Koopman Operation-Based Leader-Following Formation Control for Nonholonomic Mobile Robots Under Denial-of-Service Attacks

Zhan, Weiwei; Miao, Zhiqiang; Chen, Yanjie; Feng, Yun; Wang, Yaonan

Publication date:
2023

Citation for published version (APA):
Zhan, W., Miao, Z., Chen, Y., Feng, Y., & Wang, Y. (2023). *Koopman Operation-Based Leader-Following Formation Control for Nonholonomic Mobile Robots Under Denial-of-Service Attacks*. Paper presented at 2023 IEEE International Conference on Unmanned Systems (ICUS)
, Hefei, China.

Koopman Operation-Based Leader-Following Formation Control for Nonholonomic Mobile Robots under Denial-of-Service Attacks

Weiwei Zhan
College of Electrical and Information Engineering
Hunan University
Changsha, China
zhanweiwei@hnu.edu.cn

Zhiqiang Miao*
College of Electrical and Information Engineering
Hunan University
Changsha, China
miaozhiqiang@hnu.edu.cn

Yanjie Chen
School of Mechanical Engineering and Automation Fuzhou University
Fuzhou, China
chenyanjie@fzu.edu.cn

Yun Feng
College of Electrical and Information Engineering Hunan University
Changsha, China
fyrobot@hnu.edu.cn

Yaonan Wang
College of Electrical and Information Engineering Hunan University
Changsha, China
yaonan@hnu.edu.cn

2023 IEEE International Conference on Unmanned Systems (ICUS) | 979-8-3503-1630-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICUS58632.2023.10318241

***Abstract*—Under denial-of-service (DoS) attacks, achieving a desired formation of networked nonholonomic mobile robots (NMRs) over communication is a nontrivial challenge due to communication disconnecting and recovering at any time. Efforts have been made in prevention, detection, and resilience methods, but existing methods' generalization ability and interpretability still need improvement. This paper proposes the leader-following formation control framework for a group of NMRs under denial-of-service (DoS) attacks. The Koopman operator is utilized to express a linear lifted feature space for the discrete motion of networked NMRs. Based on an event-triggered mechanism, a data-driven loss function is presented to approximate the Koopman operator, enabling a long-term recovery capability under DoS attacks. Furthermore, according to the recovered motion of the leader, the leader-following formation controller with a variable gain is designed to ensure that the formation error converges to the neighborhoods of zero. In numerical simulation, the effectiveness of the proposed method is verified by a DoS attack example.**

***Keywords*—leader-following formation control, networked nonholonomic mobile robots, koopman operator, denial-of-service attacks**

I. Introduction

Recently, networked nonholonomic mobile robots (NMRs) are developed to work in a favorable communication environment, saving labor costs, reducing operation load, and replacing dangerous operations [1]. Hence, networked NMRs are utilized in many applications including search and rescue [2], cooperative object movement [3], and intelligent transportation. However, most existing works rely on secure and stable communication networks to share collaborative information [4], the openness and fragility nature of communication among networked NMRs makes them vulnerable to potential malicious attacks. In particular, attacks relying on transmitted signals have characteristics of being quick in diffusion and being strong stealthiness at the kinematics level of leaders and followers. Under the unreliable communication networks, the design of traditional controllers without considering the potential malicious attacks can cause system performance degradation or even instability [5]. Therefore, it is urgent to address the key technologies of networked NMRs in unreliable communication networks.

The implementation behaviors of malicious attacks on the communication channels are typically divided into DoS attacks and deception attacks [6]. Denial-of-service (DoS) that do not rely on transmission signals can make it easy to implement networked NMRs [7]. Once the robots suffer from malicious attacks, all agents are unable to communicate with their topology-connected NMRs. More seriously, even the collision accident occurs among the NMRs, causing irreversible destruction [8], [9].

The development of effective controller strategies that can handle DoS attacks is a technical challenge in the study of formation control for MASs. The proper feedback gain matrix and event-triggered parameters of consensus based on an observer model were established to ensure the mean-square consensus [10]. [11] focused on the security control architecture for resilient complex networks, choosing the coupling strength and the feedback gain matrix to achieve synchronization. Taking into account the security problems of leaderless and

*Corresponding author: Zhiqiang Miao.

This work was supported in part by the National Key Research and Development Program of China (No. 2022YFB3903804), the National Natural Science Foundation of China under Grants 62273138, 62203161, and 62273098, the Hunan Provincial Natural Science Foundation of China under Grant 2021JJ20029, the Science and Technology Innovation Program of Hunan Province under Grant 2021RC3060, the Newton International Fellowships 2022 funded by the Royal Society, UK (No.NIF\R1\221089), and also in part by the Youth Talent Support Project of the Chinese Association for Science and Technology.

leader-following under DoS attacks, [12] developed a resilient cooperative event-triggered control scheme for linear MASs to determine the scheduling of controller updates during a DoS attack activity. A fast finite time backstepping control scheme was designed to solve the consensus issue with fast convergence performance when the followers are far from the equilibrium point under DoS attacks [13]. To ensure asymptotic consensus resistance to distributed DoS attacks, a fully distributed control framework was designed to equip with strong robustness and high scalability [14]. Though two triggered functions on the measurement channel and control channel, a self-triggered secure control scheme was further developed to avoid constantly monitoring measurement errors, reducing the burden on the communication [15]. Under the premise that the sampling process is not uniform and the continuous attack duration has upper bounds, the control approach was proposed to ensure the solvability of the output consensus issue [16].

Despite the existence of several studies on the formation control of MASs under DoS attacks, there is a lack of generalization ability and interpretability. The security state estimator of these methods is designed to ensure the effectiveness of formation, which is not easy to transplant. Meanwhile, the formation convergence rate and corresponding compact set in the DoS attack-shut are not considered together. Based on data-driven, the core idea of our approach is to use a multi-step backtracking loss function, enabling a long-term recovery capability in the duration of DoS attack-active. Specifically, a resilience formation control with a variable gain is proposed for a group of NMRs over unreliable communication networks. In summary, the main contributions and features of our proposed approach are as follows:

- A Koopman operation-based recovery is presented for describing the motion of topology-connected NMRs. Different from other estimation methods, the resulting recovery is a linear time-invariant model in the lifted space, with a nonlinear mapping from the original state space. Combined with an event-triggered mechanism, the data-driven loss function is presented to compute the Koopman operator, enabling a long-term recovery capability under DoS attacks.
- An event-triggering mechanism with a dynamic threshold is designed to indicate the triggering rule in different link nodes. Compared with the constant thresholds, the proposed event-triggering mechanism can avoid false indications to reduce the communication burden.
- Considering that the available signals are not completely transmitted in the presence of DoS attacks. A novel distributed formation controller with a variable gain is designed to ensure the formation error of networked NMRs converging to the minor neighborhoods of zero.

The rest of this paper is scheduled as follows: the preliminary including control objective, problem formulation, and NMR dynamics is described in Section 2. The proposed leader-following formation controller is employed for the leader-following example in Section 3. Conclusions are stated in Section 4.

II. PRELIMINARY

The DoS attacks with intermittent direct interrupt the transmission information, causing the leader-following to disconnect or connect. To distinguish DoS attack-active and DoS attack-shut, special timelines are marked as follows. $t_k^{on} \in \mathbb{R}_{>0}$ represents the DoS attack-active instant when the communication information is rejected, and $t_k^{off} \in \mathbb{R}_{>0}$ represents the DoS attack-shut instant when the communication information is unimpeded. The duration of DoS attack-active and attack-shut represent as $\Delta_k^{off} \triangleq t_k^{off} - t_k^{on} \in \mathbb{R}_{>0}$ and $\Delta_k^{on} \triangleq t_k^{on} - t_k^{off} \in \mathbb{R}_{>0}$, respectively.

A. Nonholonomic Mobile Robot Dynamics

The dynamics model of the ith NMR is modeled by a continuous-time nonlinear system:

$$\begin{aligned} \dot{p}_i(t_k) &= \begin{bmatrix} \cos\psi_i(t_k) & 0 \\ \sin\psi_i(t_k) & 0 \\ 0 & 1 \end{bmatrix} q_i(t_k) \\ \dot{q}_i(t_k) &= M_{ic}\tau_i(t_k) + C_{ic}\omega_i(t_k)q_i(t_k) + G_{ic}q_i(t_k) \end{aligned} \tag{1}$$

where $p_i = [x_i, y_i, \psi_i]^\top$ with $[x_i, y_i]^\top$ and ψ_i respectively denoting the position and orientation in inertia frame, $q_i = [v_i, \omega_i]^\top$ with v_i and ω_i respectively expressing the linear and angular velocity of ith NMR, τ_i represents the control input, $M_{ic} = \left(M_i D_i^{-1}\right)^{-1}$, $C_{ic} = \left(M_i D_i^{-1}\right)^{-1} C_i D_i^{-1}$, and $G_{ic} = \left(M_i D_i^{-1}\right)^{-1} G_i D_i^{-1}$.

More details, M_i, and C_i are respectively defined by $M_i = [m_{1i}, m_{2i}; m_{2i}, m_{1i}]$ with $m_{1i} = 0.25 b_i^{-2} r_i^2 (m_i b_i + I_i) + I_{y,i}$ and $m_{2i} = 0.25 b_i^{-2} r_i^2 (m_i b_i^2 - I_i)$, $C_i = [g_{1i}, h_i\omega_i; -h_i\omega_i, g_{2i}]$ with $h_i = 0.5 b_i^{-1} r_i^2 m_{bi} d_i$, $g_{1i} > 0$, and $g_{2i} > 0$. Furthermore, the m_i and I_i are respectively explained in detail as follows: $m_i = 2m_{wi} + m_{bi}$ and $I_i = m_{bi} d_i^2 + 2m_{wi} b_i^2 + I_{xi} + 2I_{yi}$, where m_{wi} and m_{bi} are respectively the masses of the body and wheel, $P_i = \mathrm{diag}\{I_{xi}, I_{yi}, I_{zi}\}$ is the inertia tensor of the body, and d_i and b_i are respectively half of the length and width of the body.

In addition, $q_i = [v_i, \omega_i]^\top$ and the angular velocities of the left and right wheels $\nu_i = [\nu_{1i}, \nu_{2i}]^\top$ satisfy

$$q_i = \begin{bmatrix} v_i \\ \omega_i \end{bmatrix} = \frac{r_i}{2} \begin{bmatrix} 1 & 1 \\ b_i^{-1} & -b_i^{-1} \end{bmatrix} \nu_i \triangleq D_i \nu_i, \tag{2}$$

where r_i is the wheel radius of the ith robot, and D_i is the non-singular matrix.

B. Problem Formulation

Without DoS attacks, the received signals of leader-following NMR can be modeled by the following model with the unknown time-varying matrix A_j, B_j, E_j, and F_j:

$$\begin{cases} p_j(t_{k+1}) = A_j p_j(t_k) + B_j q_j(t_k) \\ q_j(t_{k+1}) = E_j q_j(t_k) + F_j \tau_j(t_k) \end{cases}, j \in \mathcal{N}_i \tag{3}$$

where $p_j \in \mathbb{R}^3$, $q_j \in \mathbb{R}^2$, and $\tau_j \in \mathbb{R}^2$ are the received signals.

If the attacker launches a random subset of DoS attacks to the edge (i,j), it occurs that the missed data packet $\{p_j(t_{k+d_j}), q_j(t_{k+d_j}), \tau_j(t_{k+d_j})\}$ are not able to reach their destination (ith NMR) successfully. Resulting in alterations to (3), which can be represented as follows:

$$\begin{cases} p_j(t^{on}_{k+1+d_j}) = A_j p_j(t^{on}_{k+d_j}) + B_j q_j(t^{on}_{k+d_j}) \\ q_j(t^{on}_{k+1+d_j}) = E_j q_j(t^{on}_{k+d_j}) + F_j \tau_j(t^{on}_{k+d_j}) \end{cases}, \tag{4}$$

where $d_j \in \{1, .., \Delta^{on}_{max}\}$ is the attack intensity for the edge (i,j) with $\Delta^{on}_{max} = \max\{\Delta^{on}_k\}$ representing the maxima attack-active duration.

More details, the DoS attack average intensity is defined as $\text{avg}\{d_j(k)\} = \Xi_d(t_0, t^{off}_k)/\Xi_f(t^{on}_1, t^{off}_k)$. To describe the DoS attack model [17], the DoS attack duration $\Xi_d(t_0, t^{off}_k)$ and DoS attack amount $\Xi_f(t^{on}_1, t^{off}_k)$ are respectively assumed as follows:

Assumption 1: Defining the DoS attack amount over the time interval $[t_0, t]$ as $\Xi_f(t_0, t)$, there exist constant $\Xi_1 \in \mathbb{R}_{\geq 0}$ and $l_1 \in \mathbb{R}_{\geq 1}$ such that

$$\Xi_f(t_0, t) \leq \Xi_1 + \frac{t - t_0}{l_1}, \tag{5}$$

where t_0 is the initial time.

Assumption 2: Defining the DoS attack duration over the time interval $[t_0, t]$ as $\Xi_d(t_0, t)$, there exist constant $\Xi_2 \in \mathbb{R}_{\geq 0}$ and $l_2 \in \mathbb{R}_{\geq 1}$ such that

$$\Xi_d(t_0, t) \leq \Xi_2 + \frac{t - t_0}{l_2}, \tag{6}$$

C. Control Objective

Under Assumptions 1-2, networked NMRs suffer from an adversary arbitrarily jamming certain communication channels. The received data are not able to be updated when the DoS attacks launch. Then, utilizing the available historical information, this paper aims to achieve the following control objectives:

1) Design a distributed cascade recovery $\hat{p}_j(t_{k+d_j})$ for ith NMR followers utilizing its leader's historical signals $p^*_j(t^{on}_k) = [p_j(t^{off}_k), ..., p_j(t^{on}_k)]^\top$ and $q^*_j(t^{on}_k) = [q_j(t^{off}_k), ..., q_j(t^{on}_k)]^\top$ to approximate the model (3), recovering the missed signals $p_j(t^{on}_{k+d_j})$ at the DoS attacks active instants.

2) Design the leader-following formation control command τ_i based on the distributed recovery such that desired formation configuration $p^{jc}_i \in \mathbb{R}^3$ can be achieved in networked NMRs under DoS attacks.

III. CONTROLLER DESIGN

A. Koopman Operator-based Recovery

Define $\bar{\mathcal{F}} \subset \mathcal{F}$ as the subspace of $\mathcal{F}$ spanned by $L > 3$ linearly independent basis functions $\{\phi_l : \mathbb{R}^2 \to \mathbb{R}\}^L_{l=1}$. Any observable $p_j \in \mathcal{F}$ and $q_j \in \mathcal{F}$ can be described as a linear combination of these basis functions

$$p_j(t_k) = w^\top_{p,j} \Phi_{p,j}(t_k) \tag{7}$$

$$q_j(t_k) = w^\top_{q,j} \Phi_{p,j}(t_k) \tag{8}$$

where $\Phi_{p,j}(t_k) = [\phi_1(p_j(t_k))^\top \cdots \phi_L(p_j(t_k))^\top]^\top$ and $\Phi_{p,j}(t_k) = [\phi_1(q_j(k))^\top \cdots \phi_L(q_j(t_k))^\top]^\top$ are adopted as a group of observable for practical calculation, $w^\top_{p,j} \in \mathbb{R}^L$, and $w^\top_{q,j} \in \mathbb{R}^L$.

According to the discrete state measurement model (3), the Luenberger observer can be designed as

$$\begin{cases} \hat{p}_j(t_{k+1}) = A_j \hat{p}_j(t_k) + B_j q_j(t_k) + U_{p,j}(\hat{\bar{p}}_j(t_k) - \bar{p}_j(t_k)) \\ \hat{\bar{p}}_j(t_k) = (1 - \xi_{p,j})\hat{p}_j(t_k) + \xi_{p,j} \hat{w}^{\mathrm{T}}_{p,d} \Phi(p_j(t_k)) \end{cases} \tag{9}$$

$$\begin{cases} \hat{q}_j(t_{k+1}) = E_j \hat{q}_j(t_k) + F_j \tau_j(t_k) + U_{q,j}(\hat{\bar{q}}_j(t_k) - \bar{q}_j(t_k)) \\ \hat{\bar{q}}_j(t_k) = (1 - \xi_{q,j})\hat{q}_j(t_k) + \xi_{q,j} \hat{w}^{\mathrm{T}}_{q,d} \Phi(q_j(t_k)) \end{cases} \tag{10}$$

where $\hat{w}_{q,j}(t_{k+1})^\top = \hat{w}_{q,j}(t_k)^\top + U_{q,j}\xi_{q,j}\tilde{q}_j(t_k)^\top \Phi(q_j(t_k))$ with $0 < \xi_{q,j} < 1$ and $U_{q,j} < E_j/(\xi_{q,j} - 1)$, and $\hat{w}_{p,j}(t_{k+1})^\top = \hat{w}_{p,j}(t_k)^\top + U_{p,j}\xi_{p,j}\tilde{p}_j(t_k)^\top \Phi(p_j(t_k))$ with $0 < \xi_{p,j} < 1$ and $U_{p,j} < A_j/(\xi_{p,j} - 1)$.

In this paper, the Koopman operator is utilized to recover the missed signal of the leader by capturing its inherent features through linear motion evolution. Based on [18], the Koopman operator generalization of model (3) relies on two extend state variables $z_j = [p^\top_j, q^\top_j]^\top$ and $r_j = [q^\top_j, \tau^\top_j]^\top$. The Koompan operator on (4) with the extended states z_j and r_j is respectively described as

$$\mathcal{K}\Phi(z_j, r_j, t^{on}_{k+d_j}) = \Phi(z_j, r_j, t^{on}_{k+1+d_j}) \tag{11}$$

where $\mathcal{K}$ represents the Koopman operator, and $\Phi(\cdot)$ is the observation functions in the lifted space.

At time t_k, the augmented state measurement matrix $\Omega(r_j(t_k)) = [\phi(q_j(t_k))^\top, \tau_j(t_k)^\top]^\top$ and $\Omega(z_j(t_k)) = [\phi(p_j(t_k))^\top, q_j(t_k)^\top]^\top$ are adopted as a set of observable in the actual calculation, where L is the number of observable function on $q_j(t_k)$ and $p_j(t_k)$. Furthermore, we can write the approximation model resulting from the Koopman operator as follows:

$$\begin{cases} \Phi_{q,j}(q_j(t_{k+1})) = \mathcal{K}_{q,j}\Omega_{q,j}(q_j(t_k), \tau_j(t_k)) \\ \Phi_{p,j}(p_j(t_{k+1})) = \mathcal{K}_{p,j}\Omega_{p,j}(p_j(t_k), \hat{q}_j(t_k)) \end{cases} \tag{12}$$

where $\mathcal{K}_{p,j} = [\breve{A}_j \quad \breve{B}_j] \in \mathbb{R}^{L\times N}$, $\mathcal{K}_{q,j} = [\breve{E}_j \quad \breve{F}_j] \in \mathbb{R}^{L\times N}$ with $N = L + 2$, $\Omega(q_j(t_k), \tau_j(t_k)) = [\Phi_{q,j}(q_j(t_k)^\top, \tau_j(t_k)^\top]^\top \in \mathbb{R}^N$, and $\Omega(p_j(t_k), \hat{q}_j(t_k)) = [\Phi_{p,j}(p_j(t_k)^\top, \hat{q}_j(t_k)^\top]^\top \in \mathbb{R}^N$.

It's worth noting that only the historical data at $t \in [t^{off}_k, t^{on}_k]$ is valuable. When the DoS attacks are active, the approximating operation is terminated. To introduce the available historical data constructing the loss function with multi-step, we firstly give the backtracking state in s time steps

$$\hat{p}_j(t_k) = \Psi_j(\mathcal{K}^{[s]}_{p,j}\Phi_{p,j}(t_{k-s}), w_{p,j}) + \epsilon_{j,s} \tag{13}$$

where $\epsilon_{j,s} \in \mathbb{R}^3$ is estimation error at the sth step with $s < k$, and $\mathcal{K}_{p,j}^{[s]}\Phi_{p,j}(t_{k-s})$ is the sth step ahead state from $p_j(t_{k-s})$, i.e.,

$$\begin{aligned}\mathcal{K}_{p,j}^{[s]}\Phi(t_{k-s}) &= \Phi_{p,j}(t_k)\\ &= \breve{A}_j\Phi_{p,j}(t_{k-1}) + \breve{B}_j\hat{q}_j(t_{k-1})\\ &= \breve{A}_j^2\Phi_{p,j}(t_{k-2}) + \breve{A}_j\breve{B}_j\hat{q}_j(t_{k-2}) + \breve{B}_j^2\hat{q}_j(t_{k-1})\\ &\cdots\cdots\\ &= \breve{A}_j^s\Phi_{p,j}(t_{k-s}) + \Sigma_{h=1}^{s}\breve{A}_j^{h-1}\breve{B}_j\hat{q}_j(t_{k-s})\end{aligned} \tag{14}$$

In order to minimize the evolution error of leader's state in the observable space, the loss function along the past s time steps is considered as

$$\begin{aligned}\mathcal{L} &= \sum_{h=1}^{s}\epsilon_j^h\|\Theta_{p,j}(t_k) - K_{p,j}^{[h]}\Omega(p_j(t_{k-h}))\|_2^2\\ &\quad + \sum_{h=1}^{s}\epsilon_j^h\|\Theta_{q,j}(t_k) - K_{q,j}^{[h]}\Omega(q_j(t_{k-h}))\|_2^2\end{aligned} \tag{15}$$

where $0 \ll \epsilon_j < 1$ is the forgetting factor.

By introducing the above loss function, the resulting approximation model aims to solve the following optimization problems:

$$\min_{\breve{A}_j,\breve{B}_j,\breve{E}_j,\breve{F}_j} \mathcal{L} \tag{16}$$

The Adam [19] solver based on gradient descent is utilized to deal with nonlinear terms derived from multi-step loss function. Therefore, the best $\breve{A}_j$, $\breve{B}_j$, $\breve{E}_j$, and $\breve{F}_j$ matrices of (13) are respectively embedded in $\mathcal{K}_{p,j}$ and $\mathcal{K}_{q,j}$ and can be isolated by partitioning the following partitioning:

$$\begin{cases}\Phi_{q,j}(t_{k+1}) = \breve{E}_j\Phi_{q,j}(t_k) + \breve{F}_j\tau_j(t_k)\\ \qquad\hat{q}_j = \hat{w}_{q,j}^\top\Phi_{q,j}(t_k)\\ \Phi_{p,j}(t_{k+1}) = \breve{A}_j\Phi_{p,j}((t_k)) + \breve{B}_j\hat{q}_j(t_k)\\ \qquad\hat{p}_j = \hat{w}_{p,j}^\top\Phi_{p,j}((t_k))\end{cases} \tag{17}$$

B. Event-Triggered Mechanism

Denote $p_j(t_k^*)$ as signals reaching their destination successfully. Then, the event triggering function for the edge (i,j) is designed as follows

$$\begin{aligned}t_{k+1}^{off} = \inf\{t > t_k^{off} \,|\, &\|\hat{p}_j(t) - p_j(t_k^*)\| \leq\\ &\mathrm{sgn}(\hat{p}_j(t) - p_j(t_k^*))\eta_p \cdot f_{ij}\}\end{aligned} \tag{18}$$

with $f_{ij} = \frac{\exp(\mathrm{sgn}(\hat{p}_j(t)-p_j(t_k^*))\mathcal{L})\overline{\vartheta}-\underline{\vartheta}}{\exp(\mathrm{sgn}(\hat{p}_j(t)-p_j(t_k^*))\mathcal{L})+1}$, where $\underline{\vartheta}$ and $\overline{\vartheta}$ are positive parameters, and η_p is taken as the following exponentially decaying function $\eta_p(t) = (\eta_{p0} - \eta_{p\infty})\exp(-\alpha t) + \eta_{p\infty}$ designed by positive parameters: $\eta_{p0} > \eta_{p\infty}$, and α.

The event triggering mechanism designed in (18) can be verified

$$\frac{\exp(-\mathcal{L})\overline{\vartheta} - \underline{\vartheta}}{\exp(-\mathcal{L}) + 1} \leq \hat{p}_j(t) - p_j(t_k^*) \leq \frac{\exp(\mathcal{L})\overline{\vartheta} - \underline{\vartheta}}{\exp(\mathcal{L}) + 1} \tag{19}$$

For the definition of f_{ij}, it is clear that $f_{ij} \in (-\underline{\vartheta}, \overline{\vartheta})$. If $p_j(t) = p_j(t_k^*)$, it yields

$$-\overline{\vartheta}\eta_p(t) \leq \tilde{p}_j(t) \leq \overline{\vartheta}\eta_p(t) \tag{20}$$

which means the DoS attacks are shut.

If $p_j(t) \neq p_j(t_k^*)$, we can obtain that

$$\begin{cases}\text{Case1}: & -\underline{\vartheta}\eta_p(t) \leq \tilde{p}_j(t) + (p_j(t) - p_j(t_k^*)) \leq \overline{\vartheta}\eta_p(t)\\ \text{Case2}: & \tilde{p}_j(t) + (p_j(t) - p_j(t_k^*)) \leq -\overline{\vartheta}\eta_p(t)\\ & \underline{\vartheta}\eta_p(t) \leq \tilde{p}_j(t) + (p_j(t) - p_j(t_k^*))\end{cases} \tag{21}$$

where Case2 means that the DoS attacks are active.

Moreover, Case2 of (21) indicates that once function $\|\hat{p}_j(t) - p_j(t_k^*)\|$ increases to the threshold $\min\{\underline{\vartheta}\eta_p(t), \overline{\vartheta}\eta_p(t)\}$, the event will be triggered. Then, it can be seen that the Zeno-behavior will excluded through setting the tolerance boundary upper threshold $\overline{\vartheta}$ and lower threshold $\underline{\vartheta}$. The triggering condition in (18) is a typical function with an exponentially decaying type structure. The designed event-triggered mechanism (18) will reduce the false detection for DoS attacks to avoid sacrificing the performance of the NMRs control.

C. Distributed Formation Control Law Design

Under the potential threat of DoS attacks, the signals from topology-connected NMR can not arrive at their destination. Based on the labeled timelines, a detection variable is utilized to describe the DoS attack shut/active as follows:

$$\nu_{ij}(t) = \begin{cases}1, & t \in [t_k^{on}, t_k^{off})\\ 0, & t \in [t_k^{off}, t_k^{on})\end{cases} \tag{22}$$

According to the definition of the indicator variable ν_{ij}, the locally received signals p_j of the edge (i,j) are modified as $(1-\nu_{ij})\hat{p}_j + \nu_{ij}p_j$. The relative position $p_i^{jc} = [x_i^{jc}, y_i^{jc}]^{\mathrm{T}}$ for ith NMR can be described as

$$p_i^{jc}(t) = p_i^j(t) + \iota_{ij}\begin{bmatrix}\cos\psi_{ij}(t)\\ \sin\psi_{ij}(t)\end{bmatrix} \tag{23}$$

where ι_{ij} is the offset of the auxiliary point, $\psi_{ij}(t) = \psi_i(t) - \nu_{ij}\psi_j(t) - (1-\nu_{ij})\hat{\psi}_j(t)$ is the orientation of jth NMR relative to ith NMR, and the position of jth NMR relative to ith NMR is written as

$$\begin{cases}p_i^j(t) = \begin{bmatrix}\cos\psi_j & \sin\psi_j\\ -\sin\psi_j & \cos\psi_j\end{bmatrix}(p_i - p_j), t \in [t_k^{off}, t_k^{on})\\ p_i^j(t) = \begin{bmatrix}\cos\hat{\psi}_j & \sin\hat{\psi}_j\\ -\sin\hat{\psi}_j & \cos\hat{\psi}_j\end{bmatrix}(p_i - \hat{p}_j), t \in (t_k^{on}, t_{k+1}^{off}]\end{cases}$$

Based on the definition of relative position p_i^{jc}, the local formation errors is defined as $e_i^p = p_i^{jc} - p_i^{jd}$ with p_i^{jd} representing the desired position. The following error dynamics can be derived:

$$\begin{aligned}\dot{e}_i^p = J_{ij}(\psi_{ij})\left(e_i^p + \begin{bmatrix}v_i^d\\ \omega_i^d\end{bmatrix}\right) - \begin{bmatrix}\nu_{ij}v_j + (1-\nu_{ij})\hat{v}_j\\ 0\end{bmatrix}\\ + (\nu_{ij}\omega_j + (1-\nu_{ij})\hat{\omega}_j)\begin{bmatrix}y_i^{jc}\\ x_i^{jc}\end{bmatrix}\end{aligned} \tag{24}$$

where e_i^p is the tracking error of velocity layer, and $J_{ij}(\psi_{ij})$ is given by

$$J_{ij}(\psi_{ij}) = \begin{bmatrix}\cos\psi_{ij} & -\iota_{ij}\sin\psi_{ij}\\ \sin\psi_{ij} & \iota_{ij}\cos\psi_{ij}\end{bmatrix}$$

To make the local formation error dynamics stable (24), the following desired velocities $[v_i^d, \omega_i^d]$ is designed as

$$\begin{bmatrix} v_i^d \\ \omega_i^d \end{bmatrix} = J_{ij}^{-1}(\psi_{ij})\mu_i \tag{25}$$

$$\mu_i = -\{\nu_{ij}\omega_j + (1-\nu_{ij})\hat{\omega}_j\}\begin{bmatrix} y_i^{jc} \\ x_i^{jc} \end{bmatrix} - \frac{K_{i1}e_i^p}{\|\|e_i^p\|^{\alpha_i} - \xi(e_i^p)(\overline{C}+\varepsilon)\|} + \begin{bmatrix} \nu_{ij}v_j + (1-\nu_{ij})\hat{v}_j \\ 0 \end{bmatrix} \tag{26}$$

where K_{i1} is a positive gain matrix, ε is a positive constant, $0 < \alpha_i < 1$, and the switching function $\xi(e_i^p)$ is defined as:

$$\xi(e_i^p) = \begin{cases} 0, \|e_i^p\| \geq \overline{C} \\ 1, \|e_i^p\| \leq \overline{C} \end{cases}$$

with $\overline{C}$ representing a adjustable threshold.

Noting that the computations of $\dot{v}_i^d(\dot{\hat{q}}_j, \dot{\hat{p}}_j)$ and $\dot{\omega}_i^d(\dot{\hat{q}}_j, \dot{\hat{p}}_j)$ require for $\dot{\hat{q}}_j$ and $\dot{\hat{p}}_j$. The time derivative of $\hat{q}_j$ and $\hat{p}_j$ are computed by finite difference, which are not applications in continuous space. To avoid requiring $\dot{\hat{q}}_j$ and $\dot{\hat{p}}_j$, we introduce the dynamic sliding mode through the definition of $q_i^f = [v_i^f, \omega_i^f]^\top$.

Assumption 3: In practical applications, the velocity and acceleration state of the robot are limited due to the energy limitation and hardware constraints. Therefore, it can give a reasonable assumption that $\|(1-\nu_{ij})\dot{q}_j + \nu_{ij}\dot{\hat{q}}_j\| \leq \rho_q$ with the positive constant ρ_q.

By letting q_i^d pass through a first-order filter with a coefficient matrix $\ell_i = \mathrm{diag}\{\ell_{i1}, \ell_{i2}\}$, the variable q_i^f is obtained

$$q_i^d = \ell_i\dot{q}_i^r + q_i^r, q_i^d(0) = q_i^r(0) \tag{27}$$

where the time constant matrix ℓ_i is to be determined.

The following transformation error is defined as $Q_i = q_i^d - q_i^r$, where $Q_i = [\jmath_{i1}, \jmath_{i2}]^\top$. The tracking error of velocity layer is defined as $e_i^q = q_i - q_i^r$. According to (1), the time derivative of e_i^q can be derived as follows:

$$e_i^q = M_i\tau_i - C_i\begin{bmatrix} v_i\omega_i \\ \omega_i^2 \end{bmatrix} - G_i\begin{bmatrix} v_i \\ \omega_i \end{bmatrix} - \ell_i^{-1}Q_i \tag{28}$$

Then, the control command τ_i is given as follows

$$\begin{aligned} \bar{\tau}_i &= -K_{i2}e_i^q + C_i\begin{bmatrix} v_i\omega_i \\ \omega_i^2 \end{bmatrix} + G_i\begin{bmatrix} v_i \\ \omega_i \end{bmatrix} + \ell_i^{-1}Q_i - J_{ij}e_i^p \\ \tau_i &= M_i^{-1}\tau_i \end{aligned} \tag{29}$$

We define the following Lyapunov candidate function:

$$V = \frac{1}{2}e_i^{p\top}e_i^p + \frac{1}{2}e_i^{q\top}e_i^q + \frac{1}{2}Q_i^\top Q_i \tag{30}$$

The time derivative of V can be described as

$$\dot{V} = e_i^{p\top}\dot{e}_i^p + e_i^{q\top}\dot{e}_i^q + Q_i^\top\dot{Q}_i \tag{31}$$

By (25), (26), and (29), $\dot{V}$ can be rewritten as

$$\begin{aligned} \dot{V} \leq &- \frac{\lambda_{\min}(K_{i1})e_i^{p\top}e_i^p}{\|\|e_i^p\|^{\alpha_i} - \xi(e_i^p)(\overline{C}+\varepsilon)\|} - \lambda_{\min}(K_{i2})e_i^{q\top}e_i^q \\ &- \ell_i^{-1}Q_i^\top Q_i + \|Q_i\|\|\dot{q}_i^d\| \end{aligned} \tag{32}$$

where $\lambda_{\min}(K_{i1})$ and $\lambda_{\min}(K_{i2})$ denote the smallest eigenvalue of the matrix K_{i1} and K_{i2}, respectively.

Applying Young's inequality for two variables Q_i and $\dot{q}_i^d$, it can be obtained as follows

$$\begin{aligned} \dot{V} \leq &- \frac{\lambda_{\min}(K_{i1})e_i^{p\top}e_i^p}{\|\|e_i^p\|^{\alpha_i} - \xi(e_i^p)(\overline{C}+\varepsilon)\|} - \lambda_{\min}(K_{i2})e_i^{q\top}e_i^q \\ &- \ell_i^{-1}Q_i^\top Q_i + \|Q_i\|^2\|\dot{q}_i^d\|^2 + 1 \\ \leq &- (\frac{1}{\ell_i} - \rho_q^2)\|Q_i\|^2 - \left(1 - \frac{\|\dot{q}_i^d\|}{\rho_q^2}\right)\rho_q^2\|Q_i\|^2 + 1 \\ &- \frac{\lambda_{\min}(K_{i1})e_i^{p\top}e_i^p}{\|\|e_i^p\|^{\alpha_i} - \xi(e_i^p)(\overline{C}+\varepsilon)\|} - \lambda_{\min}(K_{i2})e_i^{q\top}e_i^q \end{aligned} \tag{33}$$

where $\ell_i^{-1} > \rho_p^2$.

Defining a parameter β_i as $\beta_i = \min(\lambda_{\min}(K_{i2}), \ell_i^{-1} - \rho_p^2, \lambda_{\min}(K_{i1})/\varepsilon)$. If choosing $\beta_i \geq 1/\rho_V$ with respect to positive constant ρ_V, then it is clear that $\dot{V} \leq 0$ on $V = \rho_V$. When $V \leq \rho_V$, the inequality (33) yields

$$0 \leq V \leq \frac{1}{\beta_i} + (V(t_k^{on}) - \frac{1}{\beta_i})\exp(-\beta_i t) \tag{34}$$

According to (34), if the initial formation error $e_i^p(t_k^{on})$ in the kth DoS attack-shut satisfies $\|e_i^p(t_k^{off})\| \leq \overline{C}$, the formation error $e_i^p(t)$ in $t \in [t_k^{off}, t_k^{on}]$ can converge to the bounded region

$$-\sqrt{\frac{\{\|e_i^p\|^{\alpha_i} - \xi(e_i^p)\bar{C}\}}{\lambda_{\min}(K_{i1})}} \leq e_i^p \leq \sqrt{\frac{\{\|e_i^p\|^{\alpha_i} - \xi(e_i^p)\bar{C}\}}{\lambda_{\min}(K_{i1})}} \tag{35}$$

If the initial formation error $e_i^p(t_k^{on})$ in the kth DoS attack-shut exceeds the adjustable threshold i.e., $\|e_i^p(t_k^{off})\| > \overline{C}$, the formation error $e_i^p(t)$ in $t \in [t_k^{off}, t_k^{on}]$ with the variable-gain converge the compact set as follows:

$$\frac{-1}{\sqrt[2-\alpha_i]{\lambda_{\min}(K_{i1})}} \leq e_i^p \leq \frac{1}{\sqrt[2-\alpha_i]{\lambda_{\min}(K_{i1})}} \tag{36}$$

which exists the inequality as follows:

$$\dot{V}(e_i^p) \leq \lambda_{\min}(K_{i1})V(e_i^p)^{\frac{2-\alpha_i}{2}} + 1 \tag{37}$$

It is concluded that the formation error e_i^p in finite time given by $T = 2/[\theta\lambda_{\min}(K_{i1})V(e_i^p)^{(\frac{2-\alpha_i}{2})}]$ can renewedly converge to the boundary $\|e_i^p\| < \overline{C}$.

IV. Simulation

The desired local positions of the reference point are set as $p_1^{0d} = p_2^{1d} = [-1, -1]^\top$. The Luenberger observer gains are selected as $U_{p,1} = U_{p,2} = 3$ and $U_{p,1} = U_{p,2} = 4$. The control gains are selected as $K_{i1} = 3I_2$, $K_{i1} = 4I_2$, $\bar{C} = 0.2$, $\varepsilon = 0.2$, and $\ell_i = 0.01I_2$. The parameters of event-triggered mechanism parameters are chosen as $\overline{\vartheta} = \underline{\vartheta} = 0.1$, $\eta_{p0} = 3$, and $\eta_{p\infty} = 0.2$. The leader NMR moves along a circular trajectory.

Under the proposed method, the formation performances of networked NMRs against DoS attacks are shown in Fig.1. From the snapshots of Fig. 1(a) at an interval of 5s, the position

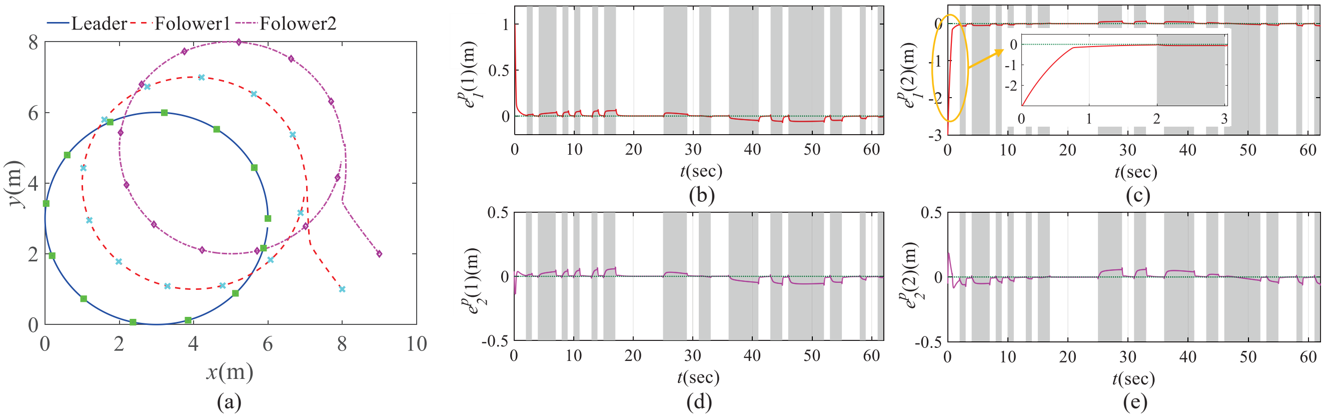

Fig. 1. Formation performances of networked NMRs in the presence of DoS attacks: (a) Trajectory for whole formation process, where snapshots of NMR position are provided at every five seconds. (b) Formation error of 1st NMR in x-axis. (c) Formation error of 1st NMR in y-axis. (d) Formation error of 2nd NMR in x-axis. (e) Formation error of 2nd NMR in y-axis.

of networked NMRs (x_i, y_i) is conducive to reaching the small neighborhood of the target formation under the DoS attack. In Figs. 1(b-e), DoS attacks are active in the gray area. Since the hard constraints render the recovery for missed signals to be limited, the formation error escaped to the unknown boundary in the presence of DoS attacks. Once formation error exceeded adjustable threshold, i.e., $e_i^p > \bar{C}$. Under the proposed specialized controller, the formation error converged to the boundary $\bar{C}$ with the finite time. Then, the networked NMRs reconverged the desired formation with variable gain.

V. Conclusions

In this paper, a novel method has been presented to handle the challenges of networked NMRs formation under DoS attacks. Firstly, to improve the accuracy of recovering the scathed signals under DoS attacks, the available historical data was utilized to approximate the Koopman operator via a finite basis function set. Utilizing the approximation model, the unavailable signals were successfully recovered to provide the preparation conditions for coping with DoS attack-active. Finally, combined with an event-triggered mechanism, the proposed controller with variable gain ensured convergence to the neighborhoods of the desired formation. The effectiveness of the proposed method under DoS attack is demonstrated by simulation experiments.

References

[1] Y. Wan, G. Wen and X. Yu, "Distributed consensus tracking of networked agent systems under denial-of-service attacks," *IEEE Trans. Syst., Man, Cyber.: Syst.* vol. 51, no. 10, pp. 6183-6196, Oct. 2021.

[2] S. -i. Azuma, M. S. Sakar and G. J. Pappas, "Stochastic source seeking by mobile robots," *IEEE Trans. Autom. Control*, vol. 57, no. 9, pp. 2308-2321, Sept. 2012.

[3] S. Musić, G. Salvietti and P. B. g. Dohmann, "HumanCrobot team interaction through wearable haptics for cooperative manipulation," *IEEE Trans. Haptics*, vol. 12, no. 3, pp. 350-362, 1 July-Sept. 2019.

[4] J. Zhao, X. Li and X. Yu, "Finite-Time cooperative control for bearing-defined leader-following formation of multiple double-integrators," *IEEE Trans. Cyber*, vol. 52, no. 12, pp. 13363-13372, Dec. 2022.

[5] A. S. Lafmejani, H. Farivarnejad, and S. Berman, "Adaptation of gradient-based navigation control for holonomic robots to nonholonomic Robots," *IEEE Robot. Auto. Letters*, vol. 6, no. 1, pp. 191-198, Jan. 2021.

[6] Z. Miao, Y. -H. Liu, and Y. Wang, "Distributed estimation and control for leader-following formations of nonholonomic mobile robots," *IEEE Trans. Auto. Sci. Eng.*, vol. 15, no. 4, pp. 1946-1954, Oct. 2018.

[7] Z. Zhang and J. Dong, "Fault-tolerant containment control for IT2 fuzzy networked multiagent systems against denial-of-service attacks and actuator faults," *IEEE Trans. Syst., Man, Cyber.: Syst.*, vol. 52, no. 4, pp. 2213-2224, April 2022.

[8] Y. -S. Ma, W. -W. Che and C. Deng, "Distributed model-free adaptive control for learning nonlinear MASs under DoS attacks," *IEEE Trans. Neural Net. Learning Syst.*, vol. 34, no. 3, pp. 1146-1155, March 2023.

[9] Y. Zhang, G. Wang, and J. Sun, "Distributed observer-based adaptive fuzzy consensus of nonlinear multiagent systems under DoS attacks and output disturbance," *IEEE Trans. Cyber.*, vol. 53, no. 3, pp. 1994-2004, March 2023.

[10] Y. Wan, G. Wen, and X. Yu, "Distributed consensus tracking of networked agent systems under denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 51, no. 10, pp. 6183-6196, Oct. 2021.

[11] P. Wang, G. Wen, and X. Yu, "Synchronization of resilient complex networks under attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 2, pp. 1116-1127, Feb. 2021.

[12] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Trans. Control Sys. Technol.*, vol. 28, no. 3, pp. 741-752, May 2020

[13] L. Ding, Q. -L. Han and B. Ning, "Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4909-4919, July 2020.

[14] W. Xu, G. Hu, and D. W. C. Ho, "Distributed secure cooperative control under denial-of-service attacks from multiple adversaries," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3458-3467, Aug. 2020

[15] Y. Xu, M. Fang and Z. -G. Wu, "Input-based event-triggering consensus of multiagent systems under denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 4, pp. 1455-1464, April 2020.

[16] D. Zhang, L. Liu and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans Cybern.*, vol. 49, no. 4, pp. 1501-1511, April 2019.

[17] C. D. Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930-2944, Nov. 2015.

[18] M. Korda and I. Mezić, "Linear predictors for nonlinear dynamical systems: koopman operator meets model predictive control," *Automatica*, vol. 93, pp. 149-160, 2018.

[19] D. P. Kingma and J. Ba, "Adam: a method for stochastic optimization," 2014, arXiv:1412.6980.