2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)
September 27 - October 1, 2021. Prague, Czech Republic

2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) | 978-1-6654-1714-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/IROS51168.2021.9635899

Detection and Inference of Randomness-based Behavior for Resilient Multi-vehicle Coordinated Operations

Paul J Bonczek and Nicola Bezzo

***Abstract*— A resilient multi-vehicle system cooperatively performs tasks by exchanging information, detecting, and removing cyber attacks that have the intent of hijacking or diminishing performance of the entire system. In this paper, we propose a framework to: i) detect and isolate misbehaving vehicles in the network, and ii) securely encrypt information among the network to alert and attract nearby vehicles toward points of interest in the environment without explicitly broadcasting safety-critical information. To accomplish these goals, we leverage a decentralized virtual spring-damper mesh physics model for formation control on each vehicle. To discover inconsistent behavior of any vehicle in the network, we consider an approach that monitors for changes in sign behavior of an inter-vehicle residual that does not match with an expectation. Similarly, to disguise important information and trigger vehicles to switch to different behaviors, we leverage side-channel information on the state of the vehicles and characterize a hidden spring-damper signature model detectable by neighbor vehicles. Our framework is demonstrated in simulation and experiments on formations of unmanned ground vehicles (UGVs) in the presence of malicious man-in-the-middle communication attacks.**

I. Introduction

The use of coordinated multi-vehicle systems to perform various tasks has been extensively explored for many years [1]–[4]. By leveraging multiple vehicles instead of only one, it is possible to perform more operations, and complete a task faster and more efficiently. Examples of such operations that can benefit from the use of multi-vehicle systems are search and rescue operations [1] depicted in Fig. 1, surveillance [2], military convoying/platooning [3], and exploration missions [4]. Generally, approaches that leverage multi-vehicle systems assume that all vehicles are cooperative while performing the desired operations to maintain swarming formations and can exchange all necessary information to achieve the desired goal. However, these vehicles are susceptible to malicious external attacks, especially on their communication infrastructure, which can affect the entire network performance. For example, with a Man-In-The-Middle (MITM) attack [5], an attacker intercepts a communication broadcast and replaces it with altered data which are then received by neighboring vehicles. Successful attackers are able to purposefully block important information from being received by nearby vehicles in the formation or control the entire multi-vehicle network to an undesired location.

Safety-critical information, if not properly encrypted, can also be intercepted creating further security issues. Although encryption techniques can be deployed, there exists attacks that are capable of discovering encryption keys to extract data. The most secure option is to avoid exchanging data altogether. In this work we propose to leverage side-channel information that contains hidden data, which is unknown to malicious attackers. For example, if a vehicle discovers an object of interest whose identity needs to be kept secret, as depicted in Fig. 1, it could perform a certain signature motion (similar to watermarking [6]) to indicate to neighboring vehicles of the discovered object. This motion triggers the surrounding vehicles to infer its position and switch tasks to get attracted to the same object. In this way, a vehicle can collect data and infer the behavior of other vehicles without explicitly broadcasting important information. With such premises, in this work we focus on applications for cooperative autonomous vehicle networks in the presence of adversaries. We expand on literature that leverage virtual springs for decentralized formation control [7]–[10] while introducing a monitoring approach to detect inconsistent behaviors between expected and received data to provide: 1) resiliency to cyber-attacks on communication broadcasts and 2) discovery of a hidden signature via side-channel states.

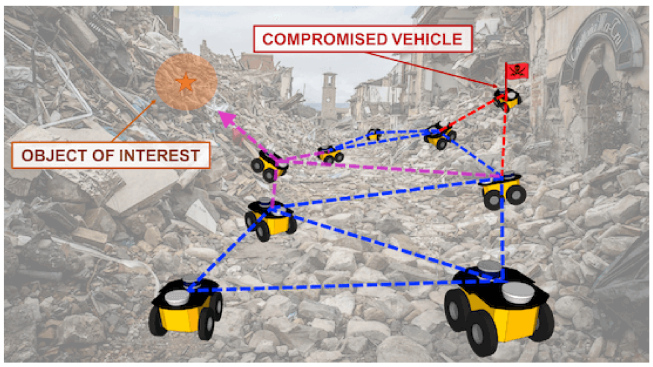

Fig. 1. Pictorial motivation of the problem in this paper in which a multi-vehicle system cooperatively performs a task while inferring the objective of other teammates and detecting if they are compromised by cyber-attacks.

A. Related Work

Analyzing the literature on the area of multi-vehicle resilience, we find works employing the Mean Subsequence Reduced (MSR) algorithm that provides resiliency to F number of uncooperative agents while still reaching a consensus of a specific value [11], [12]. While this is the standard resilient consensus algorithm to agree on a specific value (e.g., heading angle) for teams of mobile robots, it does not provide resilience to misbehaving vehicles within time-varying proximity-based formations.

Similar to previous literature, our proposed work leverages a residual-based detection technique for attack detection [13]–[18]. Authors in [19] leverage the residual-based *Cumulative Sum* (CUSUM) detection procedure to discover spoofs

Paul J Bonczek and Nicola Bezzo are with the Charles L. Brown Department of Electrical and Computer Engineering, and Link Lab, University of Virginia, Charlottesville, VA 22904, USA. Email: {pjb4xn, nb6be}@virginia.edu

to on-board navigation systems of robots in multi-vehicle systems. In our previous work, we have characterized the *Cumulative Sign* (CUSIGN) detector [17] on a single vehicle, which is designed to detect non-random (i.e., inconsistent) *signed* residual behavior. We demonstrated the effectiveness of the randomness-based CUSIGN detector when compared to the magnitude-based CUSUM in the presence of *stealthy* sensor attacks that intentionally hide within noise profiles to remain undetected. Moreover, the fundamental component we want to convey is that noisy systems will follow an expected model behavior under nominal conditions, whereas systems that experience hijacking attempts from an attacker will exhibit contradictory behavior.

In this work, we extend our recent randomness-based detection techniques for sensor spoofing introduced in [17], [18] to detect attacks and hidden signatures in multi-vehicle systems. Specifically, each vehicle monitors the *inter-vehicle residual* —defined as the difference between received information and predicted values— using the CUSIGN detector to determine whether nearby vehicles are behaving as expected or not. Additionally, we propose a detection scheme to monitor a residual sign switching rate (i.e., the frequency of residual sign changes) to identify if nearby vehicles are displaying hidden signature behavior, by leveraging known stochastic properties of the system models.

To summarize, the objective of this work is: 1) to detect stealthy MITM attacks on communication broadcasts that leave behind inconsistent inter-vehicle residual behavior, and 2) to provide a method for the network to resiliently maintain operations, while 3) using hidden side-channels to communicate the discovery of an object to nearby vehicles without explicitly sending this information. The contribution of this work is twofold: 1) a detector for discovering inconsistent behavior from stealthy MITM communication attacks in multi-vehicle systems, and 2) a 'side-channel'-based scheme to produce and detect a hidden signature to protect critical information from being intercepted in communication broadcasts by attackers in multi-vehicle operations.

II. Preliminaries

Let us consider a multi-vehicle network of N homogeneous robots modeled as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where we denote $\mathcal{V} = \{1, \dots, N\}$ as the vehicle set and the edge set $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$, such that an edge $(i, j) \in \mathcal{E}$ indicates a connection from vehicle $i \in \mathcal{V}$ to vehicle $j \in \mathcal{V}$. All vehicles are considered to have second order dynamics that can be represented in a linear time-invariant (LTI) state space form:

$$\dot{\boldsymbol{x}}_i = \boldsymbol{A}\boldsymbol{x}_i + \boldsymbol{B}\boldsymbol{u}_i + \boldsymbol{\nu}_i, \quad \forall i \in \mathcal{V}, \tag{1}$$

where $\boldsymbol{A}$ and $\boldsymbol{B}$ denote state and input matrices, the state vector $\boldsymbol{x}_i \in \mathbb{R}^n$ consisting of positions $\boldsymbol{p}_i$ and velocities $\boldsymbol{v}_i = \dot{\boldsymbol{p}}_i$, and $\boldsymbol{\nu}_i \in \mathbb{R}^n$ representing zero-mean Gaussian process noise. Each vehicle $i \in \mathcal{V}$ within the vehicle network is controlled by a virtual spring-damper physics model as,

$$\boldsymbol{u}_i = \ddot{\boldsymbol{p}}_i = \Bigg[\sum_{j \in \mathcal{S}_i} \kappa_v (l_{ij} - l_v^0) \vec{\boldsymbol{d}}_{ij} - \sum_{o \in \mathcal{O}_i} \kappa_o (l_{io} - l_o^0) \vec{\boldsymbol{d}}_{io}, + \ \kappa_g l_{ig} \vec{\boldsymbol{d}}_{ig} \Bigg] - \gamma_v \dot{\boldsymbol{p}}_i \in \mathbb{R}^m, \tag{2}$$

where $\mathcal{S}_i \subset \mathcal{V}$ is the neighbor set of a vehicle i, $\mathcal{O}_i$ denotes the set of nearby obstacles, while l_v^0 and l_o^0 are desired rest lengths between the vehicle i and its neighbors and obstacles. The variables l_{ij}, l_{io}, l_{ig} represent euclidean distances (i.e., virtual spring lengths) and κ_v, κ_o, κ_g are spring constants between neighboring vehicles, obstacles, and the goal, respectively, while $\vec{\boldsymbol{d}}$ denotes the unit vector indicating direction of the forces. Given damping coefficients that satisfy $\gamma_v > 0$, the multi-vehicle system emulates a true spring-mass mesh where dissipating forces act against the velocities, leading to an equilibrium state of zero velocity in the absence of external forces. All vehicles are fitted with a range sensor providing 360 degree field of view with a limited range $\delta_r > 0$ for obstacle avoidance. Any vehicle i that comes within sensing range of an obstacle $o \in \mathcal{O}_i$ (with position $\boldsymbol{p}_o$) attaches a spring to it.

A. Connected Proximity-based Graph

In order for the vehicle network to cooperatively maintain the desired proximity-based formation in (2), the vehicles broadcast information that is received by any other vehicle within a maximum communication range $\delta_c > 0$.

***Definition** 1 (Communication Graph):* Given the N vehicles in set $\mathcal{V}$ with a maximum communication range δ_c, we define the graph $\mathcal{G}_\mathcal{C} = (\mathcal{V}, \mathcal{E}_\mathcal{C})$ with the following edge set,

$$\mathcal{E}_\mathcal{C} = \big\{(i, j) \mid \big\|\boldsymbol{p}_i - \boldsymbol{p}_j\big\| \leq \delta_c, \ i, j \in \mathcal{V}\big\}, \tag{3}$$

as the *communication graph* of the vehicle set $\mathcal{V}$.

Consequently, the set of all vehicles within communication range of a vehicle i, denoted as $\mathcal{C}_i \subseteq \mathcal{V}$, follows,

$$\mathcal{C}_i = \big\{j \in \mathcal{V} \ \big| \ (i, j) \in \mathcal{E}_\mathcal{C}\big\}. \tag{4}$$

All N vehicles are assumed to be equipped with localization/pose sensors represented in the output vector $\boldsymbol{y}_i^{(k)}$ by,

$$\boldsymbol{y}_i^{(k)} = \boldsymbol{C}\boldsymbol{x}_i^{(k)} + \boldsymbol{\eta}_i^{(k)} \in \mathbb{R}^{N_s}, \quad \forall i \in \mathcal{V}, \tag{5}$$

where $\boldsymbol{C}$ is the output matrix and $\boldsymbol{\eta}_i^{(k)} \in \mathbb{R}^{N_s}$ denotes zero-mean Gaussian measurement noise at every discrete time iteration $k \in \mathbb{N}$. A standard Kalman Filter with gain $\boldsymbol{K} \in \mathbb{R}^{n \times N_s}$ provides a state estimate $\hat{\boldsymbol{x}}_i^{(k)} \in \mathbb{R}^n$. To enable proximity-based formation control, each vehicle $i \in \mathcal{V}$ broadcasts its position estimate $\hat{\boldsymbol{p}}_i^{(k)}$ (within the state estimate vector) that is received by any nearby vehicles $j \in \mathcal{C}_i$. The neighbor set $\mathcal{S}_i$ in (2) is used to control the motion of each vehicle i and is computed following Gabriel Graph rule [20],

$$\mathcal{S}_i = \big\{j \in \mathcal{V} \setminus \mathcal{R}_i \ \big| \ \widehat{ihj} \leq \pi/2, \ j, h \in \mathcal{C}_i\big\}, \tag{6}$$

where $\widehat{ihj}$, $i \neq j \neq h$ is the interior angle within a three vehicle configuration obtained from the on-board position estimate $\hat{\boldsymbol{p}}_i^{(k)}$ and received position estimates $\hat{\boldsymbol{p}}_j^{(k)}$ and $\hat{\boldsymbol{p}}_h^{(k)}$ from vehicles $j, h \in \mathcal{C}_i$. The set $\mathcal{R}_i \subset \mathcal{V}$ is a subset of vehicles that are deemed compromised by vehicle i and not included in the control graph.

***Definition** 2 (Control Graph):* Given the vehicle set $\mathcal{V}$ with each vehicle $i \in \mathcal{V}$ having a neighbor set for control $\mathcal{S}_i \subseteq \mathcal{C}_i$ computed from the Gabriel Graph rule in (6), we define the graph $\mathcal{G}_\mathcal{U} = (\mathcal{V}, \mathcal{E}_\mathcal{U})$ with the edge set,

$$\mathcal{E}_\mathcal{U} = \big\{(i, j) \ \big| \ j \in \mathcal{S}_i, \forall i \in \mathcal{V}\big\}, \tag{7}$$

as the *control graph* of the vehicle set $\mathcal{V}$.

Construction of the control graph by leveraging the Gabriel Graph rule [20] allows for a connected graph without crossing edges and a uniform coverage (while maintaining desired distances between vehicles) of the network [7]–[10].

B. Attack Model

We assume the multi-vehicle network is navigating within an adversarial environment, such that individual vehicles may be subject to malicious communication attacks (e.g., MITM attacks [5]). In the case of an attack on an unprotected proximity-based formation, a single compromised vehicle can affect the entire network of N vehicles as the effects of the attack are propagated throughout the network. During a persistent communication attack, we assume that an attacker can continuously intercept and modify broadcast data with stealthy (i.e., hidden within the system noise profile) information in an attempt to intentionally fool (i.e., hijack) the vehicle network. Each vehicle i exchanges state estimates, nearby obstacle positions, and neighbor set information at every time instance k such that nearby vehicles have knowledge of its intended motion by construction of the network model in (2). We indicate the spoofed broadcast information from a vehicle $i \in \mathcal{V}$ that is received by other vehicles as:

$$\begin{aligned} \hat{\boldsymbol{x}}_i^{(k)} + \boldsymbol{\xi}_i^x &\longrightarrow \tilde{\hat{\boldsymbol{x}}}_i^{(k)}, \\ \boldsymbol{p}_o + \boldsymbol{\xi}_i^o &\longrightarrow \tilde{\boldsymbol{p}}_o, \ \forall o \in \mathcal{O}_i, \\ \{\mathcal{S}_i \setminus \mathcal{S}_i^{\xi^-}\} \cup \mathcal{S}_i^{\xi^+} &\longrightarrow \tilde{\mathcal{S}}_i, \end{aligned} \tag{8}$$

where $\boldsymbol{\xi}_i^x \in \mathbb{R}^n$ and $\boldsymbol{\xi}_i^o \in \mathbb{R}^2$ denote the attack vectors on state and obstacle positions, whereas the sets $\mathcal{S}_i^{\xi^-} \subset \mathcal{V}$ and $\mathcal{S}_i^{\xi^+} \subset \mathcal{V}$, $\{\mathcal{S}_i^{\xi^-} \cap \mathcal{S}_i^{\xi^+}\} = \emptyset$ are vehicle identifications that are removed from and added to the original neighbor set $\mathcal{S}_i$, respectively. For any attack vector $\boldsymbol{\xi}_i^x \neq 0$, $\boldsymbol{\xi}_i^o \neq 0$, $\forall o$, or sets satisfying $|\mathcal{S}_i^{\xi^+}|, |\mathcal{S}_i^{\xi^-}| > 0$, an attacker is replacing the original message such that the received information by any nearby neighbors will differ from the intended broadcast.

C. Problem Formulation

Given the network described by the virtual spring model (2) and the *control graph* $\mathcal{G}_{\mathcal{U}}(\mathcal{V}, \mathcal{E}_{\mathcal{U}})$, we are interested in solving the following problems:

***Problem** 1 (Vehicle Inconsistency Detection):* Create a decentralized detection policy $\mathcal{P}_d$ such that a vehicle $j \in \mathcal{V}$ that is experiencing inconsistent behavior can be discovered and isolated by any vehicle $i \in \mathcal{V}$ such that,

$$(i, j) \notin \mathcal{E}_{\mathcal{U}}, \ i \neq j, \tag{9}$$

to prevent undesirable effects to the multi-vehicle network.

A second problem that we explore in this work is to enable indirect exchange of information by leveraging signature mobility behaviors of the agents of the swarm. While navigating through an adversarial environment, vehicles that come into sensing range of an object of interest desire to notify the remaining vehicles in the network of their discovery without revealing explicitly the identification and position of the object to maintain secrecy from adversaries.

***Problem** 2 (Hidden Signature Detection):* Given a vehicle $i \in \mathcal{V}$ that has found an object of interest while navigating within an environment, find a control policy $\mathcal{P}_u$ to covertly provide an identifiable hidden signature $\boldsymbol{u}_i^{\mathcal{H}} \in \mathbb{R}^m$ for any nearby vehicles $j \in \mathcal{C}_i \subset \mathcal{V}$ to detect without explicitly sending information of the discovered object through communication broadcasts.

Upon recognizing a signature behavior, neighbors of the vehicle will estimate the position of the object based on the same signature and switch toward that object.

III. Framework

In this section we describe the decentralized monitoring framework for detection and isolation of inconsistently behaving vehicles in the network, while allowing each vehicle to provide a hidden signature for nearby vehicles. The diagram in Fig. 2 summarizes our proposed scheme in which each vehicle follows the primary or hidden control model, as well as detects whether neighboring robots have expected behavior according to the primary or hidden models.

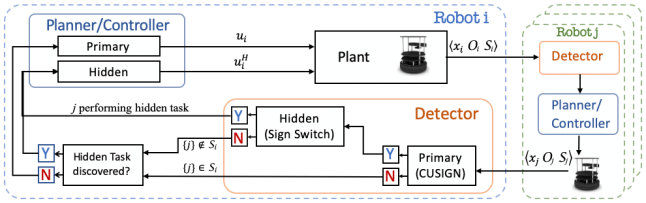

Fig. 2. Overall framework architecture followed by each vehicle $i \in \mathcal{V}$.

A. Monitoring Vehicles for Consistency

During operations, each vehicle monitors nearby vehicles for consistent behavior according to the network model described in (2). Each vehicle i receives broadcast information from any nearby vehicle $j \in \mathcal{C}_i$ as represented in (4). This vehicle i is able to make state evolution predictions of a nearby vehicle $j \in \mathcal{S}_i$ such that the neighbor set of vehicle j satisfies $\mathcal{S}_j \subset \mathcal{C}_i$. The inclusion of the neighbor set $\mathcal{S}_j \subset \mathcal{C}_i$ is needed in order for vehicle i to predict the future state of the system using (2). The state prediction of a vehicle j computed by a vehicle i is computed as,

$$\bar{\boldsymbol{x}}_{ij}^{(k+1)} = \boldsymbol{A}\hat{\boldsymbol{x}}_j^{(k)} + \boldsymbol{B}\boldsymbol{u}_{ij}^{(k)} \in \mathbb{R}^n, \tag{10}$$

where $\boldsymbol{u}_{ij}^{(k)} \in \mathbb{R}^m$ is the estimated input for vehicle j that is computed by vehicle i which follows the primary network model (2). At every kth time iteration, a vehicle i compares the *inter-vehicle residual* $\boldsymbol{r}_{ij}^{(k)}$ —defined as the difference between the received state information $\hat{\boldsymbol{x}}_j^{(k)}$ and the computed state prediction of a vehicle $j \in \mathcal{S}_i$— by,

$$\boldsymbol{r}_{ij}^{(k)} = \hat{\boldsymbol{x}}_j^{(k)} - \bar{\boldsymbol{x}}_{ij}^{(k)} \in \mathbb{R}^n. \tag{11}$$

If a vehicle j is attack-free and is following the primary network model while monitored by a vehicle i, each element $q \in \{1, \ldots, n\}$ of the inter-vehicle residual vector is normally distributed $r_{ij,q}^{(k)} \sim \mathcal{N}\big(0, \sigma_{r,q}^2\big)$ described as follows,

$$\mathbb{E}[r_{ij,q}] = 0, \quad \mathrm{Var}[r_{ij,q}] = \sum_{s=1}^{N_s} \Big(K_{(q,s)}\sigma_{z,s}\Big)^2, \tag{12}$$

where $K_{(q,s)}$ represents the element of the qth row and sth column of the steady state Kalman gain $\boldsymbol{K}$ discussed in

Section II-A. The variable $\sigma_{z,s}^2$ is the sth diagonal element of the measurement residual covariance matrix $\mathbf{\Sigma}_z \in \mathbb{R}^{N_s \times N_s}$ from the on-board state estimation process with N_s sensors (see works [16]–[18] for details of the measurement residual characteristics). Since the network consists of N homogeneous vehicles, then all vehicles share the same values $\boldsymbol{K}$ and $\mathbf{\Sigma}_z$. Each qth element of $\boldsymbol{r}_{ij}^{(k)}$ is a zero-mean normally distributed variable that is characterized as:

$$\begin{aligned} \Pr\left(r_{ij,q}^{(k)} < \mathbb{E}[r_{ij,q}^{(k)}]\right) &= p_- = 0.5, \\ \Pr\left(r_{ij,q}^{(k)} > \mathbb{E}[r_{ij,q}^{(k)}]\right) &= p_+ = 0.5, \end{aligned} \tag{13}$$

during nominal (i.e., no attack) conditions.

To monitor whether the incoming information from nearby vehicles is behaving in an expected random manner with respect to the primary network model (2), we employ the Cumulative Sign (CUSIGN) detector [17] to check for randomness with the following procedure:

CUSIGN Detector

$$\begin{aligned} &\textbf{Initialize: } S_{ij,q}^{(0),+} = S_{ij,q}^{(0),-} = 0, \ \forall i,j,q \\ &S_{ij,q}^{(k),+} = \max\big(0, S_{ij,q}^{(k-1),+} + \text{sgn}(r_{ij,q}^{(k)})\big), \\ &S_{ij,q}^{(k),+} = 0 \text{ and Alarm } \zeta_{ij,q}^{(k),+} = 1, \qquad \textbf{if } S_{ij,q}^{(k-1),+} = \tau, \\ &S_{ij,q}^{(k),-} = \min\big(0, S_{ij,q}^{(k-1),-} + \text{sgn}(r_{ij,q}^{(k)})\big), \\ &S_{ij,q}^{(k),-} = 0 \text{ and Alarm } \zeta_{ij,q}^{(k),-} = 1, \qquad \textbf{if } S_{ij,q}^{(k-1),-} = -\tau. \end{aligned} \tag{14}$$

The multi-vehicle detection procedure on a vehicle i accumulates the signed values of the inter-vehicle residual in the CUSIGN test variables for a vehicle j and triggers an alarm $\zeta_{ij,q}^{(k),\pm} = 1$ when a user-defined threshold $\tau \in \mathbb{N}$ is reached, otherwise $\zeta_{ij,q}^{(k),\pm} = 0$. As either of the test variables reach their respective thresholds, the test variable is then reset back to zero. The alarms for each qth element are then sent to a Memoryless Runtime Estimator (MRE) [17] to provide a run-time update for alarm rates $\hat{A}_{ij,q}^{(k),-}$ and $\hat{A}_{ij,q}^{(k),+}$, for simplicity denoted as $\hat{A}_{ij,q}^{(k),\pm}$, at a time k by the following,

$$\hat{A}_{ij,q}^{(k),\pm} = \hat{A}_{ij,q}^{(k-1),\pm} + \frac{\left[\zeta_{ij,q}^{(k),\pm} - \hat{A}_{ij,q}^{(k-1),\pm}\right]}{\ell}, \tag{15}$$

where $\zeta_{ij,q}^{(k)}$ is the alarm, $\ell \geq 10$ is a "pseudo-window" length, and $\hat{A}_{ij,q}^{(0)} = \mathbb{E}[A^{\pm}]$ is the expected alarm rate. The following lemma provides an expected alarm rate for a vehicle that is free from attacks (i.e., behaving nominally).

Lemma 1: Given a vehicle $i \in \mathcal{V}$ with a CUSIGN detector (14) with a threshold $\tau \in \mathbb{N}$ that is monitoring a vehicle $j \in \mathcal{V}$ during attack-free conditions , then the inverse of the first element of the following vector,

$$\boldsymbol{\mu}^{+} = (\boldsymbol{I}_\tau - \mathcal{Q}^{+})^{-1}\mathbf{1}_{\tau\times 1} = (\mu_1^{+}, \ldots, \mu_\tau^{+})^{\mathsf{T}}, \tag{16}$$

is the expected alarm rate $\mathbb{E}[A^{+}]$, and $\mathcal{Q}^{+} \in \mathbb{R}^{\tau\times\tau}$ represents the transient states of a designed Markov transition matrix.

Proof: See [17] for a similar proof. ■

Remark 1: The previous lemma describes the expected rate $\mathbb{E}[A^{+}]$ at which the CUSIGN test variable $S_{ij,q}^{(k),+}$ reaches the defined threshold value τ to trigger an alarm $\zeta_{ij,q}^{(k),+} = 1$. Similarly, the design of a transition matrix with fundamental matrix $\mathcal{Q}^{-}$ and expected alarm rate $\mathbb{E}[A^{-}] = (\mu_1^{-})^{-1}$ for the negative case is computed with transition probability (p_+ and p_-) signs inverted. For construction of $\mathcal{Q}^{+}$ and $\mathcal{Q}^{-}$, see [17].

Proposition 1: Assuming a vehicle $j \in \mathcal{V}$ is not experiencing MITM attacks while being monitored by a vehicle $i \in \mathcal{V}$ and using the MRE algorithm (15) for alarm rate estimation, the alarm rate is normally distributed by $\hat{A}_{ij,q}^{\pm} \sim \mathcal{N}\Big(\mathbb{E}[A^{\pm}], \frac{\theta\mathbb{E}[A^{\pm}](1-\mathbb{E}[A^{\pm}])}{2\ell-1}\Big)$, where $\theta \in \mathbb{R}_+$ is a scaling constant (see [17]).

By leveraging $\mathbb{E}[A^{\pm}]$ in Lemma 1, the following corollary provides detection bounds for the CUSIGN alarm rate.

Corollary 1: Given the qth element of the inter-vehicle residual (11) being monitored by CUSIGN (14), detection of attacks occur for a chosen level of significance $\alpha \in (0,1)$ when the alarm rate no longer satisfies detection bounds (i.e., $\hat{A}_{ij,q}^{(k),\pm} \notin [\Omega_-, \Omega_+]$) where $\Omega_\pm = \mathbb{E}[A^{\pm}] \pm \Phi^{-1}\big(\alpha/2\big)\sqrt{\text{Var}[A^{\pm}]}$, such that $\Phi^{-1}(\cdot)$ is the inverse cumulative distribution function of a normal distribution.

Proof: See [17] for a similar proof. ■

A vehicle i that detects non-random (i.e., inconsistent) inter-vehicle residual behavior from a vehicle j, responds by placing vehicle j in its compromised set $j \in \mathcal{R}_i$, $\mathcal{R}_i \subset \mathcal{V}$, hence removing it from the control graph (i.e., $(i,j) \notin \mathcal{E}_{\mathcal{U}}$).

B. Hidden Signature Detection

During operations, vehicles are tasked to converge to observed objects of interest while navigating through the environment. As an ith vehicle comes within sensing distance δ_r of the on-board range sensor with respect to an object,

$$l_{ip} = \|\boldsymbol{p}_i - \boldsymbol{p}_p\| \leq \delta_r, \tag{17}$$

where $\boldsymbol{p}_p$ is the position of an object of interest, the vehicle will notify neighboring vehicles by creating a detectable hidden signature. To achieve this, the vehicle switches to a *hidden* virtual spring-damper model described by,

$$\boldsymbol{u}_i^{\mathcal{H}} = \ddot{\boldsymbol{p}}_i = \left[\kappa_h(l_{ip} - l_h^0)\vec{\boldsymbol{d}}_{ip} - \gamma_h\dot{\boldsymbol{p}}_i\right] \in \mathbb{R}^m, \tag{18}$$

where the virtual spring-damper parameters $\kappa_h \neq \kappa_v$ and/or $\gamma_h \neq \gamma_v$ are distinct from the primary network model in (2) to enable an identifiable dynamical signature. A vehicle i that follows the hidden model (18) removes all virtual spring interactions to neighboring vehicles and the goal from the primary network model that affect its control input. To maintain secrecy from attackers (with regards to the observance of the object of interest), a vehicle i will continue to broadcast state, observed obstacle positions, and its neighbor set information to nearby vehicles as it would in nominal conditions. In this way, a malicious agent who is listening will continue to see the same type of information as before. Any manipulation of such information that does not conform with the new hidden model (18) or with the primary model in (2) will be considered a cyber-attack.

The challenge that arises is that the object position $\boldsymbol{p}_p$ remains unknown to the other vehicles in the network. In comparison to the primary model (2), nearby vehicles do not receive all necessary information when a vehicle i follows the hidden model (18) to monitor for consistency. This is due to constraints set in Problem 2, that information regarding

a discovered object of interest can not be explicitly shared with the network to protect from interception by attackers.

Given that the hidden model (18), vehicle dynamics (1), and maximum sensing range δ_r are known by all vehicles, an expected vehicle velocity behavior can be leveraged as a vehicle converges toward an object (i.e., a decaying velocity magnitude). More specifically, any vehicle i can recognize the hidden signature by monitoring the received velocity estimate $\hat{\boldsymbol{v}}_j^{(k)}$ behavior from a vehicle j and compare it to the expected velocity decay behavior from the hidden model. Shown in Fig. 3(a) is an example of the differing expected velocity behavior between springs of the primary and hidden models with the corresponding distances to the object.

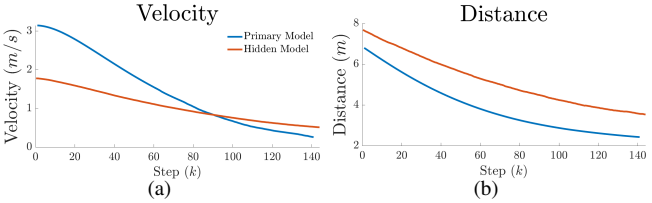

Fig. 3. Differing expected behavior of the (a) velocity decay, and (b) distance to the object for the two different virtual spring-damper models.

Given that each vehicle i is making state predictions of any neighboring vehicle j according to the primary network model (2), an alternative action by this vehicle (i.e., utilizing the hidden model) would result in an unexpected behavior. Alarm rates from CUSIGN (14) on-board a vehicle i that is monitoring vehicle j, in turn, go beyond detection bounds due to the unexpected behavior and vehicle j is placed in the compromised vehicle set $\mathcal{R}_i \subset \mathcal{V}$. Next, vehicle i would begin to monitor the received velocity information of vehicle j to determine if its behavior follows the hidden model (18). A velocity prediction of vehicle j by a vehicle i given $j \in \mathcal{R}_i$ is made from the received velocity estimate $\|\hat{\boldsymbol{v}}_j^{(k)}\|$ by,

$$\bar{v}_{ij}^{(k+1)} = h\big(\|\hat{\boldsymbol{v}}_j^{(k)}\|\big), \tag{19}$$

where the function $h(\cdot)$ represents the expected velocity behavior according to the hidden spring model (18), as shown in Fig. 3(a). At each time iteration k, the *hidden velocity residual* $\breve{r}_{ij}^{(k)}$ — the difference between received velocity magnitudes and velocity predictions using the hidden model — of vehicle j is computed by the following,

$$\breve{r}_{ij}^{(k)} = \|\hat{\boldsymbol{v}}_j^{(k)}\| - \bar{v}_{ij}^{(k)} \in \mathbb{R}, \tag{20}$$

to monitor whether vehicle j is following the hidden model in (18). We leverage the known zero-mean Normally distributed velocity estimate provided by vehicle j (see estimation error covariance in [16]–[18]) when characterizing the hidden velocity residual. An assumption can be made such that the received velocity estimate information from vehicle j is also approximately zero-mean Normally distributed around the expected velocity decay behavior in $h\big(\|\hat{\boldsymbol{v}}_j^{(k)}\|\big)$, *only* if vehicle j is following the hidden model. In this scenario, the hidden velocity residual (20) is expressed as a random variable that presents the following characteristics:

$$\begin{aligned} \Pr\big(\breve{r}_{ij}^{(k)} < 0\big) &= \breve{p}_- = 0.5, \\ \Pr\big(\breve{r}_{ij}^{(k)} > 0\big) &= \breve{p}_+ = 0.5, \end{aligned} \tag{21}$$

where the probability of the hidden velocity residual being greater or less than zero is equal. A random variable with characteristics that follow (21) should present an expected sign switching rate behavior (i.e. how frequently $\breve{r}_{ij}^{(k)}$ changes signs) in accordance to the probabilities in (21). To capture the rate of sign switching, we leverage an alarm that is triggered (i.e., $\psi_{ij}^{(k)} = 1$) when a sign switch occurs at a time k. The procedure to trigger a sign switching alarm follows:

$$\psi_{ij}^{(k)} = \begin{cases} 1, & \text{if } \operatorname{sgn}\big(\breve{r}_{ij}^{(k)}\big) = -\operatorname{sgn}\big(\breve{r}_{ij}^{(k-1)}\big), \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

The sign switching alarm $\psi_{ij}^{(k)} \in \{0, 1\}$ is then sent into the MRE algorithm (15) to provide an updated run-time estimate of the hidden signature sign switching alarm rate $\hat{H}_{ij}^{(k)} \in [0, 1]$ at time instance k.

Lemma 2: Given a vehicle j that is following the hidden model (18) while being monitored by vehicle i, the expected sign switching rate to signify random behavior is $\mathbb{E}[H] = \frac{1}{2}$.

Proof: We first examine the asymptotic distribution of the expected number of observed runs $\mathbb{E}[U]$ from the Wald-Wolfowitz runs test [21]. Then, we convert $\mathbb{E}[U]$ over a defined sequence length to a rate described by how frequently runs should occur (i.e., how often sign switching occurs) by leveraging the known characteristics of the probabilities $\breve{p}_+$ and $\breve{p}_-$, such that the random variable follows $\mathbb{E}[H] = 2\breve{p}_+\breve{p}_- = \frac{1}{2}$, thus concluding the proof. ∎

Lemma 3: The expected variance of the sign switching rate $\hat{H}_{ij}^{(k)}$ for a vehicle j that follows the hidden model (18) while monitored by vehicle $i \in \mathcal{V}$ is $\operatorname{Var}[H] = \frac{1}{4(2\ell-1)}$.

Proof: Let the expectation of a sign switch be modeled by a Binomial distribution where the probability of success (i.e., sign switch) is $\mathbb{E}[H]$. By normal approximation and utilizing MRE (15) for sign switching rate estimation, the random variable follows a normal distribution with variance $\operatorname{Var}[H] = \frac{\mathbb{E}[H](1-\mathbb{E}[H])}{2\ell-1} = \frac{1}{4(2\ell-1)}$, concluding the proof. ∎

The following corollary provides bounds of $\hat{H}_{ij}^{(k)}$ to satisfy an expected behavior to detect the hidden model signature.

Corollary 2: Given the sequence of hidden velocity residuals $\breve{r}_{ij}^{(k)}$, hidden signature detection occurs by the sign switching alarm rate when $\Psi_- \leq \hat{H}_{ij}^{(k)} \leq \Psi_+$ is satisfied.

Proof: A proof can be obtained by leveraging confidence intervals within a Normal Distribution. Due to page limitations, we omit the proof. ∎

To summarize Corollary 2, when the sign switching alarm rate for the detection of the hidden signature satisfies,

$$\hat{H}_{ij}^{(k)} \in [\Psi_-, \Psi_+] \longrightarrow \textit{Signature Detection}, \tag{23}$$

vehicle i detects a hidden signature behavior in j. Vehicle i reacts by estimating the position of the object by leveraging the training set (i.e., expected hidden model behavior) mapping $f : \mathbb{R}^2 \to \mathbb{R}$ in Fig. 3 that maps the received velocity estimate of vehicle j to its distance to the object by,

$$\hat{d}_{p,ij}^{(k)} = f(\|\hat{\boldsymbol{v}}_j^{(k)}\|). \tag{24}$$

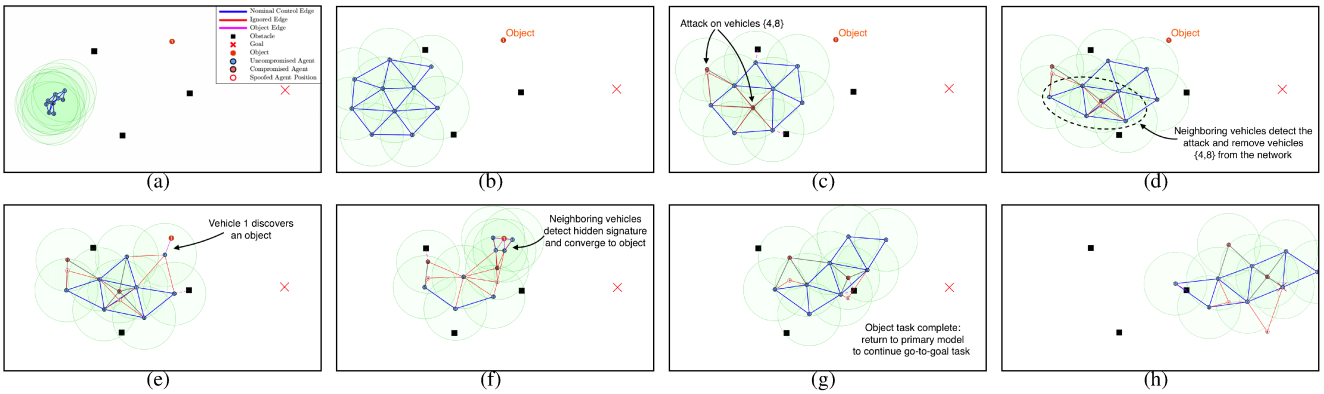

Fig. 4. A network of $N = 10$ vehicles resiliently navigate through an obstacle-filled (black squares) environment to a desired goal (red 'X'). Vehicles converge to an object (orange disk) as it comes within their viewing range (green disks) or if they detect the hidden signature from neighboring vehicles.

The position of the object $\boldsymbol{p}_p$ is then estimated by vehicle i from the received position information of vehicle j by,

$$\hat{\boldsymbol{p}}_{p,ij}^{(k)} = \hat{\boldsymbol{p}}_j^{(k)} + \hat{d}_{p,ij}^{(k)} \vec{\boldsymbol{d}}(\|\hat{\boldsymbol{v}}_j^{(k)}\|), \tag{25}$$

where $\vec{\boldsymbol{d}}(\cdot)$ is a unit vector indicating velocity direction of vehicle j. Once the object position coordinates $\hat{\boldsymbol{p}}_{p,ij}^{(k)}$ have been estimated, vehicle i then detaches virtual springs from its neighbors and goal to converge to the object of interest by also following the hidden model (23). Vehicles within the network will continue to converge toward the point of interest until its task is completed. Upon completion, all vehicles involved with the hidden task return to their normal control behavior with the primary network model in (2).

IV. Results

Our approach is validated with Matlab simulations and experiments using swarms of Turtlebot 2 robots, as shown in the provided video. In both case studies, the vehicle networks leverage a primary network model (2) to perform a go-to-goal task and a hidden model (18) to covertly notify surrounding vehicles when an object of interest has been discovered. Furthermore, vehicles are subject to MITM cyber-attacks that are attempting to hijack the network to an undesired state.

A. Simulation

For the simulation case study, we consider $N = 10$ vehicles treated as double integrator point-masses navigating in an x-y plane. A sequence of snapshots are presented in Fig. 4 showing the network of vehicles resiliently navigating through an obstacle filled environment. From Fig. 4(c)-(h), vehicles $\{4, 8\}$ (red circles) are subject to MITM attacks that falsify position information with the intention of hijacking the network. In Fig. 4(e) vehicle 1 discovers an object and then switches to the hidden model (18) to covertly notify neighboring vehicles about the discovery. In turn, neighboring vehicles detect this hidden signature (23), estimate the position of the object (25), then also switch to the hidden model to converge to the object. CUSIGN and sign switching alarm rates from the perspective of vehicle $i = 7$ are provided in Fig. 5 while monitoring neighboring vehicles for primary and hidden model behaviors. Alarm rates for CUSIGN (14) monitoring vehicles $\{1, 2, 4, 8, 10\}$ travel beyond detection bounds indicated by red dashed lines. However, shown in Fig. 5(b), the hidden signature alarm rates (23) for vehicles $\{1, 2, 10\}$ satisfy the hidden model detection bounds to signify consistent behavior is occurring with respect to the hidden model (18), thus deeming these vehicles trustworthy. Alternatively, vehicles $\{4, 8\} \in \mathcal{R}_7$ are treated compromised as a hidden signature was not detected from their motion.

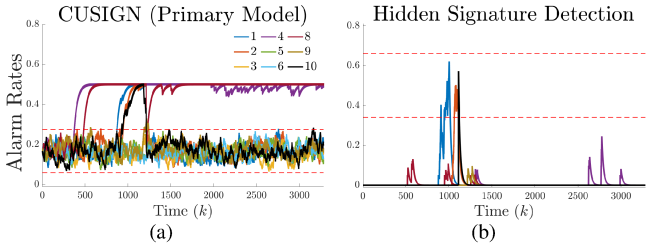

Fig. 5. (a) CUSIGN detection alarm rates from the perspective of vehicle $i = 7$ and (b) sign switching alarm rates for hidden signature detection.

B. Experiment

Experimental validations are performed on $N = 5$ TurtleBot 2 differential-drive robots performing a go-to-goal operation within a lab environment. Snapshots of this experiment are presented in Fig. 6 capturing the following sequence of events; the initial vehicle positions (Fig. 6(a)), vehicle 2 discovering the object (Fig. 6(d)), neighboring vehicles converge toward the object after detecting the hidden signature from vehicle 2 (Fig. 6(e)), and the network continuing to the goal once the object "task" has been completed (Fig. 6(f)-(g)). During the simulation, communication broadcasts from vehicle $j = 4$ are corrupted with false position data that attempt to drive the system to an undesirable location, but the CUSIGN detector finds these stealthy attacks, allowing the network to resiliently perform the operation. In Fig. 7, alarm rates that are monitoring the primary (2) and hidden (18) models throughout the experiment show vehicle 1 detecting the compromised vehicle 4, as well as detecting the hidden signature from vehicle 2.

V. Conclusions

In this paper we have proposed a decentralized framework for a network of homogeneous vehicles to resiliently perform desired operations. Vehicles are able to distinguish between received inconsistent information from neighboring vehicles due to man-in-the-middle attacks and hidden model behaviors that provide a detectable signature to implicitly pass

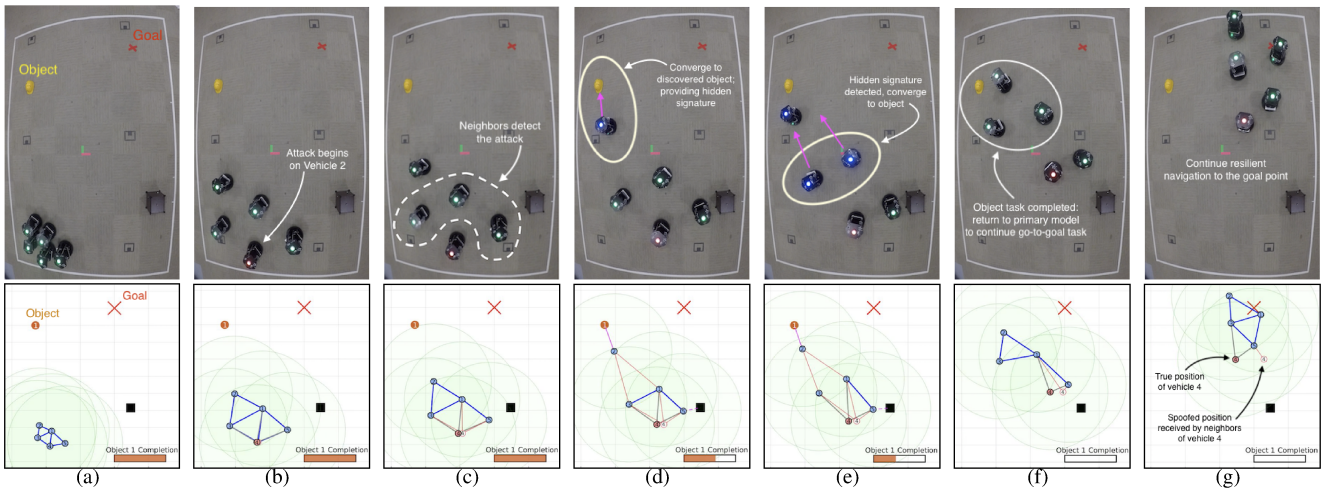

Fig. 6. An experiment showing a network of $N = 5$ TurtleBot 2 robots resiliently navigating to a goal (red 'X'). Vehicle 2 discovers an object (yellow helmet) as comes within its sensing range (depicted by the green translucent circle), then provides a hidden signature behavior for nearby vehicles to recognize as it converges to the object. Neighboring vehicles also converge to the object of interest upon detection of this hidden signature.

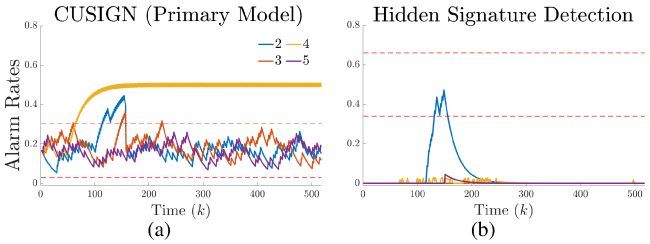

Fig. 7. (a) CUSIGN and (b) sign switching alarm rates from the perspective of vehicle $i = 1$. Detection bounds are indicated by red dashed lines.

safety-critical information. To detect stealthy attacks and the hidden signature, we leverage randomness-based detection techniques —Cumulative Sign (CUSIGN) and sign switching rate— to identify whether vehicles are following a primary or hidden network model. In our future work we plan to: i) extend the current approach by investigating the effects of different attack classes/models and ii) develop an adaptive approach for the virtual spring parameters to conform to changing network or environmental conditions.

VI. Acknowledgement

This work is based on research supported by NSF under grant number #1816591 and ONR under agreement number N000141712012. The authors would like to thank Rahul Peddi and Shijie Gao for assisting with the experiments.

References

[1] S. Sharmin, S. I. Salim, and K. R. I. Sanim, "A low-cost urban search and rescue robot for developing countries," in *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)*, 2019, pp. 60–64.

[2] D. van der Walle, B. Fidan, A. Sutton, *et al.*, "Non-hierarchical uav formation control for surveillance tasks," in *2008 American Control Conference*, 2008, pp. 777–782.

[3] C. J. R. McCook and J. M. Esposito, "Flocking for heterogeneous robot swarms: A military convoy scenario," in *2007 Thirty-Ninth Southeastern Symposium on System Theory*, 2007, pp. 26–31.

[4] R. Maeda, T. Endo, and F. Matsuno, "Decentralized navigation for heterogeneous swarm robots with limited field of view," *IEEE Robotics and Automation Letters*, vol. 2, no. 2, pp. 904–911, 2017.

[5] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[6] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, 2015.

[7] B. Shucker, T. D. Murphey, and J. K. Bennett, "Convergence-preserving switching for topology-dependent decentralized systems," *IEEE Transactions on Robotics*, vol. 24, no. 6, pp. 1405–1415, 2008.

[8] Q. Chen, Y. Meng, and J. Xing, "Shape control of spacecraft formation using a virtual spring-damper mesh," *Chinese Journal of Aeronautics*, vol. 29, no. 6, pp. 1730 – 1739, 2016.

[9] N. Bezzo, P. J. Cruz, F. Sorrentino, *et al.*, "Decentralized identification and control of networks of coupled mobile platforms through adaptive synchronization of chaos," *Physica D: Nonlinear Phenomena*, vol. 267, pp. 94 – 103, 2014, evolving Dynamical Networks.

[10] N. Bezzo, B. Griffin, P. Cruz, *et al.*, "A cooperative heterogeneous mobile wireless mechatronic system," *IEEE/ASME Transactions on Mechatronics*, vol. 19, no. 1, pp. 20–31, 2014.

[11] K. Saulnier, D. Saldaña, A. Prorok, *et al.*, "Resilient flocking for mobile robot teams," *IEEE Robotics and Automation Letters*, vol. 2, no. 2, pp. 1039–1046, 2017.

[12] Y. Shang, "Scaled consensus of switched multi-agent systems," *IMA Journal of Mathematical Control and Information*, vol. 36, no. 2, 2018.

[13] Y. Mo, E. Garone, A. Casavola, *et al.*, "False data injection attacks against state estimation in wireless sensor networks," in *49th IEEE Conference on Decision and Control*, 2010, pp. 5967–5972.

[14] C. Kwon, S. Yantek, and I. Hwang, "Real-time safety assessment of unmanned aircraft systems against stealthy cyber attacks," *Journal of Aerospace Information Systems*, vol. 13, no. 1, pp. 27–45, 2016.

[15] D. Dionne, H. Michalska, Y. Oshman, *et al.*, "Novel adaptive generalized likelihood ratio detector with application to maneuvering target tracking," *Journal of Guidance, Control, and Dynamics*, vol. 29, no. 2, pp. 465–474, 2006.

[16] C. Murguia and J. Ruths, "Characterization of a cusum model-based sensor attack detector," in *2016 IEEE 55th Conference on Decision and Control (CDC)*, Dec 2016, pp. 1303–1309.

[17] P. J. Bonczek and N. Bezzo, "Memoryless cumulative sign detector for stealthy cps sensor attacks," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 838–844, 2020, 21th IFAC World Congress.

[18] P. J. Bonczek, S. Gao, and N. Bezzo, "Model-based randomness monitor for stealthy sensor attacks," in *2020 American Control Conference (ACC)*, 2020, pp. 2036–2042.

[19] S. Lee and B. Min, "Distributed direction of arrival estimation-aided cyberattack detection in networked multi-robot systems," in *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2018, pp. 1–9.

[20] K. R. Gabriel and R. R. Sokal, "A New Statistical Approach to Geographic Variation Analysis," *Systematic Biology*, vol. 18, no. 3, pp. 259–278, 09 1969.

[21] A. Wald and J. Wolfowitz, "On a test whether two samples are from the same population," *Ann. Math. Statist.*, vol. 11, no. 2, 1940.