Sneak Attack against Mobile Robotic Networks under Formation Control

Yushan Li†, Jianping He†, Xuda Ding†, Lin Cai† and Xinping Guan†

Abstract—The security of mobile robotic networks (MRNs) has been an active research topic in recent years. This paper demonstrates that the observable interaction process of MRNs under formation control will present increasingly severe threats. Specifically, we find that an external attack robot, who has only partial observation over MRNs while not knowing the system dynamics or access, can learn the interaction rules from observations and utilize them to replace a target robot, destroying the cooperation performance of MRNs. We call this novel attack as sneak, which endows the attacker with the intelligence of learning knowledge and is hard to be tackled by traditional defense techniques. The key insight is to separately reveal the internal interaction structure within robots and the external interaction mechanism with the environment, from the coupled state evolution influenced by the model-unknown rules and unobservable part of the MRN. To address this issue, we first provide general interaction process modeling and prove the learnability of the interaction rules. Then, with the learned rules, we design an Evaluate-Cut-Restore (ECR) attack strategy considering the partial interaction structure and geometric pattern. We also establish the sufficient conditions for a successful sneak with maximum control impacts over the MRN. Extensive simulations illustrate the feasibility and effectiveness of the proposed attack.

I. INTRODUCTION

Mobile robotic networks (MRNs) have received considerable attention in recent years. Thanks to the mobility, flexibility, and distributed fashion, MRNs are widely deployed in numerous applications, e.g., surveillance, reconnaissance, search and environmental monitoring [2]. Among these applications, formation control is a fundamental technique to enhance the cooperation performance by maintaining a preset geometric shape [3]–[7].

It has been reported that MRNs under formation control may suffer severe security vulnerabilities from both cyber and physical spaces [8], [9]. Existing works mainly focus on the cybersecurity of MRNs, and various defense techniques are developed to protect the information availability, integrity and confidentiality. In the literature, the attacker is generally assumed with strong knowledge about the system (e.g., network structure, dynamics model) or powerful capabilities (e.g., access to the system), lacking for deep investigation on the capabilities and modes of attackers in more realistic situations. This paper demonstrates that an external attacker without strong prior knowledge can observe the state evolution of the MRN to obtain data, learn the interaction rules from the data analysis, and further leverage the rules to implement attacks that cannot be handled by traditional security countermeasures. Several prior works have made some progress in this direction and support our demonstration. For example, it is possible to infer whether two robots are connected [10] or learn how a single robot avoids an obstacle [11]. However, considering what exact interaction rules can be learned and under what conditions to obtain them, how to further destroy the cooperation performance by leveraging the rules and where is the attack impact boundary, they are all still open issues and need further exploration.

Motivated by above discussions, we design a sneak attack against MRNs under formation control, where the attack robot has only partial observation and aims to replace one robot therein, obtaining partial control over the MRN and destroying the cooperation performance. This attack is inspired by that i) the shape-forming process essentially reflects the internal interaction structure among cooperating robots [12]; ii) the obstacle-avoidance behavior embodies how the robots interact with the environment [13]; iii) both the interaction rules are limited by physical distance in practical applications, either by communication or sensing. These universal interaction characteristics indicate the possibility of learning them to implement advanced attacks, making our work of both theoretical and practical significance. From the attack view, it enlightens the feasibility of revealing the interaction rules that support the MRN, and guides for more advanced attack design (e.g., invade an MRN). In turn, from the defense view, it provides deeper insights into the trade-off between the system security and observability, and helps the countermeasure design by understanding the possible attack capabilities and modes.

Challenges and contributions. The major challenges of achieving the sneak attack lie in two aspects. First, the attacker can only observe the measurable states of a partial MRN (e.g., position, velocity), and the states are influenced by both the model-unknown interaction rules and the unobservable part of the MRN. It is difficult to split the coupled influences of the multiple factors and approximate the interaction rules. Second, even if the interaction rules are obtained, their mutual impacts will closely intersect with the influence of the attack dynamics, making it further hard to design feasible and efficient strategies for the attacker to achieve maximum attack rewards. To overcome above issues, we holistically formulate the entire observe (excite)-attack process as different stages. By exploiting the independence and correlation characteristics of the interaction rules in different stages, the whole attack mode is designed
in an active-knowledge-growth form and accommodates the
coupled dynamics of the attacker and the MRN.

The differences between this paper and its conference
version [1] include i) a systematic intelligent attack design
is introduced rather than mere topology inference, ii) the
learnability of both the internal interaction structure within
the MRN and the external interaction mechanism with the
environment is explored, and iii) the sneak attack is introduced
with comprehensive feasibility and performance analysis. The
main contributions of this paper are summarized as follows.

- We contribute to the existing body of research by under-
  standing what interaction rules in MRNs under formation
can be separately revealed by observing over the state
  evolution, which is a mutual consequence of multiple
  factors. No strong prior information like dynamics model
  or access to the MRN is required.

- We find a novel sneak attack where an attacker with weak
  knowledge can learn the interaction rules and replace a
  victim robot to obtain partial control over the MRN.
  The observation and excitation oriented ideas endow the
  “ignorant” attacker with growing intelligence to achieve
  maximum attack impacts, and this kind of attack is hard
  to be tackled by traditional defense techniques.

- We develop an in-depth framework to handle different
  interaction rules of MRNs. We prove the learnability of
  the interaction rules by extracting their universal charac-
  teristics. Utilizing the proposed node controllability, we
  design an ECR strategy and establish the sufficient con-
  ditions for the attack. Performance study by simulation
  demonstrates the effectiveness of the sneak attack.

In a larger sense, this paper promotes to explore the security
vulnerabilities in the interaction process, and beckons further
research to address the new physical observation and excitation
oriented attacks on generic networked systems.

Organization and Notation. The remainder of this paper is
organized as follows. Section II presents related literatures.
Section III gives the modeling for the interaction process
of MRNs and formulates the attack process. Section IV
studies how to reveal the interaction rules. Section V
develops how to design control strategies for the final sneak.
Simulation results are shown in Section VI followed by the
concluding remarks and further research issues in Section VII.
All the proofs of the Lemmas and Theorems are provided in the Appendix.

Throughout the paper, the set variable is expressed in
Euclid font, and the compact all-dimension state of a robot is
expressed in bold font. Unless otherwise noted, the formulas
with non-bold font state variable apply to every dimension of
the actual state space. $\mathcal{A} \setminus \mathcal{B}$ represents the elements in $\mathcal{A}$
that are not in $\mathcal{B}$. The superscripts $[i, :], [:, i]$ of a matrix denote
its $i$-th row vector and $i$-th column vector, respectively. The
scripts $\cdot$ and $\dagger$ right above a variable indicate its correspond-
ing observation and estimation value, respectively. The basic
notation definitions are given in Table I.

II. RELATED WORK

Formation control in MRNs. The fundamental rules for for-
mation control were first introduced by the famous Reynolds’
Rules [14]: separation, alignment, and cohesion. Based on the
rules, numerous methods have been proposed to achieve the
desired performance, and consensus-based algorithms become
the mainstream, e.g., [15]–[18]. The key idea of consensus-
based algorithms is that the formation is modeled as a graph,
and every robot implements information interaction (like po-
positions and velocities) with their neighbors and compute their
control inputs. Therefore, the interaction structure lays critical
support for effective formation control and is mostly based on
network communication. In recent years, communication-free
formation control [19]–[21] was also developed and attracts
great research interests, thanks to the emergent development
of sensor technology. Communication-free interaction avoids
information delays and network bandwidth consumption, and
ev en enables stealth modes of operation [22]. For instance,
formation control with only bearing measurements by vision
sensors was investigated in [23].

Although the Reynolds’ Rules lay a solid foundation for
formation control, they do not take into account some unant-
icipated faults (e.g., interaction failure, formation splitting),
which are easily incurred when performing tasks in the real
environment. Many advanced interaction rules and techniques
were developed to better handle those accidental and un-
premeditated faults [24]–[26]. For instance, a consensus-based
splitting/merging algorithm was designed to tackle complex
obstacle distributions in [27]. A topology recovery method was
designed to reconnect a broken link based on historical data in
[28], [29]. [30] proposed a gradient-based self-repairing
algorithm to restore the topology of formation and further
synchronize the formation motion. The motion synchronization
methods were investigated to form desired/predefined
formation configuration in the presence of robot malfunctions
[31] or undesirable formation variation [32]. [33] gave a com-
prehensive survey for more types of fault-tolerant design about
formation control. Note that by either way, the interaction
capability is limited by distance due to the energy constraint
in real-world applications, and this simple yet crucial point is
utilized in our attack design.

The security of MRNs. Effective formation control in MRNs
is supported by physical sense and network interaction, which
constitute the feedback loops for control and also incur secu-
rity vulnerabilities, and an attack on these components may
cause disastrous consequences. MRN under formation control
a typical cyber-physical-system (CPS), while the existing work
mainly focused on the defense design to cyber attacks, e.g.,
DoS, false data injection, and replay attacks [34]–[37]. The
attacker is generally assumed with strong prior knowledge
about the MRN (like knowing the system structure or node
states [38], corrupting exchanged information [39]), and for-
mulated with a powerful attack model. Recently, a few works
emerged which are dedicated to attacks against formation
from physical space. For instance, a noise-generating attack
was proposed in [40] to alter gyroscopic sensor data, leading
to drone crashes. [41], [42] proposed a spoofing attack to
disturb the GPS sensor readings, gradually causing trajectory
deviations. These attacks are against a specific transducer by
utilizing its sensing mechanism, and are hard to be generalized
to other scenarios. [11] developed a trial-and-learning based

and left eigenvector are normalized such that 

\[ p^T_{-} = 0, \quad p^T_{+} q = 0 \quad (i \neq j). \]

Specially, take \( q = 1 \) and \( p = [p_1, \ldots, p_N]^T \). All the right and left eigenvectors are normalized such that \( p^T_{+} q = 1 \).

### III. Preliminaries and Problem Formulation

#### A. Graph Basics

Let \( G = (\mathcal{V}, E) \) be a directed graph that models an MRN, where \( \mathcal{V} = \{1, \ldots, N\} \) is the finite set of nodes (i.e., robots) and \( E \subseteq \mathcal{V} \times \mathcal{V} \) is the set of interaction edges. An edge \((i, j) \in E\) indicates that \( i \) will use information from \( j \). The adjacency matrix \( A = [a_{ij}]_{N \times N} \) of \( G \) is defined such that \( a_{ij} > 0 \) if \((i, j) \in E\) exists, and \( a_{ij} = 0 \) otherwise. Denote \( N^\text{in}_i = \{ j \in \mathcal{V} : a_{ij} > 0 \} \) and \( N^\text{out}_i = \{ j \in \mathcal{V} : a_{ij} = 0 \} \) as the in-neighbor and out-neighbor sets of \( i \), respectively.

A directed path is a sequence of nodes \( \{1, 2, \ldots, j\} \) such that \((i + 1, i) \in E, i = 1, 2, \ldots, j - 1\). A directed graph has a (directed) spanning tree if there exists at least a node having a directed path to all other nodes. \( G \) must have a spanning tree to guarantee the information flow in robot formation.

Define \( L = \text{diag}\{A1\} - A \) as the Laplacian matrix of \( G \), where \( 1 \) is a vector of all ones. Then, \( L1 = 0 \) holds. Let \( \Lambda = \Gamma \Lambda^{-1} \) be the Jordan decomposition of \( L \), where \( \Gamma = [q_1 \cdots q_N] \) is the transformation matrix, \( \Gamma^{-1} = [p_1 \cdots p_N] \), and \( \Lambda = \text{diag}\{\lambda_1\} \) with \( \lambda_1 \) being the Jordan block of eigenvalue \( \lambda_1 \). The eigenvalues and eigenvectors satisfy

\[
(\lambda_1 I - L)q_1 = 0, \quad p^T_{-} (\lambda_1 I - L) = 0, \quad p^T_{+} q_1 = 0 \quad (i \neq j).
\]

Specially, take \( q_1 = 1 \) and \( p_1 = [p_{11}, \ldots, p_{1N}]^T \). All the right and left eigenvectors are normalized such that \( p^T_{+} q_1 = 1 \).

#### B. Distance Constraints and Shape Specification

The robots are assumed to be set in short distance interaction with their neighbors (by communication or sensing) and need to detect obstacles. The interaction radius \( R_c \), the obstacle detection radius \( R_o \), and the safe radius \( R_s \) indicating danger range are supposed to satisfy

\[
R_c > R_o > R_s.
\]

Let \( a_{ij}^0 \) be the preset interaction weight of \((i, j)\) initially, and \( z_i (z_k) \) be the position state of robot \( i \) (all) dimension(s).

Based on the well-known disk model that considers the boundedness of \( R_c \), \( a_{ij} \) is assumed to satisfy

\[
a_{ij} = a_{ij}^0 \cdot \text{sign}(R_c - \|z_j - z_i\|_2),
\]

where the indicative function \( \text{sign}(x) = 1 \) if \( x > 0 \), or 0 otherwise. Accordingly, define the \( R \)-disk of arbitrary \( z \) as

\[
P(z, R) = \{ z_\omega : \|z_\omega - z\|_2 < R \}.
\]

### C. Interaction Modeling of Formation Control

The following modeling is given to describe how to form the preset shape through internal interaction, and deal with the environmental interferences through external interaction.

**Forming formation shape via internal interactions.** To describe the predefined geometric shape under formation control, a group of parameters \( \{h_i\} (i \in \mathcal{V}) \) is introduced, where \( h_i \) is the desired relative deviation between robot \( i \) (abbreviated to \( r_i \) hereafter) and a common reference point. Note that once the formation shape is specified, the choice of the reference point will make no difference as \( h_{ij} = h_j - h_i \) remains unchanged. To achieve this pattern, a commonly used first-order consensus-based formation control algorithm and its global form are given by

\[
\dot{z}_i = \sum_{j \in N^\text{in}_i} a_{ij} (z_j - z_i - h_{ij}), \quad \dot{z}(t) = -Lz(t) + Lh,
\]

where \( h_{ij} = h_j - h_i, z = [z_1, \ldots, z_N]^T \), and \( h = [h_1, \ldots, h_N]^T \). Generally, to dynamically guide the formation motion, one robot will be specified as the leader with an extra velocity input. For simplicity and without loss of generality, \( r_N \) is taken as the leader and reference node, and suppose that it runs in a constant velocity \( c \). Denote \( u_0 = [0, \ldots, 0, c]^T \) and \( u = Lh + u_0 \). Then, the global dynamics in \( \{5\} \) is rewritten as

\[
\dot{z}(t) = -Lz(t) + u.
\]

Accordingly, the solution of \( \{6\} \) is given by

\[
z(t) = e^{-Lt}z(0) + \int_0^t e^{-L(t-\tau)}ud\tau.
\]

Note that \( \{7\} \) guarantees zero deviation for static formation and bounded tracking error for dynamic formation.

To eliminate the error, solutions contain imposing a virtual leader to all robots (which is impractical when the scale of the MRN is large), or adopting a second-order controller which further utilizes the velocities of its neighbors. The global form by second-order controllers is the same as that by first-order ones, except that \( z_i \) is augmented with the velocity state. Consequently, the internal interaction structure is related to both the positions and velocities of neighbors. To avoid fussy

| Symbol | Definition |
|--------|------------|
| \( z_i \) | the state of robot \( i \) (\( r_i \)) in one dimension |
| \( z_a \) | the state of attack robot (\( r_j \)) in one dimension |
| \( z_v \) | the state of victim robot (\( r_k \)) in one dimension |
| \( g \) | the external interaction mechanism with environment |
| \( W \) | the internal interaction matrix among robots |
| \( R_\omega \) | the radius indicating different interaction range, where \( \omega = c, o, s, f \) represent the interaction, obstacle avoidance, safety, and observation radius, respectively. |
| \( D_\omega \) | the dataset collected in different stages, where \( \omega = c, s, e, a \) represent the convergence, stabilization, excitation and attack processes, respectively. |
| \( V^i_\omega \) | the \( r_i \)-vertexed convex polygon covering \( N^\text{out}_i \) |
| \( N^\text{in}_i \) | the in/out-neighbor set (\( \omega = \text{in/out} \)) of robot \( i \) |
| \( V_F \) | the formation under partial observation |
| \( \Omega \) | the rule set of formation interaction |

**TABLE I**

**NOTATION DEFINITIONS**

Method to infer the obstacle-avoidance mechanism of mobile robots by disguising the attack robot as an obstacle, which requires little prior knowledge about mobile robots.

In summary, concerning what attack capability is feasible for an “ignorant” attacker from external observation and what is the upper limit of the attack impacts on MRNs, it still remains an open yet critical issue that motivates this work.
expressions and simplify the analysis, we adopt the first-order case in this paper.

Remark 1. The second-order controller approximates the real leader speed, and can be seen as a nonlinear first-order model $\dot{z}(t) = -Lz(t) + Lh(t) + u_0(t)$, where $u_0(t)$ is determined by the second-order controller design and satisfies $\lim_{t \to \infty} u_0(t) = c1$. In Section VII we will illustrate that our linear approximation method also applies to this nonlinear model if only using first-order states.

Obstacle avoidance via external interaction interface. The obstacle-avoidance mechanism is the major interface for MRNs to interact with the physical environment. Let $z_{ob}$ be the desired goal of $r_i$, $z_{ob}$ and $u_{ob}$ be the state and velocity of the obstacle, respectively. The obstacle-avoidance behavior is mainly determined by the relative positions between a robot and the obstacle, and their velocities. Therefore, regardless of the detail design of different algorithms, we formulate the universal avoidance behavior as a general mechanism

$$\dot{z}_i = g(z_{ob} - z_i, z_{ia} - z_i, v_{ob}, u_i).$$

(8)

Note that in multi-robot cases, $z_{ia}$ is usually time-varying and determined by $N_1^\text{in}$, and numerous obstacle-avoidance mechanisms do not consider the mobility of obstacles, i.e., the last parameter in $g(\cdot)$ may not be used (e.g., in artificial potential method and genetic approach). Besides, the influence of $(z_{ia} - z_i)$ is negligible when $\|z_{a} - z_i\|_2 \to R_o$, and the effect of the obstacle is dominant. Typically, the boundedness of $g(\cdot)$ is described as follows

$$g(\cdot) = 0, \quad \text{if} \quad \|z_{ob} - z_i\|_2 > R_o,$$

$$0 \leq |g(\cdot)| \leq b, \quad \text{if} \quad R_o \leq \|z_{ob} - z_i\|_2 \leq R_o,$$

$$|g(\cdot)| = b, \quad \text{if} \quad \|z_{ob} - z_i\|_2 < R_o.$$  

(9)

Formation maintenance. To deal with possible faults and hazardous interference in the environment, many methods have been developed to support autonomy and self-organization for interaction maintenance, e.g., restoring the interaction topology of splitting robot groups. In line with these considerations, we extract the main characteristics and formulate them as the following ruleset $\Omega = \{\Omega_R, \Omega_A\}$.

- Neighbor-connection restoration rule $\Omega_R$. For $r_i$, if $a_{ij}(t) \neq a_{ij}^0$, $\forall j \in N_1^\text{in}$ at time $t$, then $r_i$ will try to move back to its desired position $z_{ia}$ and reconnect with $r_j$, $\forall j \in N_1^\text{in}$. The necessary condition of successful restoration is that $z_{ia}$ is available.

- Neighbor-replacement authentication rule $\Omega_A$. Given $r_a \notin \mathcal{V}$, $i \in \mathcal{V}$ and a time slot $t_i$, $j \in N_1^\text{in}$ can be replaced by $r_a$ at $(t_0 + t_i)$ if and only if $\forall t \in \{t_0, t_0 + t_i\}$,

$$a_{ij}(t) \neq a_{ij}^0, \quad z_a(t) \in T(z_i(t), R_c),$$

$$\|z_a(t) - z_{ja}(t)\|_2 < \|z_j(t) - z_{ja}(t)\|_2.$$  

(10)

(11)

Remark 2. The reasonability and generality of the $\Omega$ lie in that it i) considers the prespecified neighborhood configuration, instead of merely proximity among robots as in many existing works; ii) works for situations where cyber authentication is not available, e.g., the interaction is purely based on sensors.

The existence of the internal interaction structure, the external interaction mechanism, the organization ruleset $\Omega$ and their distance-constrained characteristic constitute all the weak knowledge of the attacker about the MRN. The knowledge is natural for an external attacker and provides no explicit information about system structure, model or parameters.

D. Partial Observation Ability of The Attacker

Denote the sampling moment by $k$ and the discrete time form of (7) is given by

$$z^{k+1} = (I - \varepsilon_T L)z^k + \varepsilon_T u^k = Wz^k + \varepsilon_T u^k,$$  

(12)

where the sampling interval $\varepsilon_T$ is small enough, and $W$ is the interaction structure matrix. Note that $W$ equivalently reflects the internal interaction structure and effect as $L$, since they are all linear transformation of the adjacent matrix $A$. Therefore, we directly seek to obtain $W$ for revealing the structure in the following sections.

Suppose the observation of the attacker is with i.i.d. Gaussian noise $\xi_k^\mathcal{V} \sim N(0, \sigma^2 I)$, and it is given by

$$\tilde{z}^k = z^k + \xi_o^\mathcal{V} = Wz^{k-1} + \varepsilon_T u^k + \xi_o^\mathcal{V}.$$  

(13)

For every two consecutive observations, we obtain

$$\tilde{z}^k = W(\tilde{z}^{k-1} - \xi_o^{k-1}) + \varepsilon_T u^k + \xi_o^\mathcal{V} = Wz^{k-1} + \varepsilon_T u^k + \xi,$$  

(14)

where $\xi = \xi_o - W\xi_o$. Note that (14) only illustrates the quantitative relationship between two consecutive measurements and does not represent the essential dynamic process.

Next, denote the partially observable part of $\mathcal{V}$ by $\mathcal{V}_F$, and use the smallest enclosing circle covering $\mathcal{V}_F$ with radius $R_F$. For convenience, we assume $R_F \geq 2R_c$. Since a robot will only use information from their neighbors within its interaction range, for the robots near the observation boundary, their neighbors may not all be in $\mathcal{V}_F$, making it hard to infer the interaction structure in $\mathcal{V}_F$ with high accuracy. To deal with this issue, we narrow down the inferring range and use a concentric circle to cover the feasible subset $\mathcal{V}_H \subseteq \mathcal{V}_F$ with radius $R_h$, as shown in Fig. 1.
Stage 3.

Fig. 2. The whole scheme of our proposed sneaking attack. First, at Stage 1 and 2, $r_a$ leverages $D_c$ and $D_s$ to infer the steady pattern parameters and $W$. At Stage 3, $r_a$ makes tentative excitation on $r_a$ and and regresses $g$ based on the observed response dataset $D_s$. Meanwhile, the interaction radius $R_c$ is estimated and used as feedback to further optimize $W$. Finally, at Stage 4, $r_a$ begins its sneak with the support of the learned rules. And the response dataset $D_s$ can also be used to expand the data for regressing $g$.

E. Problem of Interest

An MRN $G = (V, E)$ of $N$ robots is deployed to execute mission in physical environment, while running to a goal position $z_g$ with specified formation shape configuration $\{h_{ij}\}$. A malicious attack robot (denoted as $r_a$) who has limited observation over $V_p \subseteq V$, aims to sneak into $V$ by replacing a victim robot (denoted as $r_v$).

To achieve above purpose, $r_a$ needs to acquire sufficient interaction knowledge about $V$. Note that what is most regular to $r_a$ is the steady formation shape, therefore, $r_a$ can first identity the steady pattern and then determine the convergence process, which reflects the internal interaction structure in $V$. Since a robot in $V$ has to react to the obstacles nearby, $r_a$ can actively make excitation on the robot to learn the external interaction rule. With the interaction rules obtained, $r_a$ begins the sneak attack efficiently. Accordingly, we divide the whole process into four stages: formation shape convergence (observe), steady formation maintenance (observe), tentatively excitation (explore), and attack launching (sneak). The observations on the four stages are constructed as four datasets: $D_c$, $D_s$, $D_a$, and $D_v$. Overall, to achieve the sneak attack, we need to solve the following four problems.

- **Stage 1:** Given $D_a$, infer the steady pattern $\hat{h}$, $\hat{c}$.
- **Stage 2:** Given $D_c$, $\hat{h}$ and $\hat{c}$, find the mapping relation $\phi$ that embodies $W$ by solving

\[
\min_{\phi(D_c)\rightarrow W} \| W - \hat{W} \|_{\text{Frob}}. \tag{15}
\]

- **Stage 3:** given $D_e$, find the mapping relation $\varphi$ that embodies $g$ by solving

\[
\min_{\varphi(D_e)\rightarrow g} \| g - \hat{g} \|_2. \tag{16}
\]

- **Stage 4:** given $\hat{W}$ and $\hat{g}$, design a control strategy $u_{a,0:H} = \{u_{a_0}^1, u_{a_1}^1, \ldots, u_{a_H}^1\}$ such that

\[
V(t_H) = (V(t_0) \backslash \{r_v\}) \cup \{r_a\}. \tag{17}
\]

By solving the problems sequentially, $r_a$ is enabled to learn the interaction rules and leverage them to implement sneak attack. The whole framework with details is shown in Fig. 2.

![Fig. 3. Illustration of the approximation of the interaction rules. The formation state evolution is governed by the interaction rules, and the observed state at instant $k$ is a resulting output of the interaction rules taking the observed state at instant $k-1$ as input (possibly with preprocessing).](image)

IV. REVEALING THE INTERACTION RULES

In this section, we first analyze the feasibility of revealing the internal and external interaction rules of an MRN, and then highlight the methods addressing the closely related problems in Stage 1-3, respectively. Note that the interaction range $R_c$ is estimated by active excitation in Stage 3 and is used to approximate a more informative internal interaction structure than the one obtained in Stage 2. The obtained results are leveraged to constitute the cornerstone for the sneak attack.

A. Feasibility Analysis

To reveal the interaction rules from the observations, there are two foremost issues that need to be addressed. First, under what condition the observations are meaningful and reflect the interaction rules. Second, how large the observations amount is sufficient to approximate the interaction rules with tolerable errors. If these issues are settled, the problem is then converted to parameter identification of a given system model or model fitting from a statistic perspective, and different methods are adopted to approximate the two kinds of interaction rules, as shown in Fig. 3. The details are given below.

For the internal interaction rule, what matters most is the structure among the robots. Therefore, the classical linear state space equation is sufficient to approximate the internal interaction rule, where the structure is explicitly represented as the state transition matrix. Under this model, the widely used least square method (LSM) provides an efficient way to obtain the optimal parameter estimation in the sense of minimizing...
the observation errors \[s\]. Note that we can only approximate \(W\) locally due to the partial observation nature.

For the external interaction rule, the obstacle-avoidance mechanism is fundamentally needed for a robot, and the avoidance behavior is inevitable if an obstacle is involved. Our major focus is to exploit how the robot will react to a close obstacle by \(g\), not necessarily seeking the explicit analytical expression of \(g\), especially considering its wide varieties. Therefore, we adopt generic learning-based methods to approximate the external interaction rule. Besides, due to the distance-constrained interaction, the interaction radius \(R_c\) can be inferred through active excitation, and this result is utilized to expand the approximation range of a local \(W\).

### B. Steady Pattern Identification

The steady pattern of the MRN reflects the formation shape and moving speed of the MRN.

Assume that \(r_a\) begins its observation as the MRN begins forming the formation shape from an unstable pattern, and \(\mathcal{V}_h\) is initially determined by a small \(R_h\) (e.g., \(R_h = 0.3R_f\)). When the formation pattern is reached, its state dynamics are illustrated by the following result.

**Theorem 1.** For the global dynamic model \([2]\) with \(u = Lh + [0 \cdots 0 c]^T\), we have

\[
\lim_{t \to \infty} \|z(t) - ct \cdot 1 - s\|_2 = 0,
\]

where the offset vector \(s = q_1 p_1^T z(0) + (I - q_1 p_1^T) h + \sum_{i=2}^{N} \epsilon_i \lambda_i c_i q_i\).

Theorem 1 illustrates that when the formation reaches the steady pattern, all robots are running at a common speed with fixed relative state deviations. This provides a theoretical foundation to identify the steady pattern parameters. Before that, let \(\Delta z^k_e = z^k_e - z^{k-1}_e\), \(d^k_{1e} = \|z^k_e - z^1_e\|_2\), and we define the \(l\)-period window as \([k, k+l]\). The second-order state difference accumulation of \(r_i\) during \(l\)-period is given by

\[
\Delta S^k_{i: k+l} = \sum_{k = k_0 + 1}^{k_0 + l - 1} \|\Delta z^{k+1}_i - \Delta z^k_i\|_2.
\]

Then, based on the observations, the steady velocity is obtained by solving

\[
\hat{c}(k_0, l) = \arg \min_c \sum_{k=k_0}^{k_0+l} \|z^k_F - (c \varepsilon_T k + b_0) 1\|_2,
\]

where \(b_0\) is an auxiliary constant. Note that \([20]\) can be easily solved by generic LSM. Next, define the real time when the steady pattern is reached as \(k_a\), and we present the following theorem to show how to identify the formation leader and the performance of estimated \(\hat{c}\).

**Corollary 1.** Given \(\mathcal{V}_F\) and \(k_a\), if the leader \(r_N \in \mathcal{V}_F\), then it is identified by

\[
\hat{r}_N = \arg \min_i \left\{ \Delta S^{2:k_a} : \Delta S^{2:k_a} < \epsilon, i \in \mathcal{V}_F \right\},
\]

where \(\epsilon\) is an arbitrarily small positive constant. \(\forall k_0 > k_a\), we have \(\lim_{l \to \infty} \hat{c}(k_0, l) = c\).

Corollary 1 is straightforward due to the uniqueness of \(r_N\) and the steady pattern characteristic. Thus the proof is omitted here. Note that smaller \(\Delta S^{k_0:k_a+l}\) means less velocity variation in \(r_i\), and it illustrates how to identify the leader and estimate the stable velocity. Based on it, given preset \(l\) and \(\epsilon\), the following criterion is designed to estimate \(k_a\), i.e.,

\[
\hat{k_a} = \inf \left\{ k_0 : \left( \sum_{i \in \mathcal{V}_F} \Delta S^{k_0:k_a+l}_i \right) \leq \epsilon \right\}.
\]

Once \(r_a\) obtains \(\hat{k_a}\), the datasets \(D_c\) are constructed by

\[
D_c = \{ z^k_F : k \leq \hat{k_a} \}, \quad D_s = \{ z^k_F : k > \hat{k_a} \},
\]

where \(z^k_F = [z^k_F, z^k_F, \ldots, z^k_F]_{(\mathcal{V}_F)}^T\). Meanwhile, the formation shape parameters \(\{ h_i \}\) are calculated by

\[
\hat{h} = \hat{s} - \hat{s} 1,
\]

where \(\hat{s} = \sum_{k=k_a+1} z^k_F/(\hat{s} - \epsilon F k \cdot 1)/l\).

### C. Internal Interaction Structure Approximation

After identifying the steady pattern, we then try to extract the interaction structure among \(\mathcal{V}_F\).

Denote the unobserved robot set as \(\mathcal{V}_{F'} = \mathcal{V} \setminus \mathcal{V}_F\), and define the indicative leader vector

\[
\|\hat{f}\| = \begin{cases} 1, & \text{if } \exists i \in \mathcal{V}_F, i = \hat{r}_N, \\ 0, & \text{otherwise}. \end{cases}
\]

Then, the global dynamics \([14]\) is divided into

\[
\begin{bmatrix} z_{k+1}^c_F \\ z_{k+1}^e_F \end{bmatrix} = \begin{bmatrix} W_{FF} & W_{F'F} \\ W_{F'F'} & W_{F''F''} \end{bmatrix} \begin{bmatrix} z_{k}^c_F \\ z_{k}^e_F \end{bmatrix} + \varepsilon_T \begin{bmatrix} u_{k}^c_F \\ u_{k}^e_F \end{bmatrix},
\]

where \(u_F = h_F + \epsilon \lambda_F \) and \(u_{F'} = h_{F'} + \epsilon \lambda_{F'}\). Accordingly, the observations of \(r_a\) over \(\mathcal{V}_F\) is given by

\[
z_{k+1}^c_F = W_{FF} z_{k}^c_F + W_{F'F} z_{k}^e_F + \varepsilon_T \hat{u}_F + \xi_F^k.
\]

Based on \([27]\), there are two points that need to be noticed:

- For \(r_a\), it can only observe \(z^c_F\), unaware of \(W_{F'F}\) and \(z^e_F\);
- The evolution of \(z^e_F\) is a coupled consequence of \(z^c_F\) itself and the unobservable \(z^e_F\).

Therefore, it is quite difficult to directly solve \(W_{FF}\) by \([27]\).

To avoid the above issue, we narrow down the inference range from \(\mathcal{V}_F\) to a smaller \(\mathcal{V}_h\). Let \(\mathcal{V}_h = \mathcal{V}_F \setminus \mathcal{V}_h\), \(W_{FF} = [W_{HH} \ W_{Hh}^T, \ y_F^k = z^k_F - \hat{h} - \varepsilon_T \lambda_F \) and \(y_{F'}^k = [(z_{k}^c_F - \hat{h})^T, (z_{F'}^c)^T]^T\). We obtain the following result of approximating the structure.

**Theorem 2.** Given \(D_c\) and \(\hat{k_a}\), if \(D_c\) is linearly modeled by \(r_a\), then in the sense of expectation, the observations satisfy

\[
E(y_{F'}^{k+1}) = W_{HF} E(y_{F'}^k).
\]

If \(|\mathcal{V}_F| + 1 \leq |D_c|\), then the optimal estimation of \(\phi(D_c)\) is

\[
\phi(D_c) = \tilde{W}_{HF} = \begin{bmatrix} (Y_F Y_F^T)^{-1} Y_F Y_{H}^T \end{bmatrix}^T,
\]

where \(Y_{H} = [y_{H}^2, y_{H}^3, \ldots, y_{H}^l]\) and \(Y_{F} = [y_{F}^2, y_{F}^3, \ldots, y_{F}^{l-1}]\).

Theorem 2 gives the least square solution of \(W_{HF}\) under the linear approximation model. Although the number of feasible
observations is limited in practice. Theorem $\text{[2]}$ nevertheless can be used as the basis for approximating $W_{HF}$, especially to obtain a robust connection structure even the real model is nonlinear and with different noise variance, which will be verified in Section $\text{[VI]}$.

D. External Interaction Rule Approximation

Next, we present the tentative excitation based method to how infer the interaction radius $R_e$ and construct dataset $D_e$ for learning the external interaction rule $g$.

Definition 1. (Direct controllability) A node is directly controllable if one can control it to reach any given state $z_i^\ast$ in finite steps by direct external excitations.

Lemma 1. If $g$ and $z_i^\ast$ is known, $\forall i \in V_{P}$, $r_i$ is directly controllable by $\tau_a$.

Lemma $\text{[1]}$ shows that $r_i$ can be steered to any state by utilizing the characteristic of $g$. Given the input configuration of $g$, the avoidance behavior is unique. Therefore, as in $\text{[11]}$, we make $\tau_a$ actively excite on $r_i$ and observe its external interaction response to learn $g$.

First, based on the analysis in last section, for $i \in V_{P}$, its desired position of $z_i^\ast$ is estimated by

$$z_i^{k+1} = \begin{cases} \hat{c} \cdot k + \hat{s}[i], & \text{if } N_i^{\text{in}} \text{ is in steady pattern;} \\ \sum_{j \in V} \hat{a}_{ij}(\hat{z}_j - z_i^k - h[j] + h[i]), & \text{otherwise,} \end{cases}$$

where $\hat{a}_{ij} = \hat{u}_{ij}/\varepsilon_r$ ($i \neq j$). The next implicit issue is the obstacle detection radius $R_o$, which can be directly inferred by approaching $r_i$ from a distant position.

Then, the excitation strategy is designed considering two possible situations. If there $\exists i \in V_{H}, |N_i^{\text{in}}| > 1$, we randomly select a $j \in N_i^{\text{in}}$ as the direct excitation target. Note that the excitation is adopted when $N_j^{\text{in}}$ is in steady pattern, thus $z_j^\ast$ is available. The excitation input is designed such that $u_{e}$ is orthogonal to the ideal moving direction of $r_j$, $\hat{d}_{r}(z_j^\ast)$, i.e.,

$$\{ u_e : u_e = \lambda \hat{d}_{r}(z_j^\ast), \| u_e \|_2 \leq b, \| z_a(u_e) - z_j^\ast \|_2 < \bar{R_e} \},$$

where $\lambda > 0$ and $\perp$ means the orthogonal vector. Since $r_i$ is an out-neighbor of $r_j$, when within the interaction range, its state is predicted by

$$z_i^{k+1} = \hat{W}_{HF}[i,z_i^k] + \varepsilon_r \hat{u}_k.$$  

(32)

Once the continuous excitation of $\tau_a$ makes $r_i$ lose connections with any one in $N_i^{\text{in}}$, the deviation $\| z_i^{k+1} - z_i^k \|_2$ will be significant large, which inspires us to design the following criterion to estimate $R_e$, given by

$$\begin{cases} k_e = \min \{ k : \| z_i^{k+1} - z_i^k \|_2 > \beta \}, \\ \bar{R_e} = \max \{ \| z_i^k - z_i^j \|_2 : j \in N_i^{\text{in}} \}, \end{cases}$$

(33)

where $\beta > 0$ is a given threshold. Technically, a larger $\beta$ will guarantee a more conservative $\bar{R_e}$.

If there $\forall i \in V_{H}, |N_i^{\text{in}}| \leq 1$, we randomly select a $r_i$ with $|N_i^{\text{in}}| = 1$ as the direct excitation target. In this case, we introduce a time window $k_l$ to design an intermittent excitation strategy. At each iteration $k$ satisfying $[k \text{ mod } k_l = 0]$, $u_e(k)$ is randomly selected from

$$\{ u_e : z_a(u_e) = \alpha z_i + (1 - \alpha) z_i, \| z_a(u_e) - z_i^\ast \|_2 < \bar{R_e} \},$$

(34)

and $\tau_a$ stays still at other iterations. Likewise, the same judging criterion $\text{[14]}$ is used to estimate $R_e$ at iteration $k$ satisfying $[k \text{ mod } k_l = k_l - 1]$. Once a $R_e$ is estimated, $\tau_a$ does reverse excitation to steer the robot to form the original steady pattern, and observes more obstacle-avoidance behaviors.

Finally, with $R_e$ determined, $V_{H}$ is re-specified by setting $R_h = R_f - R_e$, and a more informative $W_{HF}$ is further approximated by $\text{[29]}$. During the whole process of this stage, the avoidance behavior corresponding to every active excitation is recorded as the following input-output pair

$$\begin{cases} Q^{k}_{in} = [z_v^k - z_{a}^k, z_v^{k} - z_{v}^{k}, \Delta z_v^k/\varepsilon_r, \Delta z_v^k/\varepsilon_r], \\ Q^{k}_{out} = \Delta z_v^{k+1}. \end{cases}$$

(35)

Further, construct the dataset $D_e = \{ \cup (Q_{in}^{k}, Q_{out}^{k}) \}$, and $g$ can be learned using many mature learning methods by solving

$$\hat{g} = \arg \min_{g : Q_{in}^{k} \in Q_{out}^{k}} \sum_{k=1}^{D_e} ||Q_{out}^{k} - g(Q_{in}^{k})||_2.$$  

(36)

Specifically, we adopt SVR method, which has good performance on nonlinear approximation and strong generalization ability when the amount of data is not vast $\text{[48]}$.

At the end of this stage, $R_e, W_{HF}$ and $\hat{g}$ are all obtained, providing support to design efficient sneak strategies.

V. SNEAK ATTACK DESIGN

In this section, we first analyze the attack feasibility by introducing the definitions of 1-hop convex formation and the indirect controllability of a robot. Then, the sufficient conditions for the attack are established. Finally, we propose the ECR strategy to dynamically replace $r_v$ by $\tau_a$, completing sneak.

A. Feasibility Analysis

In this part, we give the theoretical guarantees for the existence of attack positions and the controllability of robots.

Note that the success of the attack lies in two parts: i) there exists a feasible attack position and ii) $r_v$ is controllable such that the attack condition is satisfied. Accordingly, we introduce the following definitions.

Definition 2. (1-hop convex pattern) Given $r_v$, if $\exists \mathcal{V}_{P} \subseteq \{ i \cup N_i^{\text{out}} \}$ such that i) the nodes in $\mathcal{V}_{P}$ constitutes a convex polygon; ii) the polygon covers $\{ i \cup N_i^{\text{out}} \}$; iii) $i$ is one vertex of the polygon, then $\mathcal{V}_{P}$ is the 1-hop convex pattern of $r_v$.

Definition 3. (Indirect controllability) A node is indirectly controllable if one can control another node, and a let a chain reaction make the tagged node reach any $z_i^\ast$ in finite steps.

Theorem 3. Given $r_v$, if $\mathcal{V}_{P}$ exists, then

1) $\mathcal{V}_{P}$ is unique.
2) $Z_i^{\ast} = \bigcap_{l \in \mathcal{P}(z_j, d_{ij}) \neq \emptyset} \{ z \in Z_i \}, j \in N_i^{\text{out}}.
\forall z \in Z_i^{\ast}, j \in N_i^{\text{out}}.$
Theorem 3 shows the nice distance properties brought by $V^p_i$, which helps to the sneak strategy design. Besides, in its proof in Appendix, we also provide a method to find the positions that satisfy the property. Next, we illustrate under what conditions the robots are indirectly controllable.

Suppose that $i \in V$ is under the excitation of $r_a$, and it can be seen as another leader. Then, $z_i$ is directly determined by $u_c = g(r)$. In this situation, denote the new adjacent matrix as $A^e$ where $a^e_{ij} = 0, \forall j \in N^i_{\text{out}},$ and other elements are the same as in $A$. Accordingly, its Laplacian matrix is $L^e = \text{diag}(A^e \mathbf{1}) - A^e$, and $p^e_i = [p^e_{1i}, \ldots, p^e_{N^i, i}]^T$ is the corresponding left eigenvector for $\lambda_1$ of $L^e$.

Lemma 2. Given desired state $z^e_i$ and initial state $z^0_i$, $r_i$ is indirectly controllable by $r_j$ if the following conditions hold

$$
\begin{align}
\sum_{j \in N^i_{\text{out}}} a_{ij} u_c > 0, & \quad \text{if } (z^e_i - z^0_i) u_c > 0, \\
|p^e_{ij} u_c| > |p^e_{j, i} u_c|, & \quad \text{if } (z^e_i - z^0_i) u_c < 0.
\end{align}
$$

Lemma 2 points out the necessary and sufficient condition for indirect controllability from the perspective of global connectivity. However, under partial observation, the eigenvectors of the interaction matrix are hard to obtain, making it impossible to verify the conditions. To overcome this issue, we leverage the idea of Lemma 2 and obtain the local conditions that guarantee the direct controllability.

Theorem 4. Given desired state $z^e_i$ and initial state $z^0_i$, $r_i$ is indirectly controllable by $r_j$ when $u_c, u_c$ satisfy

$$
\begin{align}
\sum_{j \in N^i_{\text{out}}} a_{ij} u_c > 0, & \quad \text{if } (z^e_i - z^0_i) u_c > 0, \\
|a_{ij} u_c| > |\bar{a}_{ij} u_c|, & \quad \text{if } (z^e_i - z^0_i) u_c < 0,
\end{align}
$$

where $\bar{a}_{ij} = \sum_{j' \in \{N^i_{\text{out}} \setminus \{i\}\}} a_{ij'}$.

Without knowing the global interaction structure in $V$, Theorem 4 provides a sufficient criterion to find the robots satisfying the indirect controllability by considering the local interaction with their in-neighbors. This condition will be used in the following strategy design.

B. Sneak Strategy: Evaluate-Cut-Restore

To achieve maximum attack rewards, a feasible $r_v$ needs to be selected based on its significance evaluation in the formation first, and then $r_a$ is controlled to replace $r_v$. Besides, the strategy design should be flexible for different local geometric patterns of $r_v$. To meet the neighbor-replacement rule $\Omega_A$, the key point is to ensure the existence of $V^p_i$. Briefly, the ideas of our proposed sneak strategy are summarized as follows.

- **Evaluate** the significance of the robots based on their potential indirect controllability and the state-propagation effects. Select the most valuable one as $r_a$.
- **Cut** the connections between $r_v$ and $N^i_{\text{out}}$. If the 1-hop convex pattern $V^p_i$ does not exist, $r_a$ needs to make $V^p_i$ form first.
- **Restore** the original steady pattern, by making $r_a$ be regarded as the in-neighbor of $N^i_{\text{out}}$ based on ruleset $\Omega$ and replacing $r_v$ by $r_a$.

During the sneak stage, the estimated state of $r_v$ under attack and the state of $r_a$ are respectively given by

$$
\begin{align}
\hat{z}^{k+1}(u_a^k) = \hat{z}^k + \hat{g}(u_a^k), \\
\hat{z}^{k+1}_a = z^k_a + u^k_a,
\end{align}
$$

$\hat{g}(u_a^k)$ is simplified for $\hat{g}(z^k_a - z^k_i, z^k_a - z^k_i, u^k - c^k_i)$.

The details of ECR strategy are given below.

**Evaluate phase.** With $W_{HF}^i$ obtained, we need to find a victim robot to achieve the maximum rewards. Note that for a robot in the MRN, a larger out-degree means it has the potential capability to control more robots while a smaller in-degree indicates it is less affected by others. From this perspective, the evaluation criteria is designed as

$$
\begin{align}
\max & \quad (|N^i_{\text{out}}| + \|W^i_{HF}^i\|_1 - |N^i_{\text{in}}| - \|W^i_{HF}^i\|_1) \\
\text{s.t.} & \quad i \in V, |N^i_{\text{out}}| \geq 1, |N^i_{\text{in}}| \leq \alpha_1,
\end{align}
$$

where $W^i_{HF}^i, W^i_{HF}^j$ represent the $i$-th column and row of $W_{HF}$, respectively, and $\alpha_1$ a preset integer. The solution of (41) is selected as $r_v$. Due to the small scale of the observed formation, (41) can be easily solved by a common traverse search method with algorithm complexity of $O(|H||F|)$.

**Cut phase.** In this core phase, $r_a$ aims to make the connections between $r_v$ and its in-neighbors break, i.e., $a_{ij}(t) \neq a^0_{ij}$. If $V^p_i$ exists and $r_v$ is readily to be excited directly (i.e., not many other robots are distributed around), the following strategy is adopted to break the connections,

$$
\begin{align}
\max & \quad \alpha_2 \|\hat{z}^{k+1}_v(u_a^k) - \hat{z}^{k+1}_v\|_2 + \alpha_3 \sum_{j \in N^i_{\text{in}}}|\hat{z}_v^{k+1} - \hat{z}_v^{k+1} - \bar{h}_{j, v}|_2, \\
\text{s.t.} & \quad (39), (40), (42a), (42b), (42c)
\end{align}
$$

where $\alpha_2, \alpha_3 > 0$ are the weight parameters to balance the offsets of $r_v$ with its ideal position and in-neighbors. An efficient way to solve this cut-edge problem is to adopt a greedy heuristic by sampling from the feasible solution space.

The attack iteration under (42) is terminated by the same criterion (43) for estimating $R_c$ in Section IV-D.

If $V^p_i$ does not exist or the $r_v$ can not be attacked readily, we utilize the indirect controllability to attack an in-neighbor of $r_v$ first, such that the formation pattern $V^p_i$ is reached and $r_v$ is easier to approach. Let $r_{l_1}, r_{l_2}$ be the two robots in $N^i_{\text{out}}$ that are closest to $r_j$, and $z_{l_1}, z_{l_2}$ be the vector from $z_{l_1}$ to $z_{l_2}$.

Then, the following strategy is adopted

$$
\begin{align}
\arg \max_{u_a} & \quad \max_{u_a} \left\{ \|\hat{z}_v^{k+1} - \hat{z}_v^{k+1} \|_2 : u_a \in \mathcal{U}_F, j \in N^i_{\text{in}} \right\} \\
\text{s.t.} & \quad (38), (42c)
\end{align}
$$

where $\mathcal{U}_F = \{u_a : \|u_a\|_2 < b, u_a = \lambda z_{l_1} z_{l_2}^\top, \forall \lambda > 0 \}$. Iteratively, $r_a$ updates the control inputs until $V^p_i$ is formed, then the control mode is turned to (42).

**Restore phase.** After the $V^p_i$ is formed and the connections between $r_v$ and $N^i_{\text{out}}$ are cut, $r_v$ only needs to be in a position
Algorithm 1 Sneak Attack against MRNs

**Input:** Partial observation range $R_F$, moving ability bound $b$.

**Output:** Interaction rules $W_{HF}$, $g$.

1. Observe the dynamic process of $V_F$ converging to the steady formation geometric pattern.
2. Judge when the steady pattern is reached by \((22)\).
3. Construct datasets $D_c$, $D_s$, and estimate the parameters of steady pattern by \((23)\).
4. Obtain an initial approximation of $W_{HF}$ based on $D_c$ by \((29)\).
5. Leveraging direct controllability, make tentative excitation on $r_j$ continuously to infer $R_i$, $R_c$ by \((33)\).
6. Expand the approximation range of $W_{HF}$ utilizing $R_c$.
7. Construct dataset $D_a = \{Q^k_{in}, Q^k_{out}\}$ during the excitation process, and learn the external interaction mechanism $g$ by \((36)\).
8. Leveraging indirect controllability, adopt ECR (Evaluate-Cut-Restore) attack strategy to replace a selected $r_u$ by $r_a$.
9. Construct dataset $D_a = \{Q^k_{in}, Q^k_{out}\}$ during the sneak attack process, and update $g$ online by \((36)\).
10. Obtain partial control over $V_F$ and support further attacks.

that is close to arbitrary $j \in N^r_{v}$. Utilizing the properties in Theorem $[3]$ $r_a$ is controlled by
\[
u^k_{a} = \text{arg} \max_{u} \{\|z^k_{v}+1(u_a) - \hat{z}^k_{v} + 1\|_2 : \hat{z}^k_{v} + 1 \in Z_{v}^f\}\]. (44)

By continuously implementing the procedure, $r_a$ takes the ideal position that belongs to $r_u$, and will be regarded as the real $r_u$ by $r_u$’s out-neighbors at certain time according to rule $\Omega_A$. After that, the original $r_u$ becomes an outlier and $r_a$ is controlled to move towards $\hat{z}_{v_a}$ and $z_a \in P(z_j, R_c)$. Finally, $r_a$ is recognized as a member and obtains partial control over $V$. The sneak attack is completed.

During this attack-implementing stage, $r_a$ also collects dataset $D_a = \{Q^k_{in}, Q^k_{out}\}$ and uses it to update $\tilde{g}$ online. After sneaking into the MRN, $r_a$ is able to implement further attacks, for example, infer the interaction structure in $V_H'$, or intentionally split the MRN by misleading $N^r_{out}$ and the out-neighbors of them. These interesting problems are not the focus of this paper and are omitted here.

To sum up, the whole procedures of the sneak attack consisting of four stages are summarized in Algorithm 1.

**VI. SIMULATION**

In this section, we conduct extensive simulations to demonstrate the feasibility of revealing the interaction rules from external observations and excitation, and also validate the theoretical analysis and the proposed sneak attack strategy.

**A. Simulation Setting**

**MRN specification.** An MRN consisting of 17 robots is considered, with two kinds of interaction structure and common preset formation shape, as shown in Fig. 4. Specifically, robot 1 is set as the leader, and the moving speed in stable stage is set as $0.2 \text{m/s}$. The maximum speed of $r_a$ is $1 \text{m/s}$, and the radii are setting as $R_c = 7 \text{m}$, $R_s = 2 \text{m}$ and $R_a = 0.5 \text{m}$.

**Comparisons under different models and parameters.** For the interaction structure $W_{HF}$, we present the approximation results from three perspectives. First, we adopt the linear model $\hat{z}(t) = -Lz(t) + LH + u_0$ and the nonlinear model $\hat{z}(t) = -Lz(t) + LH + u_a(t)$, respectively. Second, we consider the influence of different sample amounts and different observation noise variance. Additionally, $\hat{W}_{HF}$ can be further optimized by considering the feedback of $R_c$, i.e.,
\[
\begin{align*}
\min_{\hat{W}_{HF}} &\|Y_H - \hat{W}_{HF}Y_F\|_{nab} \\
\text{s.t.} &\ W_{HF}^{[i,j]} = 0, \text{if } \|\hat{z}_i - \hat{z}_j\|_2 > \tilde{R}_e, i \in V_H, j \in V_F. 
\end{align*}
\]
As a typical constrained linear least square problem, \(45\) can be solved by many mature optimization techniques, e.g., Newton interior-point method \([49]\). For the external interaction mechanism $g$, we present the approximation results under different sample amounts and different noise variance.

**Metric of evaluation.** To evaluate $\hat{W}_{HF}$, we use the following two indexes
\[
\begin{align*}
\varepsilon_1 &= (\|\text{sign}(\hat{W}_{HF}) - \text{sign}(W_{HF})\|_0) / (|V_H||V_F|), \\
\varepsilon_2 &= (\|\hat{W}_{HF} - W_{HF}\|_{\text{Prob}}) / (\|W_{HF}\|_{\text{Prob}}),
\end{align*}
\]
where $\varepsilon_1$ evaluates the structure correctness in terms of whether two robots have an interaction connection, and $\varepsilon_2$ represent the magnitude correctness in terms of how larger is the connection weight between two robots. To evaluate $\tilde{g}$, we adopt mean directional accuracy (MDA), root mean square error (RMSE) and mean absolute error (MAE), which are respectively calculated by
\[
\begin{align*}
\text{MDA} &= \frac{1}{m} \sum_{i=1}^{m} \text{sign}(y_i - y'_i), \\
\text{RMSE} &= \sqrt{\frac{1}{m} \sum_{i=1}^{m} (y_i - y'_i)^2}, \\
\text{MAE} &= \frac{1}{m} \sum_{i=1}^{m} \frac{|y_i - y'_i|}{m},
\end{align*}
\]
where $y_i, y'_i$ are the actual and predicted values, $m$ is the amount of samples.

**B. Results and Analysis**

We mainly illustrate the results from the perspectives of the four stages described in Section III-E.

**Stage 1.** Recall that the time instant $\hat{k}_a$ is computed by \((22)\) to identify when the MRN has reached the steady pattern.
Using different threshold $\epsilon$ to compute $\hat{k}_s$ will result in different sample number of $D_c$. As shown in Fig. 5(a) when the MRN reaches steady state, the velocity estimation remains stable. Fig. 5(b)-5(c) illustrate the sample number mainly affects the accuracy of $\hat{W}$. When the amount becomes larger, both $\epsilon_1$ and $\epsilon_2$ become stable. This is because that the latter observations in $D_c$ are observed from the stage that is close to the steady process, only providing redundant information to approximate $W_{HF}$. In fact, this demonstrates that an accurate calculation of $\hat{k}_s$ is not important under both linear and nonlinear models, especially for the structure error. Nevertheless, more data are still helpful to obtain $W_{HF}$ with smaller magnitude errors.

**Stage 2.** Hereafter, we present the results based on the interaction structure given in Fig. 4(a). Fig. 6 shows the approximation errors of the internal interaction structure under different variances of observation noises. The variance of observation noise varies from 0 to 0.5. Fig. 6(a) presents the approximation evaluation of the MRN under linear formation law. As it shows, the structure error $\epsilon_1$ is smaller than $\epsilon_2$, and when noises are involved, the approximation error is generally stable under different noise variances. Specifically, when the interaction radius feedback is used to further optimize $W_{HF}$, i.e., solving (45), the approximation errors are reduced significantly. The details in Fig. 6(b) is likewise, and under the same conditions other than the nonlinear formation control, the approximation errors are basically larger than that under linear formation control, which is not hard to understand. However, we observe that even though the approximation errors in the nonlinear case is higher, the difference is not significant. The errors remain small and are sufficient to get a feasible $W_{HF}$ to support the following attack, especially in terms of the connection structure. These results verify that the accuracy of the proposed linear approximation for $W_{HF}$.

**Stage 3.** To verify the approximation performance of the obstacle-avoidance mechanism (here we use classical artificial potential method [50]), SVM with a Gaussian kernel function is used for regression, and the parameters are optimized by 10-fold grid search cross-validation. We conduct 4 groups of regression with 3 repeated procedures based on $D_c$ collected from the tentative excitation process. The $\sigma = 0.1$ here. We randomly select 25, 50, 100, 200 samples to train the SVR model in each group, respectively. A fixed set of 120 samples are used for testing. The testing results are shown in Fig. 7 with the statistic results given in Table II. By comparing the results of the test samples in each group, it is obvious that the fitting performance is improved with more training data. Meanwhile, the index does not vary much with more samples, which is illustrated by comparing the results of repeated tests. The MDA result shows a rising trend from 25-sample-training to 200-sample-training, which indicates that more training samples lead to high accuracy. Nevertheless, we observe that even though a larger number of samples bring more accurate results, the improvement of the accuracy is not significant.

![Image](image64x617.png)

**Fig. 5.** The approximation results based on calculated $\hat{k}_s$. (a) Formation velocity estimation. (b) and (c) are the approximation results with increasing data amount of $D_c$ structure case 1 and 2, respectively.

![Image](image229x617.png)

**Fig. 6.** The approximation result comparison of $W_{HF}$ with and without the feedback of $R_c$. (a) under linear formation control. (b) under nonlinear formation control.

| TABLE II | STATISTIC OBSTACLE-AVOIDANCE MECHANISM REGRESSION RESULTS BASED ON SVR METHOD. |
|----------|-----------------------------------------------------|
|          | 25 samples  | 50 samples  | 100 samples | 200 samples |
| Index    | MDA   | RMSE  | MAE  | MDA   | RMSE  | MAE  | MDA   | RMSE  | MAE  |
| Training | 0.880 | 0.233 | 0.154 | 0.913 | 0.217 | 0.113 | 0.933 | 0.581 | 0.300 |
| Testing  | 0.933 | 0.601 | 0.404 | 0.933 | 0.581 | 0.300 | 0.976 | 0.496 | 0.206 |

Overall, these show the effectiveness of the proposed method to learn the external interaction rule.

**Stage 4.** First, at the Evaluate phase, robot 5 is selected as $r_v$ by the evaluation criteria [41], which has only one in-neighbor and three out-neighbors, and its corresponding 1...
Fig. 7. Obstacle-avoidance mechanism regression results based on SVR method. Under different numbers of the samples, 3 groups of experiments are conducted for each sample number.

Fig. 8. The illustration of the sneak process. (a). The position errors between the real and the desired positions of the robots, and \( r_a \) takes the \( z^*_5 \) as its desired position. (b) The distance deviations \( (\|z_a - \tilde{z}_j\|_2 - \|\tilde{z}_i - \tilde{z}_j\|_2) \), where the deviations are all negative. Based on the neighbor-replacement authentication rule \( \Omega_A \), the robots \( N_{\text{out}}^5 \) will take \( r_a \) as the new neighbor replace robot 5. Finally, \( r_a \) here just moves towards \( z_5^* \) and its out-neighbors begin following it, and the formation will reach steady state again. Note that the position fluctuation of \( N_{\text{out}}^5 \) before beginning sneaking in Fig. 8(a) also verifies the indirect controllability in Theorem 4. Likewise, this can be used to intentionally split the MRN formation shape, and the results are omitted here due to space limits.

VII. Conclusion

In this paper, we investigated the security of MRNs under formation control by designing a sneak attack. We demonstrated that the interaction rules in MRNs are learnable even the attacker is only with partial observation over the MRN, without any strong prior knowledge like the system dynamics model or structure. First, we proposed an excitation-based method to approximate the internal interaction structure within the MRN and the obstacle-avoidance mechanism with the environment. Then, we designed the ECR strategies, which make the attacker replace a victim robot and gain optimal local control over the MRN. Finally, comprehensive theoretical analysis and numerical results illustrated the effectiveness of the proposed attack. This work reveals the possibility of learning the interaction rules of an MRN from physical observations and excitations, and shows how to utilize them.
to design an intelligent attack, even though the interaction rules are model agnostic to the attacker.

In a broader sense, our work broadens the horizons of the security of CPSs by exploiting the system vulnerabilities from physical observations and interactions. Furthermore, we emphasize that the system interaction nature can be leveraged by malicious attackers to cause disastrous consequences on the system. Concerning the CPS security from this perspective, a lot of issues remain to be further addressed, including i) how to design efficient detection methods to identify the potential threats; ii) how to reliably secure the interaction protocols that only leak confusing states on the external observer; and iii) how to construct robust and dynamic interaction defensive strategies with the physical world.

REFERENCES

[1] Y. Li, J. He, and L. Cai, “Topology Inference on Partially Observable Mobile Robotic Networks under Formation Control,” submitted to 2021 European Control Conference.
[2] F. Bullo, J. Cortes, and S. Martinez, Distributed control of robotic networks: A mathematical approach to motion coordination algorithms. Princeton University Press, 2009, vol. 27.
[3] R. Olfati-Saber and R. M. Murray, “Consensus problems in networks of agents with switching topology and time-delays,” IEEE Transactions on Automatic Control, vol. 49, no. 9, pp. 1520–1533, 2004.
[4] K.-K. Oh, M.-C. Park, and H.-S. Ahn, “A survey of multi-agent formation control,” Automatica, vol. 53, pp. 424–440, 2015.
[5] P. London, S. Vardi, and A. Wiernan, “Logarithmic communication for distributed optimization in multi-agent systems,” Proc. ACM Meas. Anal. Comput. Syst., vol. 3, no. 3, Dec. 2019.
[6] A. Sankararaman, A. Ganesh, and S. Shakkottai, “Social learning in multi agent multi armed bandits,” Proc. ACM Meas. Anal. Comput. Syst., vol. 3, no. 3, Dec. 2019.
[7] M. A. Kamel, X. Yu, and Y. Zhang, “Formation control and coordination of multiple unmanned ground vehicles in normal and faulty situations: A review,” Annual Reviews in Control, 2020.
[8] H. Choi, W.-C. Lee, Y. Aafer, F. Fei, Z. Tu, X. Zhang, D. Xu, and X. Xianyu, “Detecting attacks against robotic vehicles: A control invariant approach,” in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018, pp. 801–816.
[9] X. Fu and E. Modiano, “Fundamental limits of volume-based network dos attacks,” Proc. ACM Meas. Anal. Comput. Syst., vol. 3, no. 3, Dec. 2019.
[10] C. Liu, J. He, S. Zhu, and C. Chen, “Dynamic topology inference via external observation for multi-robot formation control,” in 2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), 2019, pp. 1–6.
[11] Y. Li, J. He, C. Chen, and X. Guan, “Learning-based intelligent attack against formation control with obstacle-avoidance,” in Proceedings of the 2019 American Control Conference. IEEE, 2019, pp. 2690–2695.
[12] R. Olfati-Saber, J. A. Fax, and R. M. Murray, “Consensus and cooperation in networked multi-agent systems,” Proceedings of the IEEE, vol. 95, no. 1, pp. 215–233, 2007.
[13] A. Pandey, S. Pandey, and D. R. Parhi, “Mobile robot navigation and obstacle avoidance techniques: A review,” International Robotics and Automation Journal, vol. 2, no. 3, p. 00022, 2017.
[14] C. W. Reynolds, “Flocks, herds and schools: A distributed behavioral model,” in Proceedings of the 14th Annual Conference on Computer Graphics and Interactive Techniques, 1987, pp. 25–34.
[15] X. Sun and C. G. Cassandras, “Optimal dynamic formation control of multi-agent systems in constrained environments,” Automatica, vol. 73, pp. 169–179, 2016.
[16] S. Zhao, "Affine formation maneuver control of multi-agent systems," IEEE Transactions on Automatic Control, vol. 63, no. 12, pp. 4140–4155, 2018.
[17] A. Alonso-Mora, P. Montijano, T. Nägeli, O. Hilliges, M. Schwager, and D. Rus, “Distributed multi-robot formation control in dynamic environments,” Autonomous Robots, vol. 43, no. 5, pp. 1079–1100, 2019.
[18] Y. Xu, S. Zhao, D. Luo, and Y. You, “Affine formation maneuver control of high-order multi-agent systems over directed networks,” Automatica, vol. 118, p. 109004, 2020.
[19] M. Deghat, I. Shames, B. D. O. Anderson, and C. Yu, “Localization and circumnavigation of a slowly moving target using bearing measurements,” IEEE Transactions on Automatic Control, vol. 59, no. 8, pp. 2182–2188, 2014.
[20] T.-H. Cheng, Z. Kan, J. R. Klotz, J. M. Shea, and W. E. Dixon, “Event-triggered control of multi-agent systems for fixed and time-varying network topologies,” IEEE Transactions on Automatic Control, vol. 62, no. 10, pp. 5365–5371, 2017.
[21] M. H. Trinh, S. Zhao, Z. Sun, D. Zelazo, B. D. O. Anderson, and H.-S. Ahn, “Bearing-based formation control of a group of agents with leader-first follower structure,” IEEE Transactions on Automatic Control, vol. 64, no. 2, pp. 598–613, 2018.
[22] Z. Kan, A. P. Dani, J. M. Shea, and W. E. Dixon, “Network connectivity preserving formation stabilization and obstacle avoidance via a decentralized controller,” IEEE Transactions on Automatic Control, vol. 57, no. 7, pp. 1827–1832, 2012.
[23] S. Zhao, Z. Li, and Z. Ding, “Bearing-only formation tracking control of multi-agent systems,” IEEE Transactions on Automatic Control, vol. 64, no. 11, pp. 4541–4554, 2019.
[24] Z. Feng, C. Sun, and G. Hu, “Robust connectivity preserving rendezvous of multi-robot systems under unknown dynamics and disturbances,” IEEE Transactions on Control of Network Systems, vol. 4, no. 4, pp. 725–735, 2016.
[25] M. Khalili, X. Zhang, M. M. Polycarpou, T. Parisini, and Y. Cao, “Distributed adaptive fault-tolerant control of uncertain multi-agent systems,” Automatica, vol. 87, pp. 142–151, 2018.
[26] C. Liu, B. Jiang, R. J. Patton, and K. Zhang, “Hierarchical-structured fault estimation and fault-tolerant control for multi-agent systems,” IEEE Transactions on Control of Network Systems, vol. 6, no. 2, pp. 586–597, 2019.
[27] H. Zhu, J. Juhl, L. Ferranti, and J. Alonso-Mora, “Distributed multi-robot formation splitting and merging in dynamic environments,” in Proceedings of IEEE International Conference on Robotics and Automation, 2019.
[28] Y. Li, H. Wang, J. He, and X. Guan, “Optimal topology formation scheme for multi-robot formation control,” in 28th International Symposium on Industrial Electronics. IEEE, 2019, pp. 1847–1852.
[29] L. Zhe, J. Ju, W. Chen, X. Fu, and H. Wang, “A gradient-based self-healing algorithm for mobile robot formation,” in Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems, 2015.
[30] Z. Liu, W. Chen, H. Wang, Y.-H. Liu, Y. Shen, and X. Fu, “A self-repairing algorithm with optimal repair path for maintaining motion synchronization of mobile robot network,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2017.
[31] Z. Liu, H. Wang, L. Xu, Y.-H. Liu, J. Lu, and W. Chen, “A failure-tolerant approach to synchronous formation control of mobile robots under communication delays,” in Proceedings of IEEE International Conference on Robotics and Automation, 2018.
[32] X. Dong and G. Hu, “Time-varying formation tracking for linear multi-agent systems with multiple leaders,” IEEE Transactions on Automatic Control, vol. 62, no. 7, pp. 3658–3664, 2017.
[33] H. Yang, Q.-L. Han, X. Ge, L. Ding, Y. Xu, B. Jiang, and D. Zhou, “Fault tolerant cooperative control of multi-agent systems: A survey of trends and methodologies,” IEEE Transactions on Industrial Informatics, vol. 16, no. 1, pp. 4–17, 2020.
[34] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715–2729, 2013.
[35] Y. Mo and B. Sinopoli, “On the performance degradation of cyber-physical systems under stealthy integrity attacks,” IEEE Transactions on Automatic Control, vol. 61, no. 9, pp. 2618–2624, 2015.
[36] H. Sandberg, S. Amin, and K. H. Johansson, “Cyber-physical security in networked control systems: An introduction to the issue,” IEEE Control Systems Magazine, vol. 35, no. 1, pp. 20–23, 2015.
[37] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, “Bibliographical review on cyber attacks from a control oriented perspective,” Annual Reviews in Control, vol. 48, pp. 103–128, 2019.
[38] F. Pasqualetti, A. Bicchi, and F. Bullo, “Consensus computation in cyber-physical systems,” IEEE Transactions on Automatic Control, vol. 60, no. 3, pp. 90–104, 2012.
[39] D. Silvestre, P. Rosa, J. P. Hespanha, and C. Silvestre, “Stochastic and deterministic fault detection for randomized gossip algorithms,” Automatica, vol. 78, pp. 46–60, 2017.
Then, define an auxiliary variable $z_{ss} = q_1p_1^T u_0 + q_1p_1^T z(0) + (I - q_1p_1^T) + \sum_{i=2}^{N} \frac{1}{\lambda_i} q_ip_i^T u_0$. Substituting \((53)\) into $z_{ss}$, we further obtain

$$z_{ss} = q_1p_1^T u_0 + q_1p_1^T z(0) + (I - q_1p_1^T) + \sum_{i=2}^{N} \frac{1}{\lambda_i} q_ip_i^T u_0. \quad (54)$$

Since $\tau_N$ is a unique leader and does not use information from others, the last row of matrix $A$ and $L$ are zeros. Then, the following equations hold

\[
\begin{align*}
    p_1^T L &= [p_{11}, \ldots, p_{1N}]^T L = [0, \ldots, 0], \\
    p_1^T q_1 &= [p_{11}, \ldots, p_{1N}]^T 1 = 1.
\end{align*}
\]

By solving \((55)\), we obtain

\[
\begin{align*}
    p_{1N} &= 1, \\
    p_{ik} &= 0, k = 1, 2, \ldots, N - 1.
\end{align*}
\]

Substituting \((56)\) into \((54)\) and it follows that

$$z_{ss} = q_1p_1^T z(0) + (I - q_1p_1^T) + \sum_{i=2}^{N} \frac{Cp_{iN}}{\lambda_i} q_i + ct \cdot 1 = s + ct \cdot 1 \quad (57)$$

Finally, it is derived that $\lim_{t \to \infty} ||z(t) - ct - 1||_2 = 0$.  \(\Box\)

B. Proof of Theorem 2

Proof. Here we adopt the limit analysis method. First, if $R_f = R_c$ (i.e., the circle center locates on a robot $i$), then $N_{i/n} \subseteq \mathcal{V}_r$, which yields

$$z_{i}^{k+1} = W_{f/r}^{[i,:]} z_{i}^{k} + \varepsilon_T \hat{u}_{i}^{k} + \xi_{i}^{k}, \quad (58)$$

where $W_{f/r}^{[i,:]}$ represents the corresponding row for $z_i$. By moving terms, it follows that

$$W_{f/r}^{[i,:]} z_{i}^{k} = z_{i}^{k+1} - \varepsilon_T \hat{u}_{i}^{k} - \xi_{i}^{k} = y_{i}^{k+1} - \xi_{i}^{k}. \quad (59)$$

Suppressing the observations are noise-free and no other prior information is available, then $|\mathcal{V}_r|$ groups of observation equations are sufficient to solve $W_{f/r}^{[i,:]}$. This case shows that robot $r_i$ is only influenced by its in-neighbors that are within its communication range.

Next, if $R_f > R_c$, then $\exists \hat{i} \in \mathcal{V}_h \subseteq \mathcal{V}_r, \{i \cup N_{i/n} \} \subseteq \mathcal{V}_r$. Therefore, \((58)\) is generalized as

$$z_{i}^{k+1} = W_{h/f} z_{i}^{k} + W_{h/r} \hat{z}_{h} + \varepsilon_T \hat{u}_{i}^{k} + \xi_{i}^{k} = W_{h/f} z_{i}^{k} + \varepsilon_T \hat{u}_{i}^{k} + \xi_{i}^{k}. \quad (60)$$

Substitute $\hat{u}_{i} = \hat{h}_{i} + \hat{e}_{i}^{k}$ into \((60)\) and it follows that

$$z_{i}^{k+1} = W_{h/f} z_{i}^{k} + \varepsilon_T \left( \hat{e}_{i}^{k} + I - W_{h/r} \right) \hat{h}_{i}$$

$$= W_{h/r} \left( z_{h}^{k} - \hat{h}_{i} \right) + W_{h/r} \hat{z}_{h} + \varepsilon_T \hat{e}_{i}^{k} + \hat{h}_{i} + \xi_{i}^{k} \quad (61)$$

By the definition of $y_{h}$ and $y_{r}$, we obtain

$$y_{h}^{k+1} = z_{h}^{k+1} - \varepsilon_T \hat{e}_{i}^{k} - \hat{h}_{i}$$

$$= W_{h/r} \left( z_{h}^{k} - \hat{h}_{i} \right) + W_{h/r} \hat{z}_{h} + \xi_{i}^{k}$$

$$= W_{h/r} y_{r}^{k} + \xi_{i}^{k} \quad (62)$$

Since $E(\xi_{i}^{k}) = 0$, we have $E(y_{h}^{k+1}) = W_{h/r} E(y_{r}^{k})$. 

\[\]
Finally, to obtain the least square solution of $W_{H^T}$ from
the observations, we ignore the noise term in (62). Note that
a single group $y^{k+1}_i = W_{H^T}y_k$ is based on two consecutive
observations over $\mathcal{V}_p$, and contains $|\mathcal{V}_h|$ groups of equations
about $W_{H^T}$, which consist of $|\mathcal{V}_h|/|\mathcal{V}_p|$ parameters. For $i \in
\mathcal{V}_h$, the transpose of $y^{k+1}_i = W_{H^T}y_k$ is given by
\[
y^{k+1}_i = (\overline{y}^T_i)(W_{[i,:]}^T)^T. \tag{63}
\]
Stack the states of continuous moments into one and it yields
\[
\begin{pmatrix}
y^T_1
\vdots
y^T_f
\vdots
y^T_l
\end{pmatrix}
= \begin{pmatrix}
(y^T_1)
\vdots
(y^T_f)
\vdots
(y^T_l)
\end{pmatrix}
(W_{H^T})^T. \tag{64}
\]
Then, one easily infers the least square solution of the vector
$(W_{H^T})^T$. Integrating all robots in $\mathcal{V}_h$, it follows that
\[
Y^T_{H^T} = \begin{pmatrix}
(y^T_1)
\vdots
(y^T_f)
\vdots
(y^T_l)
\end{pmatrix}
= W_{H^T}^T Y_{H^T}. \tag{65}
\]
To avoid a under-determined solution of $W_{H^T}$, at least
$(|\mathcal{V}_h| + 1$) consecutive observations over $\mathcal{V}_p$ are needed to solve
(65).

The final estimation is given by $W_{H^T} = \left((Y^T_{H^T})^{-1}Y_{H^T}Y^T_{H^T}\right)$. The proof is completed.

\section{Proof of Lemma 1}

\section{Proof. Due to $r_a \notin \mathcal{V}_p$, when $\|z_a - z_i\|_2 < R_a$, $r_a$ is
regarded as an external obstacle by $r_i$. Note that in cases where
$\|z_a - z_i\|_2 < R_a$, the influence of $(z_a - z_i)$ is neglected since
$r_i$ aims to move as far as $r_a$ as it could. By Definition 1,
given the goal state $z^{\ast}_a$, the proof turns to find a groups of
inputs $u_a = \{u^k, k = 1, \ldots, k_H\}$ to satisfy
\[
z^{\ast}_a - z^0 = \sum_{k=1}^{k_H} g(z^k(u^k_a) - z^0, z^k_a - z^0, v_i, k_H). \tag{66}
\]
With $g$ known and $(z_i - z_i), (z_a - z_i)$ and $v_i$ measurable, an
available choice of $u_a$ and $k_H$ can always be found such that
\[
|g(z^k(u^k_a) - z^0, z^k_a - z^0, v_i, k_H)| = \frac{\|z^k_a - z^0\|_2}{k_H} \leq b, \tag{67}
\]
where $R_a \leq \|z^k_a - z^0\|_2 < R_a$. The proof is completed.

\section{Proof of Theorem 1}

\section{Proof. We prove this theorem by contradiction.

For $i$), suppose there are two distinct convex polygons $\mathcal{V}^p_i$ and
$\mathcal{V}^p_{i,b}$ and the cardinal number $|\mathcal{V}^p_{i,a}| \geq |\mathcal{V}^p_{i,b}|$, then we
obtain
\[
\mathcal{V}^p_i = \mathcal{V}^p_{i,a} \cap \mathcal{V}^p_{i,b} \neq \emptyset. \tag{68}
\]
Then, $\forall i' \in \mathcal{V}^p_{i,a}$, $i'$ is not covered by $\mathcal{V}^p_{i,b}$ which renders a
contradiction by Definition 2. Therefore, $\mathcal{V}^p_i$ is unique.

For ii), the conclusion obviously holds when $|\mathcal{V}^p_i| = 2$, thus we
consider nontrivial cases where $|\mathcal{V}^p_i| \geq 3$. First, when
$|\mathcal{V}^p_i| = 3$, there are only two vertex adjacent to $i$, here denoted
as $j_1$ and $j_2$, and let $d_{i,j_k} = \|z_{j_k} - z_i\|_2, k = 1, 2$. In this case,
$P(z_{j_1}, d_{i,j_1}) \cap P(z_{j_2}, d_{i,j_2}) = \emptyset$ if and only if the states $z_{j_1}, z_{j_2}$ and $z_{j_3}$ are linear dependent, which contradicts with convex
vertex condition of $i$. Therefore, it follows that
\[
P_i(d_{i,j_1}, d_{i,j_2}) = P(z_{j_1}, d_{i,j_1}) \cap P(z_{j_2}, d_{i,j_2}) \neq \emptyset. \tag{69}
\]
When $|\mathcal{V}^p_i| > 3$, $\forall j_3 \in \{\mathcal{V}^p_i \setminus \{i \cup j_1 \cup j_2\}\}$, utilizing (69),
we easily obtain
\[
P_i(d_{i,j_1}, d_{i,j_3}) \neq \emptyset. \tag{70}
\]
Then, what we need to do is to prove
\[
P_i(d_{i,j_1}, d_{i,j_3}) \cap P_i(d_{i,j_1}, d_{i,j_3}) \neq \emptyset. \tag{71}
\]
Similarly, suppose $P_i(d_{i,j_1}, d_{i,j_3}) \cap P_i(d_{i,j_1}, d_{i,j_3}) \neq \emptyset$. This case is
equivalent to the states of four vertex satisfying
\[
z_{j_3} - z_i = \alpha_1(z_{j_1} - z_i) + \alpha_2(z_{j_2} - z_i), \tag{72}
\]
where $\alpha_1 \leq 0$ and $\alpha_2 \leq 0$. Note that $\alpha_1 = 0$ (or $\alpha_2 = 0$)
denotes $j_1$ (or $j_2$), $j_3$ and $i$ are on the same line, and $\alpha_1, \alpha_2$ are
not zero at the time. Consequently, we have
\[
z_i = z_{j_3} - \alpha_1 z_{j_1} - \alpha_2 z_{j_2}, \tag{73}
\]
which means $z_i$ is a convex combination of $z_{j_k}$ ($k = 1, 2, 3$) and thus
contradicts with convex vertex condition of $i$. Therefore, it follows that if $P_i(d_{i,j_1}, d_{i,j_3}) \neq \emptyset$ and $P_i(d_{i,j_1}, d_{i,j_3}) \neq \emptyset,$
then $P_i(d_{i,j_2}, d_{i,j_3}) \neq \emptyset$. By this transitivity property, we have
\[
\mathcal{Z}^{t_0} = \bigcap_{j \in \mathcal{V}^p_i} P(z, d_{j,i}) \neq \emptyset. \tag{74}
\]
If there exists $j \in \{\mathcal{V}^p_i \setminus \{i\}\}$, it is also covered by $\mathcal{V}^p_i$.
Likewise, by the convex properties, $P(z, d_{j,i}) \cap \mathcal{Z}^{t_0} = \emptyset$.
To sum up, define the feasible position set as
\[
\mathcal{Z}^{t_1} = \bigcap_{j \in \mathcal{V}^p_i} P(z, d_{j,i}), \tag{75}
\]
and by the definition of $P(z, R_i)$, it yields that $\forall z \in \mathcal{Z}^{t_1}, \|z - z_j\|_2 < \|z_i - z_j\|_2$. The proof is completed.

\section{Proof of Lemma 2}

\section{Proof. For simplicity of expression, we directly consider the
excitation is injected at the steady stage.

Based on Theorem 1 at steady stage, the error $(z(t) - ct - s)$ is
extremely minor and negligible. Then, the global steady
state evolution is represented as
\[
z_{ss}(t) = q(t)u_t + q(t)u_t + \sum_{i=0}^{N} \frac{1}{\lambda_i} q(t)u_t. \tag{76}
\]
Note that the desired state deviation vector $h$ contained in $u$
only incurs a constant offset in $z_{ss}$. Therefore, ignore $h$ and
let $u = \{0, \ldots, 0, u_0, 0, \ldots, 0, u_c\}$, and we obtain
\[
z_{ss} = (p^e_iu + p^e_iu_c, u_c) \tag{77}
\]
When $u_c > 0$, it means that the excitation of $r_a$ aims to
strengthen the movement in the direction of the original leader.
In this case, arbitrary $u_c$ satisfying $u_c > 0$ is available to
meet the indirect controllability.
When \( u_c u_c < 0 \), it means that the excitation of \( r_n \) aims to strengthen the movement in the direction of \( u_c \). Thus, one infers from (77) that, to counteract the influence of the original leadership \( u_c \) and ensure \( \hat{z}_i u_c > 0 \), the following condition must hold, given by

\[
|p_{i_j}^c u_c| > |p_{i_N}^c u_c|.
\]  

(78)

The proof is completed. \( \square \)

\section*{F. Proof of Theorem 4}

\textbf{Proof.} The core of this proof is to analyze the influence of the in-neighbors of \( r_i \). First, we begin with a simple situation where \( \forall j' \in \{N_i^{in} \backslash j\} \), \( a_{ij'} = 0 \), i.e., other in-neighbors of \( r_i \) do not interact with \( r_j \). Recalling the dynamics of \( r_i \) given by (5), when \( r_j \) is under the excitation of \( u_c \), we have

\[
\dot{z}_i = a_i j \bigl( z_j - z_i - h_j + h_i \bigr) + \sum_{j' \in \{N_i^{in} \backslash j\}} a_{ij'} \bigl( z_{j'} - z_j - h_{j'} + h_i \bigr) \\
= a_{ij} \bigl( u_c t + z_0^j - z_i - h_j + h_i \bigr) \\
+ \sum_{j' \in \{N_i^{in} \backslash j\}} a_{ij'} \bigl( u_c t + z_0^j - z_i - h_{j'} + h_i \bigr).
\]  

(79)

Let \( b_{ij} = a_{ij} (z_0^j - h_{j'} + h_i) \), \( \tilde{b}_{ij} = \sum_{j' \in \{N_i^{in} \backslash j\}} a_{ij'} (z_0^j - h_{j'} + h_i) \), and \( \bar{a}_{ij} = \sum_{j' \in \{N_i^{in} \backslash j\}} a_{ij'} \). Then, (79) is rewritten as

\[
\dot{z}_i = a_{ij} u_c t - a_{ij} z_i + \bar{b}_{ij} + a_{ij} u_c t - a_{ij} z_i + \bar{b}_{ij} \\
= (a_{ij} u_c + \bar{a}_{ij} u_c) t - (a_{ij} + \bar{a}_{ij}) z_i + (h_j + \bar{b}_{ij}) \\
= b_1 t - b_2 z_i + b_3.
\]  

(80)

Note that (80) is a first-order constant coefficient non-homogeneous linear equation, and leveraging constant variation method, the solution is given as

\[
z_i(t) = \frac{b_1}{b_2} t + \left( \frac{b_1}{b_2} - \frac{b_3}{b_2} \right) (e^{-b_2 t} - 1).
\]  

(81)

Then, we obtain

\[
\dot{z}_i(t) = \frac{b_1}{b_2} = \frac{a_{ij} u_c + \bar{a}_{ij} u_c}{a_{ij} + \bar{a}_{ij}}.
\]  

(82)

The next step is the same as the proof of Lemma 2. It follows that whether \( r_i \) is indirectly controllable is determined by \( (z_0^* - z_0^i) u_c \) and \( a_{ij} u_c + \bar{a}_{ij} u_c \). Accordingly, one infers that \( r_i \) is indirect controllable if and only if (38) is satisfied.

Finally, consider \( \exists j' \in \{N_i^{in} \backslash j\}, a_{ij'} > 0 \), i.e., other in-neighbors of \( r_i \) are also influenced by \( r_j \). Then, (79) is rewritten as

\[
\dot{z}_i = a_{ij} \bigl( z_j - z_i - h_j + h_i \bigr) + \sum_{j' \in \{N_i^{in} \backslash j\}} a_{ij'} \bigl( z_{j'} - z_j - h_{j'} + h_i \bigr),
\]  

(83)

where \( z_{j'}(z_j) \) is also determined by \( z_j \) and no longer linearly increasing. However, \( a_{ij'} > 0 \) yields \( |z_{j'}(t) - z_j(t)| < |u_c t + z_0^j - z_j(t)| \), which incurs \( z_i(t) \) more close to \( z_0^* \) compared with that when \( a_{ij'} = 0 \) at the same time. Therefore, by (38), it is sufficient to guarantee the indirect controllability of \( r_i \). The proof is completed. \( \square \)

\begin{itemize}
  \item \textbf{Yushan Li} (S’19) received the B.E. degree in School of Artificial Intelligence and Automation from Huazhong University of Science and Technology, Wuhan, China, in 2018. He is currently working toward the Ph.D. degree with the Dept. of Automation, Shanghai Jiaotong University, Shanghai, China. He is a member of Intelligent of Wireless Networking and Cooperative Control group. His research interests include robotics, security of cyber-physical system, and distributed computation and optimization in multi-agent networks.
  
  \item \textbf{Jianping He} (SM’19) is currently an associate professor in the Department of Automation at Shanghai Jiao Tong University. He received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2013, and had been a research fellow in the Department of Electrical and Computer Engineering at University of Victoria, Canada, from Dec. 2013 to Mar. 2017. His research interests mainly include the distributed learning, control and optimization, security and privacy in network systems.
  
  \item \textbf{Xunda Ding} (S’20) received the B.E. and M.E. degree in School of Automation from North China Electric Power University, China, in 2016 and 2019, respectively. He is currently working toward the Ph.D. degree with the Dept. of Automation, Shanghai Jiaotong University, Shanghai, China. He is a member of Intelligent of Wireless Networking and Cooperative Control group. His research interests include robotics, learning theory and its application in practical systems.
  
  \item \textbf{Cai Lin} (F’20) received the M.A.Sc. and Ph.D. degrees (awarded Outstanding Achievement in Graduate Studies) in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2002 and 2005, respectively. Since 2005, she has been with the Department of Electrical and Computer Engineering at the University of Victoria, where she is currently a Professor. She is an NSERC E.W.R. Steacie Memorial Fellow. Her research interests span several areas in communications and networking, with a focus on network protocol and architecture design supporting emerging multimedia traffic and the Internet of Things.
  
  \item She was a recipient of the NSERC Discovery Accelerator Supplement (DAS) Grants in 2010 and 2015, respectively, and the best paper awards of IEEE ICC 2008 and IEEE WCNC 2011. She has co-founded and chaired the IEEE Victoria Section Vehicular Technology and Communications Joint Societies Chapter. She has been elected to serve the IEEE Vehicular Technology Society Board of Governors, 2019 - 2021. She has served as an Area Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, a member of the Steering Committee of the IEEE TRANSACTIONS ON BIG DATA (TBD) and IEEE TRANSACTIONS ON CLOUD COMPUTING (TCC), an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON COMMUNICATIONS, EURASIP Journal on Wireless Communications and Networking, International Journal of Sensor Networks, and Journal of Communications and Networks (JCN), and as the Distinguished Lecturer of the IEEE VTS Society. She has served as a TPC co-chair for IEEE VTC2020-Fall, and a TPC symposium co-chair for IEEE Globecom’10 and Globecom’13. She is a Registered Professional Engineer in British Columbia, Canada.
  
  \item \textbf{Xinping Guan} (F’18) received the B.S. degree in Mathematics from Harbin Normal University, Harbin, China, in 1986, and the Ph.D. degree in Control Science and Engineering from Harbin Institute of Technology, Harbin, China, in 1999. He is currently a Chair Professor with Shanghai Jiao Tong University, Shanghai, China, where he is the Dean of School of Electronic, Information and Electrical Engineering, and the Director of the Key Laboratory of Systems Control and Information Processing, Ministry of Education of China. Before that, he was the Professor and Dean of Electrical Engineering, Yanshan University, Qinhuangdao, China.
\end{itemize}
Dr. Guan’s current research interests include industrial cyber-physical systems, wireless networking and applications in smart factory, and underwater networks. He has authored and/or coauthored 5 research monographs, more than 270 papers in IEEE Transactions and other peer-reviewed journals, and numerous conference papers. As a Principal Investigator, he has finished/been working on many national key projects. He is the leader of the prestigious Innovative Research Team of the National Natural Science Foundation of China (NSFC). Dr. Guan received the First Prize of Natural Science Award from the Ministry of Education of China in both 2006 and 2016, and the Second Prize of the National Natural Science Award of China in both 2008 and 2018. He was a recipient of IEEE Transactions on Fuzzy Systems Outstanding Paper Award in 2008. He is a National Outstanding Youth honored by NSF of China, Changjiang Scholar by the Ministry of Education of China and State-level Scholar of New Century Bai Qianwan Talent Program of China.