and $FH = \mathbf{0}$. It is known [16, 17] that if the number of attacked nodes is small enough, exact state estimation can be guaranteed by solving the above problem. However, it is shown [18] that exact recovery is unattainable by solving the problem above if more than 50% of the sensor nodes are attacked. Moreover, the ℓ_0 optimization problem above is NP-hard and is often relaxed by solving a convex problem if coding matrix satisfies *Restricted Isometry Property* (RIP) [16, 19].

Suppose there is an oracle which gives the exact $\mathsf{supp}(\mathbf{e})$ a priori, then the resilient state estimation problem becomes trivial since any decent regression algorithm will be able to recover the states exactly from the non-attacked set. The challenge, however, is that no such oracle exists. Although, there is a host of localization algorithms [20] designed to serve this purpose, they are always not exact with significant *false positive and false negative rates*. This observation is the central motivation for developing the pruning algorithm. Therefore, the pruning problem to increase the `signal-to-attack-ratio` of the measurement system using any pre-designed inexact attack localization scheme (subsequently referred to as the `oracle`). Then the existing least-square based robust estimation algorithms can be implemented for the *pruned* measurements sets to create a resilient estimator. This process requires a certain amount of redundancy in the measurement system. Otherwise, the estimation problem will be rendered under-determined by the pruning process. Quantifying the required redundancy level for a given oracle is beyond the scope of this present work and will be addressed in future work.

Although, there is a lot of work in the literature on resilient Kalman filtering, typical least-square based robust estimator, mitigating sensors failures, distortion, delay, strong noise interference and more reasons for corrupt signals [21,22,23]. However, the specific characteristics of attack, unbounded but sparse, make those resilient filters be hard to perform attack-resiliently. To the best of the authors' knowledge, this paper represents one of the earliest approach to prune measurement channels in real-time in order to improve the resiliency of an underlying observer against FDIA.

The rest of paper is organized as follows. In Section 2, a two-layer controller is designed, with UKF, to track a reference trajectory with noisy measurement system. In Section 3, an optimization-based FDIA algorithm designed to bypass the monitor is also implemented. In Section 4, the channel pruning algorithm is developed and combined with traditional UKF to create a resilient observer. In Section 5, simulation results are presented to validate the proposed pruning-based resilient observer. In Section 6, concluding remarks and future directions are given.

2 path-tracking control for DDWMR

In this section, we present a basic two-layer observer-based path tracking controller for a differential-driven wheeled mobile robot (DDWMR). This will be the platform where subsequent pruning algorithm and FDIA are implemented. Figure. 1 shows the schematic of the DDWMR considered in this paper.

The dynamic and kinematic models of DDWMR are given

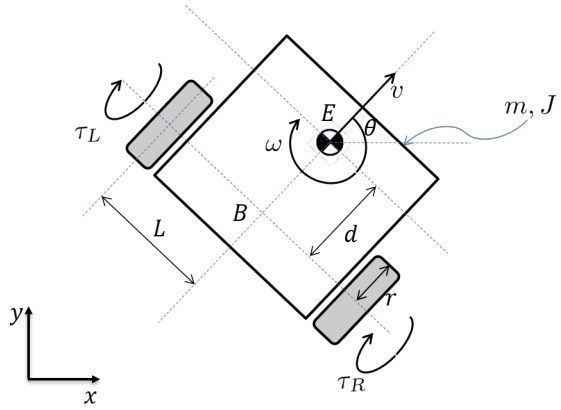

Figure 1. Schematic Diagram of the Considered DDWMR Showing Relevant Kinematic and Geometric Quantities

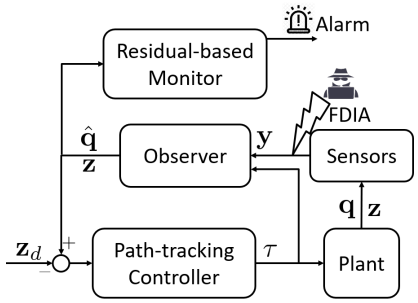

Figure 2. Schematic Diagram of the two-layer observer based control system and the attack injection

by [24]:

$$\begin{aligned}\dot{\mathbf{q}} &= M^{-1}(-D\mathbf{q}+B\tau)+\mathbf{w} \triangleq g(\mathbf{x},\mathbf{u})+\mathbf{w}\\ \begin{bmatrix}\dot{\theta}\\ \cdots\\ \dot{\mathbf{z}}\end{bmatrix} &= \begin{bmatrix}0 & 1\\ \cdots & \\ C(\theta) & \end{bmatrix}\mathbf{q} \triangleq \bar{C}(\theta)\mathbf{q},\end{aligned} \tag{1}$$

where, $\mathbf{q} = [v \;\; \omega]^\top$ is the generalized body velocities vector, $\mathbf{u} \triangleq \tau = [\tau_R \;\; \tau_L]^\top$ is a vector of the wheels torques, and $\mathbf{z} = [x \;\; y]^\top$ is the task-space position vector, $\mathbf{x} = [\theta \;\; v \;\; \omega]^\top$ is defined as a state vector, $\mathbf{w} \sim \mathcal{N}(0,R)$ is the process noise in dynamics.

The kinematic and dynamical parameters are given by:

$$\begin{aligned}M &= \begin{bmatrix}m & 0\\ 0 & md^2+J\end{bmatrix},\;\; D = \begin{bmatrix}0 & -md\omega\\ md\omega & 0\end{bmatrix}\\ B &= \frac{1}{r}\begin{bmatrix}1 & 1\\ L & -L\end{bmatrix},\;\; C(\theta) = \begin{bmatrix}\cos(\theta) & -d\sin(\theta)\\ \sin(\theta) & d\cos(\theta)\end{bmatrix}.\end{aligned}$$

Given a reference task-space trajectory $[\theta_d(t) \;\; \mathbf{z}_d(t)^\top]^\top$, where $\mathbf{z}_d(t) \in \mathbb{R}^2$ is the corresponding planar Cartesian coordinates of the desired trajectory. We assume that $\mathbf{z}_d(t)$ is continuously differentiable with bounded derivatives, and that all its derivative up to the 2nd order are known. Next, consider the tracking error given by

$$\widetilde{\mathbf{e}} = \begin{bmatrix}\theta-\theta_d\\ \mathbf{z}-\mathbf{z}_d\end{bmatrix} = \begin{bmatrix}\mathbf{e}_\theta\\ \mathbf{e}_\mathbf{z}\end{bmatrix}. \tag{2}$$

Then, the control law is then designed as:

$$\tau = B^{-1}(M\mathbf{u}+D\mathbf{q}), \tag{3}$$

where,

$$\mathbf{u} = -k_q(\mathbf{q}-\mathbf{q}_d)+\dot{\mathbf{q}}_d-\bar{C}(\theta)^\top\widetilde{\mathbf{e}}$$

with

$$\begin{aligned}\mathbf{q}_d &= C^{-1}(\theta)(\dot{\mathbf{z}}_d-k_e\mathbf{e}_\mathbf{z})\\ \dot{\mathbf{q}}_d &= -k_e(\dot{C}^{-1}(\theta)\mathbf{e}_\mathbf{z}+\mathbf{q})+C^{-1}(\theta)[\ddot{\mathbf{z}}_d+(k_e+C(\theta)\dot{C}^{-1}(\theta))\dot{\mathbf{z}}_d]\end{aligned}$$

and k_q, k_e are positive scalar control gains.

Proposition 1. *Consider the control law given in (3), if control gains $k_q > 0$ and $k_e > 0$, then the tracking errors in (2) converges to zero asymptotically. Moreover, the generalized velocities tracking error $\widetilde{\mathbf{q}} = \mathbf{q}-\mathbf{q}_d$ converges to zero asymptotically with $\dot{\mathbf{z}}_d = C(\theta)\mathbf{q}_d$ satisfied in the limit.*

Proof. Consider the candidate Lyapunov function:

$$V = \frac{1}{2}\|\widetilde{\mathbf{q}}\|^2+\frac{1}{2}\|\widetilde{\mathbf{e}}\|^2 \tag{4}$$

taking the first time derivative and substituting (1), (2), (3) yields

$$\begin{aligned}\dot{V} =& \widetilde{\mathbf{q}}^\top\left(-k_q\widetilde{\mathbf{q}}-\begin{bmatrix}0\\ \mathbf{e}_\theta\end{bmatrix}-C(\theta)\mathbf{e}_\mathbf{z}\right)+\mathbf{e}_\theta^\top\dot{\mathbf{e}}_\theta+\mathbf{e}_\mathbf{z}^\top\left(C(\theta)\mathbf{q}_d-\dot{\mathbf{z}}_d\right)\\ =& -k_q\|\widetilde{\mathbf{q}}\|^2-(\omega-\omega_d)\mathbf{e}_\theta-\mathbf{e}_\mathbf{z}^\top C(\theta)(\mathbf{q}-\mathbf{q}_d)+\mathbf{e}_\theta^\top\dot{\mathbf{e}}_\theta\\ &+\mathbf{e}_\mathbf{z}^\top(C(\theta)\mathbf{q}-\dot{\mathbf{z}}_d)\\ =& -k_q\|\widetilde{\mathbf{q}}\|^2+\mathbf{e}_\mathbf{z}^\top(C(\theta)\mathbf{q}_d-\dot{\mathbf{z}}_d)\\ =& -k_q\|\widetilde{\mathbf{q}}\|^2-k_e\|\mathbf{e}_\mathbf{z}\|^2\end{aligned} \tag{5}$$

This implies that $\dot{V}$ is negative semi-definite, and since V is positive, it follows that $V \in \mathcal{L}_\infty$. From (4), it follows that $\widetilde{\mathbf{q}}, \widetilde{\mathbf{e}} \in \mathcal{L}_\infty$, which also implies that $\mathbf{e}_\theta \in \mathcal{L}_\infty$.

Integrating (5) yields

$$V - V(0) \leq -\int_0^t \left(k_q \|\widetilde{\mathbf{q}}(\tau)\|^2 + k_e \|\mathbf{e}_\mathbf{z}(\tau)\|^2\right) d\tau$$

from which it follows that $\widetilde{\mathbf{q}}, \mathbf{e}_\mathbf{z} \in \mathcal{L}_2$. Also, $\dot{\widetilde{\mathbf{q}}} = -k_q \widetilde{\mathbf{q}} - \bar{C}(\theta)^\top \widetilde{\mathbf{e}} \in \mathcal{L}_\infty$ and $\dot{\widetilde{\mathbf{e}}} = \bar{C}(\theta)\widetilde{\mathbf{q}} - k_e \begin{bmatrix} 0 \\ \mathbf{e}_\mathbf{z} \end{bmatrix} \in \mathcal{L}_\infty$, which implies that $\widetilde{\mathbf{e}}$ and $\widetilde{\mathbf{q}}$ are uniformly continuous. Thus, by Barbalat's Lemma [25], it follows that

$$\widetilde{\mathbf{e}}(t) \to 0, \widetilde{\mathbf{q}}(t) \to 0$$

3 False data injection attack

An attacker can inject false data computed based on a partial or complete knowledge of system model, in order to covertly and accurately change the physical behavior of the plant [26]. This section gives the notion of a monitor used in this paper. Based on the monitor, we give a design of FDIA algorithm while assuming an attacker has complete knowledge of system.

For the DDWMR described in previous section, we consider a redundant measurement system of the form:

$$\mathbf{y} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1/4r & L/4r \\ 1/4r & -L/4r \\ \cos(\theta) & -d\sin(\theta) \\ \sin(\theta) & d\cos(\theta) \end{bmatrix} \cdot \mathbf{q} + \mathbf{v} \triangleq f(\mathbf{x}) + \mathbf{v} \tag{6}$$

consisting of both linear and nonlinear components, where $\mathbf{x} = [\theta \;\; v \;\; \omega]^\top$ is defined as a state vector, and $\mathbf{v}$ denotes measurement noises.

Definition 1 (Residual-based Monitor of Horizon T). *Based on the closed-loop system in Figure. 2, a monitor scheme is any mapping of the form:*

$$\Psi_T : \{Y_T, U_T\} \mapsto \{\Psi_1, \Psi_2\}$$

where, $Y_T = \in \mathbb{R}^{m \times T}, U_T \in \mathbb{R}^{l \times T}$ are historical measurements and controlled inputs for T horizon respectively, $\Psi_1 = \{0(safe), 1(unsafe)\}$ is the first output argument indicating whether or not the data contains attacks, $\Psi_2 = 2^{\{1,2,\cdots,m\}}$ is the second output argument indicating the support of attacks' location.

The monitor outputs $\Psi_1 = \{0\}$ for any measurement vector history $\mathbf{Y}_T = [\mathbf{y}_k, \mathbf{y}_{k-1}, \cdots, \mathbf{y}_{k-T+1}]$ and corresponding control history $\mathbf{U}_T = [\tau_{k-1} \;\; \tau_{k-2} \cdots \tau_{k-T}]$ if there exists estimate history $\hat{\mathbf{X}}_T = [\hat{\mathbf{q}}_k, \hat{\mathbf{q}}_{k-1}, \cdots, \hat{\mathbf{q}}_{k-T}]$ such that

$$\begin{aligned} \|\hat{\mathbf{q}}_{j+1} - g(\hat{\mathbf{q}}_j, \tau_j)\| \leq \varepsilon_w, \quad j = k-T, \cdots, k-1 \\ \|\mathbf{y}_j - f(\hat{\mathbf{q}}_j)\| \leq \varepsilon_v, \quad j = k-T+1, \cdots, k \end{aligned}$$

where ε_w and ε_v are any real numbers related to process noise and measurement noise.

Otherwise, the monitor outputs $\Psi_1 = \{1\}$ and the support of the sparsest attack vector history $E_T = \{\mathbf{e}_k, \mathbf{e}_{k-1}, \cdots, \mathbf{e}_{k-T+1}\}$ such that

$$\begin{aligned} \|\hat{\mathbf{q}}_{j+1} - g(\hat{\mathbf{q}}_j, \tau_j)\| \leq \varepsilon_w, \quad j = k-T, \cdots, k-1 \\ \|\mathbf{y}_j - f(\hat{\mathbf{q}}_j) - \mathbf{e}_j\| \leq \varepsilon_v, \quad j = k-T+1, \cdots, k \end{aligned}$$

After linearizing (6) about the operating point $\mathbf{x}_0 = [\theta_0 \;\; v_0 \;\; \omega_0]^\top$, we discretize it using Euler's approximation with a sampling time T_s, and iterate forward T_f samples, one obtains:

$$Y_f = H\mathbf{x}_k + G\mathbf{u}_f + e \tag{7}$$

where, $Y_f = \begin{bmatrix} \mathbf{y}_k & \mathbf{y}_{k+1} & \cdots & \mathbf{y}_{k+T_f} \end{bmatrix}^\top$,

$$H = \begin{bmatrix} C_d \\ C_d A_m \\ C_d A_m^2 \\ \vdots \\ C_d A_m^{T_f} \end{bmatrix}, G = T_s \begin{bmatrix} 0 & 0 & \cdots & 0 \\ C_d B_m & 0 & \cdots & 0 \\ C_d A_m B_m & C_d B_m & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ C_d A_m^{T_f-1} B_m & C_d A_m^{T_f-2} B_m & \cdots & C_d B_m \end{bmatrix}$$

with

$$A_m = I + T_s \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 2d\omega_0 \\ 0 & -\frac{md\omega_0}{md^2+J} & -\frac{mdv_0}{md^2+J} \end{bmatrix}, \quad B_m = T_s \begin{bmatrix} 0 \\ M^{-1}B \end{bmatrix},$$

$$C_d = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1/4r & L/4r \\ 0 & 1/4r & -L/4r \\ -v_0\sin(\theta_0) - d\omega_0\cos(\theta_0) & \cos(\theta_0) & -d\sin(\theta_0) \\ v_0\cos(\theta_0) + d\omega_0\sin(\theta_0) & \sin(\theta_0) & -d\cos(\theta_0) \end{bmatrix}$$

Let H admits the singular value decomposition:

$$H = [U_1 \;\; U_2] \begin{bmatrix} \sum_1 \\ 0 \end{bmatrix} V,$$

where, $U_1 \in \mathbb{R}^{m\times n}$, $U_2 \in \mathbb{R}^{m\times(m-n)}$, $\sum_1 = \text{diag}(\sigma_1, \sigma_2, \cdots, \sigma_n)$, and $V \in \mathbb{R}^{n\times n}$, it is obvious that, the FDIA would pass the monitor if the attack vector $\mathbf{e}$ is defined such that the attack measurement $\mathbf{y}_a$ is in the *range space* of the observation matrix H ($= \mathsf{Range}(U_1)$). Consequently, the FDIA is generated by solving the optimization problem:

$$\begin{aligned} \mathsf{Maximize} \quad & \|{U_1}_{\mathcal{T}_\cdot}{}^\top \mathbf{y}_A\|^2 \\ \mathsf{Subject\ to} \quad & \|{U_2}_{\mathcal{T}_\cdot}{}^\top \mathbf{y}_A\|^2 \le \alpha \end{aligned} \tag{8}$$

for a given support $\mathcal{T}$ of attack locations under upper bound of percentage of attack injection, and α is a threshold value related to observation matrix H and monitor's threshold ε_v.

4 Resilient pruning observer design

Data-driven attack localization algorithms [27, 28] are effective ways of achieving resiliency under FDIA. However, it is challenging to correctly locate all attacked nodes due to the fundamental inexactness associated with data-driven algorithms. In this section, we propose a pruning algorithm to improve the accuracy of localization algorithms. The underlying philosophy is that if the measurement set is sufficiently redundant, a subset with reduced attacked percentage can be obtained by systematically pruning the measurement set. If the attack percentage is reduced to 0, the pruned measurement set is then used with UKF to produce an improved resilient state estimation under FDIA.

Let the unknown actual support of safe measurements be $\mathcal{T}^c = supp(\mathbb{1} - \mathbf{e})$ with an indicator vector $\mathbf{q}$ given, elementwise, as:

$$\mathbf{q}_i = \begin{cases} 1 & \text{if } \; i \in \mathcal{T}^c \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

Suppose the localization oracle gives an estimated support $\hat{\mathcal{T}}^c$ with $\hat{\mathbf{q}}$. Then, the disagreement between the oracle and the actual support can be modeled as:

$$\mathbf{q}_i = \varepsilon_i \hat{\mathbf{q}}_i + (1-\varepsilon_i)(1-\hat{\mathbf{q}}_i), \tag{10}$$

where ε_i depicts the agreement between the estimated and actual support as follows:

$$\varepsilon_i = \begin{cases} 1 \;\; \text{if } \hat{\mathbf{q}}_i = \mathbf{q}_i \\ 0 \;\; \text{if } \hat{\mathbf{q}}_i = 1 - \mathbf{q}_i \end{cases} \tag{11}$$

It is assumed that $\varepsilon_i \sim \mathcal{B}(1, p_i)$, where p_i is given by the true positive rate from the oracle ROC statistics. Moreover, one can see that $\sum_{i=1}^m \varepsilon_i$ is Poisson-Binomially distributed with probability mass function given by:

$$\mathsf{Pr}\left(\sum_{i=1}^m \varepsilon_i = k-1\right) = \mathbf{r}(k), k = 1, \cdots, m+1 \tag{12}$$

where [29], $\mathbf{r} = \prod_{i=1}^m P_i \cdot \begin{bmatrix} \frac{1-P_1}{P_1} \\ 1 \end{bmatrix} * \begin{bmatrix} \frac{1-P_2}{P_2} \\ 1 \end{bmatrix} * \cdots * \begin{bmatrix} \frac{1-P_m}{P_m} \\ 1 \end{bmatrix}$, $\mathbf{r} \in \mathbb{R}_{m+1}$.

Thus, given a reliability level $\eta \in (0,1)$, we define the maximum integer $l_\eta \le m$ for which oracle will correctly localize at least l_η nodes with a probability of at least η:

$$\begin{aligned} l_\eta &= \max\left\{k \middle| \mathsf{Pr}\left(\sum_{i=1}^m \varepsilon_i \ge k\right) \ge \eta\right\} \\ &= \max\left\{k \middle| 1 - \sum_{i=1}^{k+1} \mathbf{r}_i \ge \eta\right\} \\ &= \max\left\{k \middle| \sum_{i=1}^{k+1} \mathbf{r}_i \le 1 - \eta\right\} \end{aligned} \tag{13}$$

Next, we retain the oracle output for the first l_η most trusted nodes. Let $\mathbf{s} \in [0,1]^m$ be a vector of confidence values for the oracle output for each node, then a robust support can be estimated as:

$$\hat{\mathcal{T}}_\eta^c = \hat{\mathcal{T}}^c \cap \left\{\mathsf{argsort}\downarrow (\mathbf{p} \circ \mathbf{s})\right\}_1^{l_\eta}. \tag{14}$$

Remark 1. *(13) and (14) constitute a pruning scheme for which the resulting $\hat{\mathcal{T}}_\eta^c$ excludes all attacked channel with a probability larger than η,*

$$Pr\{\hat{\mathcal{T}}_\eta^c \cap \mathcal{T} = \emptyset\} \ge \eta.$$

Following the pruning operation, the safe measurement model used for a UKF is:

$$\mathbf{y}_{\hat{\mathcal{T}}_\eta^c} = f_{\hat{\mathcal{T}}_\eta^c}(\mathbf{x}) + \mathbf{v}_{\hat{\mathcal{T}}_\eta^c}. \tag{15}$$

Following standard unscented transformation [30], we use $2n+1$ sigma points to approximate the n-dimensional normally distributed state $\mathbf{x}$ with assumed mean $\bar{\mathbf{x}}$ and covariance $P_\mathbf{x}$ as follows:

$$\begin{aligned} &\chi_0 = \bar{\mathbf{x}} \\ &\chi_i = \bar{\mathbf{x}} + (\sqrt{(\lambda+n)P_\mathbf{x}})_i, \;\; i = 1, \cdots, n \\ &\chi_{i+n} = \bar{\mathbf{x}} + (\sqrt{(\lambda+n)P_\mathbf{x}})_{i-n}, \;\; i = n+1, \cdots, 2n \end{aligned}$$

The corresponding weights for the sigma points are then given by:

$$W_0^m = \lambda/(n+\lambda), W_0^c = W_0^m + (1-\alpha^2+\beta)$$
$$W_i = 1/2(L+\lambda)$$

where, $\lambda = \alpha^2(n+\kappa) - n$ represents how far the sigma points are away from the state, $\kappa \geq 0, \alpha \in (0,1]$, and $\beta = 2$ is the optimal choice for Gaussian distribution.

Assume $\mathbf{x}_{k-1} \sim \mathcal{N}(\bar{\mathbf{x}}_{k-1}, P_{\mathbf{x},k-1})$, sigma points update through time in sequence with the pruning measurement model in (15). Moreover, according to the corresponding weight, we can predict the new time step state and calculate the new error covariances between the sigma points and the predicted state as follow:

$$\mathcal{X}_k^\star = g(\mathcal{X}_{k-1}, L_{\hat{\mathcal{T}}_\eta^c}(\hat{\mathbf{x}}_k))$$
$$\hat{\mathbf{x}}_k^- = \sum_{i=0}^{2n} W_i \mathcal{X}_{k,i}^\star$$
$$\hat{P}_{\mathbf{x},k} = \sum_{i=0}^{2n} W_i (\mathcal{X}_{k,i}^\star - \hat{\mathbf{x}}_k)(\mathcal{X}_{k,i}^\star - \hat{\mathbf{x}}_k)^T + R$$
$$\mathcal{Y}_{k,\hat{\mathcal{T}}_\eta^c} = f_{\hat{\mathcal{T}}_\eta^c}(\mathcal{X}_k)$$

Next, the measurements and Kalman gains updates are given by:

$$\hat{\mathbf{y}}_{k,\hat{\mathcal{T}}_\eta^c} = \sum_{i=0}^{2n} W_i \mathcal{Y}_{(k,i),\hat{\mathcal{T}}_\eta^c}$$
$$\hat{P}_{\mathbf{y},k} = \sum_{i=0}^{2n} W_i (\mathcal{Y}_{(k,i),\hat{\mathcal{T}}_\eta^c} - \hat{\mathbf{y}}_{k,\hat{\mathcal{T}}_\eta^c})(\mathcal{Y}_{(k,i),\hat{\mathcal{T}}_\eta^c} - \hat{\mathbf{y}}_{k,\hat{\mathcal{T}}_\eta^c})^T + Q$$
$$\hat{P}_{\mathbf{xy}} = \sum_{i=0}^{2n} W_i (\mathcal{X}_{k,i}^\star - \hat{\mathbf{x}}_k)(\mathcal{Y}_{(k,i),\hat{\mathcal{T}}_\eta^c} - \hat{\mathbf{y}}_{k,\hat{\mathcal{T}}_\eta^c})^T$$
$$\mathbf{K}_k = \hat{P}_{\mathbf{xy}} \hat{P}_{\mathbf{y},k}^{-1}$$
$$\bar{\mathbf{x}}_k = \hat{\mathbf{x}}_k + \mathbf{K}_k(\mathbf{y}_{k,\hat{\mathcal{T}}_\eta^c} - \hat{\mathbf{y}}_{k,\hat{\mathcal{T}}_\eta^c}), \quad P_{\mathbf{x},k} = \hat{P}_{\mathbf{x},k} - \mathbf{K}_k \hat{P}_{\mathbf{y},k} \mathbf{K}_k^T$$

where, Q and R are the measurement and process noise covariance matrices respectively.

In order to numerically verify that the robust support generated by (14) can achieve 100% localization with a probability of at least η, we implemented the pruning localization algorithm in a numerical simulation with time-varying FDIAs. The results Figure. 3 shows that the algorithm achieves 100% localization even for reliability setting $\eta = 0.5$! When the reliability is set to just 0.1, this algorithm misses only two attacked measurement nodes.

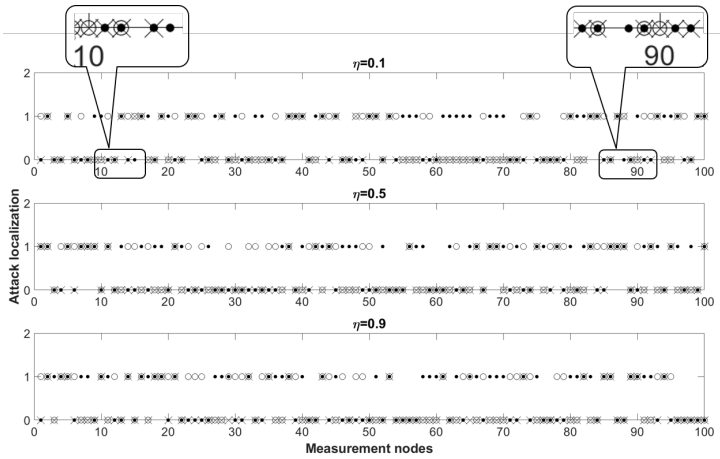

Figure 3. Numerical Simulation of pruning algorithm with time-varying FDIAs with $\eta = 0.1$, $\eta = 0.5$ and $\eta = 0.9$ (**cross** $\rightarrow$ pruning, **circle** $\rightarrow$ oracle, **dots at 0** $\rightarrow$ attacked nodes, the perfect result is all dots at 0 are covered)

5 Simulation

In this section, numerical simulation is carried out for DDWMR using three observer strategies under FDIA and the resulting path tracking performance and estimated inner states are compared. The observers compared are: (1) Only UKF, (2) UKF combine directly with the oracle and (3) the proposed pruning-based UKF. For the path-tracking control system, the control gains are set as $k_1 = k_2 = 10$. The nominal performance of the control system with UKF in an attack-free setting is shown in Figure 4. It is seen that the control system, together with UKF, performs well when measurement contains no attack. Next, a FDIA is implemented and the generated attack vector is added to the system measurements. The oracle is simulated based on the uncertainty model in (10) with defined true positive rate $r_p = 0.6$ and confidence for each node localization $s = 0.5$. Localization results were then generated to match the specified ROC statistics. The pruning algorithm is implemented with $\eta = 0.8$. The codes for simulation can be found in https://github.com/ZYblend/Resilient-Pruning-Observer-against-False-Data-Injection-Attacks.

Figures 5, 6 and 7 show the comparison of the performance of three observer strategies under FDIA: "*only UKF*", "*UKF with machine learning*" and "*pruning observer*. The results show that robot cannot track the trajectory under FDIA without any localization and pruning operation, and the estimated dynamic states has very large deviation from the true states. With the oracle, due to the uncertainty, the tracking path is very oscillatory although not as bad as with UKF alone. However, with the proposed observer, the robot was able to track the reference path very closely and smoothly.

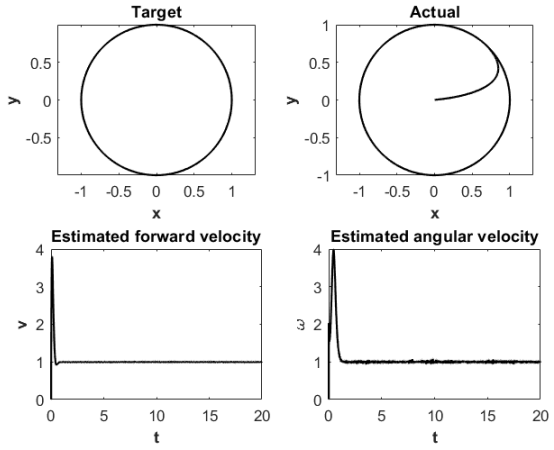

Figure 4. Path-tracking and state estimation results of the proposed control system without attacks

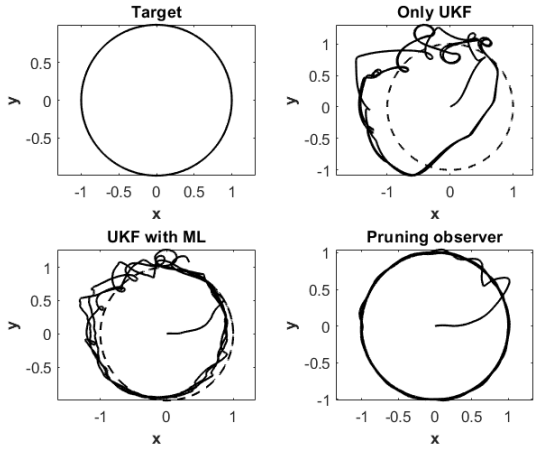

Figure 5. A comparison of path tracking results. The proposed pruning observer-based control scheme is able to focus robot to track better, while UKF cannot handle the attacks and machine learning cannot smooth the trajectory. (dot line: reference trajectory, solid line: actual path)

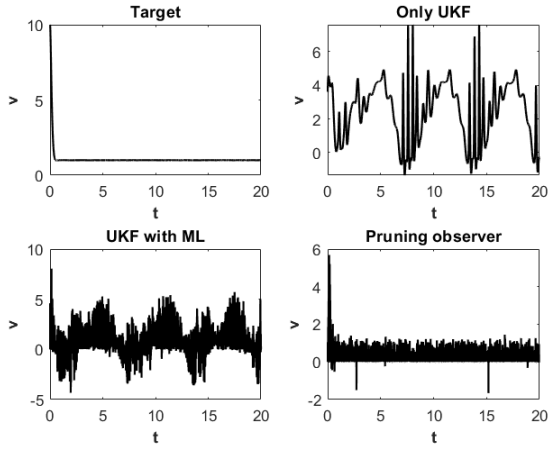

Figure 6. A comparison of estimated forward velocity. The proposed pruning observer gives more stable and accurate estimation.

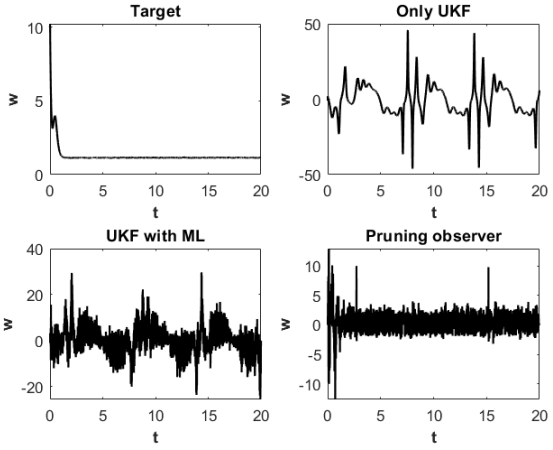

Figure 7. A comparison of estimated angular velocity. The proposed pruning observer gives more stable and accurate estimation.

6 Conclusion

In this paper, an attack-resilient path tracking control scheme for wheeled mobile robot under an optimization-based FDIA was designed. The main contributions include: (1) Stable path-tracking control system for DDWMR, (2) Optimization-based FDIA for DDWMR, and (3) The pruning-based observer design using UKF as the underlying observer. It was shown that the proposed pruning-based observer significantly improves the signal-to-attack ratio such that the UKF is able to resiliently estimate the state of the DDWMR even when portion of the sensor measurements were subject to an FDIA. Although this paper shows how promising the resiliency boosting through pruning algorithm is, the results presented only represent the initial stages of this development. Hence there are several open problems that need to be addressed. We name a few:

1. As with other resilient observers, the pruning-based resilient observer relies heavily on the inherent redundancy in the measurement system [31]. However, there is no systematic way to quantify the level of redundancy required given any oracle. With ℓ_1-based methods, the RIP property partly provide answers to this question. What would be interesting to see is how much of a relaxation do we get on the RIP

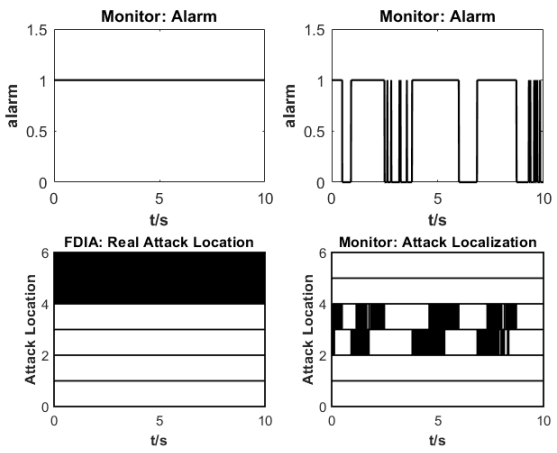

Figure 8. FDIAs are localized wrongly by residual-based monitor

requirements by including pruning? Partial answer to this question can be found in [32]. We plan to expand on the results as it applies to this problem.

2. It would be beneficial to see some results on the potential gain by combining pruning and ℓ_1-based methods.
3. There are indications from this paper that it is possible to combine pruning directly with the update laws of Kalman filtering algorithms. In future, we will develop a systematic way to achieve this.
4. We plan to generalize and identify the salient properties for a class of oracles that would combine well with a given underlying estimator.

ACKNOWLEDGMENT

Thanks to Florida State University and the Center for Advanced Power Systems for remote working support on this paper during the COVID-19 outbreak. The authors wish everyone safety in these difficult times.

REFERENCES

[1] Roy, S., Nandy, S., Ray, R., and Shome, S. N., 2015. "Robust path tracking control of nonholonomic wheeled mobile robot: Experimental validation". *International Journal of Control, Automation and Systems,* ***13***(4), pp. 897–905.

[2] Kim, D.-H., and Oh, J.-H., 1999. "Tracking control of a two-wheeled mobile robot using input-output linearization". *Control Engineering Practice,* ***7***(3), pp. 369–374.

[3] Oriolo, G., De Luca, A., and Vendittelli, M., 2002. "Wmr control via dynamic feedback linearization: design, implementation, and experimental validation". *IEEE Transactions on control systems technology,* ***10***(6), pp. 835–852.

[4] d'Andrea Novel, B., Bastin, G., and Campion, G., 1992. "Dynamic feedback linearization of nonholonomic wheeled mobile robots". In Proceedings 1992 IEEE International Conference on Robotics and Automation, IEEE, pp. 2527–2532.

[5] Dixon, W., Dawson, D., Zergeroglu, E., and Zhang, F., 2000. "Robust tracking and regulation control for mobile robots". *International Journal of Robust and Nonlinear Control: IFAC-Affiliated Journal,* ***10***(4), pp. 199–216.

[6] Aguiar, A. P., and Hespanha, J. P., 2007. "Trajectory-tracking and path-following of underactuated autonomous vehicles with parametric modeling uncertainty". *IEEE transactions on automatic control,* ***52***(8), pp. 1362–1379.

[7] Cortesão, R. P. D., 2003. "Kalman techniques for intelligent control systems: theory and robotics experiments". PhD thesis.

[8] Coelho, P., and Nunes, U., 2005. "Path-following control of mobile robots in presence of uncertainties". *IEEE Transactions on Robotics,* ***21***(2), pp. 252–261.

[9] Pajic, M., Weimer, J., Bezzo, N., Sokolsky, O., Pappas, G. J., and Lee, I., 2017. "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators". *IEEE Control Systems Magazine,* ***37***(2), pp. 66–81.

[10] Mo, Y., Garone, E., Casavola, A., and Sinopoli, B., 2010. "False data injection attacks against state estimation in wireless sensor networks". In 49th IEEE Conference on Decision and Control (CDC), IEEE, pp. 5967–5972.

[11] Mo, Y., and Sinopoli, B., 2010. "False data injection attacks in control systems". In Preprints of the 1st workshop on Secure Control Systems, pp. 1–6.

[12] Fawzi, H., Tabuada, P., and Diggavi, S., 2014. "Secure estimation and control for cyber-physical systems under adversarial attacks". *IEEE Transactions on Automatic control,* ***59***(6), pp. 1454–1467.

[13] Anubi, O. M., Konstantinou, C., and Roberts, R., 2019. "Resilient optimal estimation using measurement prior". *arXiv preprint arXiv:1907.13102*.

[14] Guo, P., Kim, H., Virani, N., Xu, J., Zhu, M., and Liu, P., 2017. "Exploiting physical dynamics to detect actuator and sensor attacks in mobile robots". *arXiv preprint arXiv:1708.01834*.

[15] Anubi, O. M., Mestha, L., and Achanta, H., 2018. "Robust resilient signal reconstruction under adversarial attacks". *arXiv preprint arXiv:1807.08004*.

[16] Candes, E. J., and Tao, T., 2005. "Decoding by linear programming". *IEEE transactions on information theory,* ***51***(12), pp. 4203–4215.

[17] Candes, E. J., Romberg, J. K., and Tao, T., 2006. "Stable signal recovery from incomplete and inaccurate measurements". *Communications on Pure and Applied Mathematics: A Journal Issued by the Courant Institute of Mathe-*

matical Sciences, ***59***(8), pp. 1207–1223.

[18] Pajic, M., Lee, I., and Pappas, G. J., 2016. "Attack-resilient state estimation for noisy dynamical systems". *IEEE Transactions on Control of Network Systems,* ***4***(1), pp. 82–92.

[19] Candes, E. J., et al., 2008. "The restricted isometry property and its implications for compressed sensing". *Comptes rendus mathematique,* ***346***(9-10), pp. 589–592.

[20] Mestha, L. K., Anubi, O., and John, J. V., 2019. Cyber-attack detection, localization, and neutralization for unmanned aerial vehicles, Aug. 22. US Patent App. 15/899,903.

[21] Wang, X., and Yaz, E. E., 2014. "Stochastically resilient extended kalman filtering for discrete-time nonlinear systems with sensor failures". *International Journal of Systems Science,* ***45***(7), pp. 1393–1401.

[22] Mahmoud, M., 2007. "Resilient $\mathcal{L}_2$–$\mathcal{L}_\infty$ filtering of polytopic systems with state delays". *IET Control Theory & Applications,* ***1***(1), pp. 141–154.

[23] Qu, X., and Zhou, J., 2013. "The optimal robust finite-horizon kalman filtering for multiple sensors with different stochastic failure rates". *Applied Mathematics Letters,* ***26***(1), pp. 80–86.

[24] Dhaouadi, R., and Hatab, A. A., 2013. "Dynamic modelling of differential-drive mobile robots using lagrange and newton-euler methodologies: A unified framework". *Advances in Robotics & Automation,* ***2***(2), pp. 1–7.

[25] Barbalat, I., 1959. "Systemes d'équations différentielles d'oscillations non linéaires". *Rev. Math. Pures Appl,* ***4***(2), pp. 267–270.

[26] de Sá, A. O., d. C. Carmo, L. F. R., and Machado, R. C. S., 2017. "Covert attacks in cyber-physical control systems". *IEEE Transactions on Industrial Informatics,* ***13***(4), Aug, pp. 1641–1651.

[27] Abbaszadeh, M., Mestha, L. K., Bushey, C., and Holzhauer, D. F., 2019. Automated attack localization and detection, Sept. 17. US Patent 10,417,415.

[28] Sabbah, E., Majeed, A., Kang, K.-D., Liu, K., and Abu-Ghazaleh, N., 2006. "An application-driven perspective on wireless sensor network security". In Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks, pp. 1–8.

[29] Fernandez, M., and Williams, S., 2010. "Closed-form expression for the poisson-binomial probability density function". *IEEE Transactions on Aerospace and Electronic Systems,* ***46***(2), April, pp. 803–817.

[30] Julier, S. J., and Uhlmann, J. K., 1997. "New extension of the kalman filter to nonlinear systems". In Signal processing, sensor fusion, and target recognition VI, Vol. 3068, International Society for Optics and Photonics, pp. 182–193.

[31] Zhang, Q., Yu, T., and Ning, P., 2006. "A framework for identifying compromised nodes in sensor networks". In 2006 Securecomm and Workshops, IEEE, pp. 1–10.

[32] Vaswani, N., and Lu, W., 2010. "Modified-cs: Modifying compressive sensing for problems with partially known support". *IEEE Transactions on Signal Processing,* ***58***(9), pp. 4595–4607.