Adaptive Resilient Formation for Multi-agent Systems Subject to Cyber Attacks

Kunpeng Pan(✉), Quan Pan, and Yang Lyu

School of Automation, Northwestern Polytechnical University, Xi'an, Shaanxi 710129, China
pankunpeng@mail.nwpu.edu.cn, quanpan@nwpu.edu.cn

Abstract. This article investigates the problem of adaptive time-varying resilient formation for multi-agent systems (MASs) under cyber attacks. First, MASs model, energy-limited DoS attacks and actuator attacks are described. Second, an adaptive formation control protocol for MASs is proposed. Sufficient conditions on the control gain and duration of the DoS attacks are given in terms of linear matrix inequalities. Finally, an example is given to verify the feasibility of a resilient formation scheme.

Keywords: Resilient formation · DoS attacks · Actuator attacks · Multi-agent systems

1 Introduction

Multi-agent systems (MASs) are widely used in UAV, power systems, robots, and other fields, due to they are more efficient than a single agent system to complete complex tasks. The deep integration of network communication and MASs builds a bridge of communication between agents, but it is also easy to be attacked by cyber-attacks. It becomes an obstacle to guaranteeing the security of MASs. Thus, it is necessary and urgent to study the security problem of MASs [1,2].

Cyber-attacks are diverse, such as actuator attacks, sensor attack [3], denial of service (DoS) attack [4], deception attack [5], false data injection attack, replay attack. Fruitful theoretical results show that many researchers have studied the security problems of MASs, which can be roughly divided into three aspects: attack detection [6], security state estimation [7], resilience/security control [1,8]. For the first class, authors in the paper [9] propose a set-membership filtering approach to detect attacks. This method can accurately detect attacks, but it involves an iterative algorithm and convex optimization problem solving, which is complicated. From another perspective, Jan et al. [10] designed a detection scheme through a graph analysis approach. Based on graph theory, it is less complicated than traditional distributed filter methods. Attack detection plays a critical role in cyber-security by determining the occurrence of attacks but can obtain no more state and attack information.

Z. Ren et al. (Eds.): *Proceedings of 2021 5th Chinese Conference on Swarm Intelligence and Cooperative Control*, LNEE 934, pp. 629–638, 2023.
https://doi.org/10.1007/978-981-19-3998-3_60

Security state estimation is concerned with system state and attack information. Fawzi et al. [11] propose a method to achieve secure state estimation for MASs subject to sensor attacks. They first characterize the number of attacked sensors and then propose a specific computationally feasible decoding algorithm. The same sensor attacks, Lu et al. [12,13] propose a switched Lunberger observer to achieve secure state estimation for cyber-physical systems, and the attack type is defined as sparse sensor attack. Although all of the above works of literature can achieve security state estimation, they have in common that they target a single type of sensor attack. Secure state estimation of cyber-physical systems under switching attacks is investigated in [7]. Resilient control means the system can operate stably under attacks. In [14], for linear MASs subjected to random attacks, a secure consistency control scheme is proposed, the core idea of which is to design a distributed observer. Shang et al. [15] propose a switched filtering strategy for cooperative nodes based upon available local information, withstanding the threat of non-cooperative nodes. The two control schemes designed from observer and filter are reliable and ensure the safe operation of multi-agent under attack.

However, most of the MASs mentioned above have fixed weights and are subject to attack. Attacks are often mixed and injected simultaneously. This paper considers the adaptive formation problem for MASs under two types of attacks: DoS attack and actuator attack. Inspired by [16], the decay rate and attack duration are taken into account in the design process. The main contributions of this paper are summarized as follows:

1. Resilient formation protocol for MASs with adaptive adjusting weights is proposed. DoS attacks and actuator attacks are considered simultaneously.
2. For DoS attacks, various attack models are considered. Sufficient conditions for controller gain, decay rate, and maximum allowable DoS attack duration are given in the form of LMI.

The rest is organized as follows. Section 2 describes the leader-following MAS model and hybrid attacks, including energy-limited DoS attacks and actuator attacks. In Sect. 3, an adaptive resilient formation is proposed under hybrid attacks. By orthogonal transformation, the control gain and decay rate are given as LMIs. Section 4 analyzes the stability and gives the maximum attack duration. The simulation results are given in Sect. 5, and Sect. 6 concludes the whole paper.

Notation: The superscript T stands for a matrix transposition, and $S > 0$, $S < 0$ denote positive-definiteness and negative-definiteness. $\lambda_{max}(R)$ and $\lambda_{min}(R)$ denote the largest and smallest eigenvalues of R, respectively. $\mathbb{R}^{n\times n}$ denotes the n-dimensional Euclidean space and $\mathbb{R}^{n\times m}$ denotes the $n \times m$ real matrices. $*$ in the symmetric matrix stands for the symmetric terms, and $\otimes$ is Kronecker product. $He(R) = R^T + R$. $\mathbf{0}$ and $\mathbf{I}$ denote the zero matrices and unit matrix with appropriate dimensions. For interval $\mathcal{D}(t_1, t_2)$, $|\mathcal{D}(t_1, t_2)|$ is its length over $[t_1, t_2)$. Given two sets Φ_1 and Φ_2, $\Phi_1 \backslash \Phi_2$ is the relative complement of Φ_2 in Φ_1.

2 Preliminaries

2.1 Graph Theory

In this article, the communication topology of a leader-follower MASs is represented by a graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ are the set of vertices that represents the local agents and the set of edges that stands for the communication links, respectively. Followers are unconnected to each other, and their connection to the leader is directed. It is assumed that $\mathcal{V} = \{0, 1, \cdots, N\}$ without loss of generality. MASs with one leader and N followers are studied, where the leader is labeled 0 and the followers are labeled $1, 2, 3 \cdots, N$. An edge $(i, j) \in \mathcal{E}$ denotes that j can obtain information from i. The intensity of the connection is called the weight. The index set $\mathcal{N}_i = \{j : (j, i) \in \mathcal{E}\}$ is applied to represent the neighbor set of agent i. We define $0-1$ Laplacian matrix of L as $L = [l_{ij}] \in \mathbb{R}^{(N+1)\times(N+1)}$ with $l_{ii} = \sum_{j=0, j\neq i}^{N} \omega_{ij,0}$, $l_{ij} = -\omega_{ij,0} = -1$ if $(v_i, v_j) \in \mathcal{E}$ and $l_{ij} = 0$, otherwise. We define a variable Laplace matrix $L(t) = [l_{ij}(t)] \in \mathbb{R}^{(N+1)\times(N+1)}$ with $l_{ij}(t) = l_{ij}\omega_{ij}(t)$ where $\omega_{ij}(t) \geq 1$ is designed later.

2.2 System Description

We consider a second-order leader-following MAS with N followers. The dynamic model of the leader and follower are presented as:

$$\dot{p}_0(t) = v_0(t), \dot{v}_0(t) = 0,$$
$$\dot{p}_i(t) = v_i(t), \dot{v}_i(t) = u_i(t),$$

where p_0, p_i and v_0, v_i are the position and velocity vectors of leader and ith follower, respectively. The formation structure for MAS is specified by a vector function $f(t) = [f_0, f_1, \cdots f_N]$, where $f_0 = \mathbf{0}, f_i = [f_{ip}, f_{iv}]$. Let

$$\psi_0 = \begin{bmatrix} \psi_{0p} \\ \psi_{0v} \end{bmatrix} = \begin{bmatrix} p_0 \\ v_0 \end{bmatrix}, \psi_i = \quad \begin{bmatrix} \psi_{ip} \\ \psi_{iv} \end{bmatrix} = \begin{bmatrix} p_i - f_{ip} \\ v_i - f_{iv} \end{bmatrix}$$

and it has

$$\dot{\psi_0} = A\psi_0 + Af_0 - \dot{f}_0, \dot{\psi_i} = A\psi_i + Bu_i + Af_i - \dot{f}_i, \tag{1}$$

where $A = \begin{bmatrix} \mathbf{0} & \mathbf{I} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$ and $B = \begin{bmatrix} \mathbf{0} \\ \mathbf{I} \end{bmatrix}$ are system matrices. $u_i(t)$ is the resilient protocol to be designed. $u_i(t)$ is the formation protocol to be designed.

2.3 Attacks Description

DoS Attack. As a common attack in network system, DoS attacks block network communication, making part or all control units ineffective. This article shows that different channels are attacked independently of each other. In addition, attacks occur in pairs, where (i, j) and (j, i) are attacked, simultaneously. The following assumptions are given to illustrate the main results.

Assumption 1. *[17](DoS Duration) Consider scalars $\xi_{ij} > 0$ and $0 < \mu_{ij} < 1$ such that*

$$|\mathcal{D}_{(i,j)}(s,t)| \leq \xi_{ij} + \mu_{ij}(t-s) \tag{2}$$

where $\mathcal{D}_{(i,j)}(s,t)$ stand for the union of DoS intervals of channel (i,j) over $[s,t)$. μ_{ij} is the attack intensity. The bigger the μ_{ij}, the more intense the attack.

By [16], the the set of channels attacked at time t are defined as

$$\digamma(t) = \{(i,j) \in \mathcal{E} | t \in \mathcal{D}_{(i,j)}(0,+\infty)\} \tag{3}$$

and define$\Xi_{\digamma}(t_1,t_2) = (\cap_{(i,j)\in\digamma}\mathcal{D}_{(i,j)}(t_1,t_2)) \cup (\cap_{(i,j)\notin\digamma}\bar{\mathcal{D}}_{(i,j)}(t_1,t_2))$ as the union of the intervals where the channels indexed by the set $\digamma \in \mathcal{E}$ are attacked and the channels indexed by $\mathcal{E} \setminus \digamma$ are not attacked. Herein, $\bar{\mathcal{D}}_{(i,j)}(t_1,t_2) = [t_1,t_2] \setminus \mathcal{D}_{(i,j)}(t_1,t_2)$.

Actuator Attack. In addition to DoS attacks, the framework also considers actuator attacks. Then, the system input $\tilde{u}_i$ is represented as $\tilde{u}_i = u_i(t) + \mathfrak{a}_i(t)$, where u_i and $\mathfrak{a}_i$ are the formation control protocol and actuator attacks injected into MASs. It is a nonlinear function with respect to MAS states.

Assumption 2. *[18] Actuator attacks satisfies $\|\mathfrak{a}_i(\zeta(t))\|_2 \leq \|G\zeta(t)\|_2$, where G is a given matrix. $\zeta(t)$ is attack variables from system state.*

Remark 1. The matrix G is defined as a restrictive condition for actuator attacks, whose value is determined by attack detection. It is assumed that the construction information of the attacks comes from the state information $\psi_i(t)$ and $\psi_0(t)$, and then the attack model changes the state of the system. In order to ensure concealment, the attack variable $\zeta(t)$ selects a finite energy value such as $\psi_i(t) - \psi_0(t)$. In such a way, the adversaries are easier to escape from network security detections.

3 Formation Protocol

An adaptive resilient formation protocol for MASs subject to DoS attack and actuator attack is given as follows:

$$\begin{aligned} u_i(t) =& \omega_{i0,0}\omega_{i0}(t)K_u(\psi_0 - \psi_i) + K_u \sum_{j\in\mathcal{N}_i, i\neq 0 (j,i)\notin\digamma(t)} (\omega_{ij,0}\omega_{ij}(t)(\psi_j - \psi_i)) \\ \dot{\omega}_{ij}(t) =& \dot{\omega}_{ji}(t) = (\psi_j - \psi_i))^T K_\omega(\psi_j - \psi_i)) \end{aligned} \tag{4}$$

where $i,j = 1,2,\cdots,N$. $Q = Q^T \in \mathbb{R}^{n\times n} > 0$ is the gain matrix. $K_u \in \mathbb{R}^{m\times n}$ and $K_\omega = K_\omega^T \in \mathbb{R}^{n\times n}$ are the controller gain matrix and adaptive weight gain matrix, which are to be designed. The definition of $\omega_{ij,0}$ and $\omega_{ij}(t)$ are given as Definition 1. Under DoS attacks and FDI attack, the control target of resilient formation of MASs makes $\lim_{t\to+\infty}\psi_i - \psi_0 = 0$ by obtaining appropriate K_u and K_ω.

Definition 1. *$\omega_{ij,0}$ is the $0-1$ weight of agent j to agent i. If agent i can receive information from agent j, $\omega_{ij,0}=1(i\neq j)$; otherwise, $\omega_{ij,0}=0$. $\omega_{ij}(t)$ is the adaptive change coefficient, and its initial value is $\omega_{ij}(0)=\omega_{ji}(0)=1$. $\dot{\omega}_{ij}(t)=\dot{\omega}_{ji}(t)$ and $\omega_{ij}(t)=\omega_{ji}(t)$ are obtained from the equality definition of $\dot{\omega}_{ij}(t)$. According to the definition of $0-1$ action weight $\omega_{ji,0}$ and its adaptive coefficient $\omega_{ji}(t)$, the 0-1 Laplace matrix L and Laplace matrix $L(t)$ are given as:*

$$
\begin{aligned}
L=&\begin{bmatrix}0 & \mathbf{0}\\ L^{fl} & L^{ff}+\Delta^{fl}\end{bmatrix}, L(t)=\begin{bmatrix}0 & \mathbf{0}\\ L^{fl}(t) & L^{ff}(t)+\Delta^{fl}(t)\end{bmatrix},\\
L^{fl}=&\begin{bmatrix}-\omega_{10,0} & -\omega_{20,0} & -\omega_{30,0}\cdots -\omega_{N0,0}\end{bmatrix}^T,\\
\Delta^{fl}=&diag([-\omega_{10,0},\cdots,-\omega_{N0,0}])\\
L^{fl}(t)=&\begin{bmatrix}-\omega_{10,0}\omega_{10}(t)\cdots\cdots -\omega_{N0,0}\omega_{N0}(t)\end{bmatrix}^T,\\
\Delta^{fl}(t)=&diag(-\omega_{10,0}\omega_{10}(t),\cdots,\cdots,-\omega_{N0,0},\omega_{N0}(t))\\
L^{ff}=&\begin{bmatrix}\sum_{i=1}^{N}\omega_{1i,0} & -\omega_{12,0} & \cdots & -\omega_{1N,0}\\ -\omega_{21,0} & \sum_{i=1}^{N}\omega_{2i,0} & \cdots & -\omega_{2N,0}\\ \cdots & \cdots & \cdots & \cdots\\ -\omega_{N1,0} & -\omega_{N2,0} & \cdots & \sum_{i=1}^{N}\omega_{Ni,0}\end{bmatrix}\\
L^{ff}(t)=&\begin{bmatrix}\sum_{i=1}^{N}\omega_{1i,0}\omega_{1i}(t) & \cdots & -\omega_{1N,0}\omega_{1N}(t)\\ \cdots & \ddots & \cdots\\ -\omega_{N1,0}\omega_{N1}(t) & \cdots & \sum_{i=1}^{N}\omega_{Ni,0}\omega_{Ni}(t)\end{bmatrix}
\end{aligned}
$$

Defining $\hat{\psi}(t)=\begin{bmatrix}\psi_1(t)-\psi_0(t)\cdots\psi_N(t)-\psi_0(t)\end{bmatrix}^T$, we can obtain

$$
\dot{\hat{\psi}}(t)=(I_N\otimes A-(L^{ff}(t)+\Delta^{fl}-L_F^{ff}(t)-\Delta_F^{fl})\otimes BK_u)\hat{\psi}(t)+I_N\otimes B\zeta(\hat{\psi}). \tag{5}
$$

To get the sufficient conditions of the resilient formation protocol, Theorem 1 is given.

Theorem 1. *For a connected undirected graph with agents (1), given decay rate β_F and constant γ, if there exist positive symmetric X such that*

$$
He(AX)-\beta_F X-2(\gamma+1+\underline{\lambda})BB^T+XG^TGX<0 \tag{6}
$$

where $\underline{\lambda}=\lambda min(L^{ff}-L_F^{ff})$, $X=P^{-1}$, and $F\in\mathcal{E}$, under the distributed formation controller (4) with $K_u=B^TP$ and adaptive weight gain $K_\omega=PBB^TP$, the inequality is guaranteed

$$
\dot{V}(t)<\beta_F V(t). \tag{7}
$$

Proof. Introducing translation factor $\gamma>0$, the Lyapunov function is chosen as

$$
\begin{aligned}
V(t)=&\hat{\psi}^T(t)(I_N\otimes P)\hat{\psi}(t)+2\gamma\sum_{i=1}^{N}(\gamma_{0i}-\omega_{0i}(t))\\
&+\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{(\omega_{ij,0}\omega_{ij}(t)-\omega_{ij,0})^2}{2}\mid_{(j,i)\notin F(t)}
\end{aligned} \tag{8}
$$

where $\gamma_{0i} \geq \omega_{0i}(t)$, that is $V(t) > 0$. When $I_N \otimes (He(AX) - \beta_{\digamma} X) - 2(\gamma I_N + L^{ff} + \Delta^{fl} - L_{\digamma}^{ff} - \Delta_{\digamma}^{fl}) \otimes BB^T + XG^{\top}GX < 0$, there is $\dot{V}(t) < \beta_{\digamma} V(t)$.

4 Stability Analysis

In this section, we focus on analyzing the stability of the closed-loop system under DoS attacks and FDI attacks. Inspired by switched systems, the concept of the subsystem is introduced. θ_1^{ij} and θ_2^{ij} are defined as two subsystems, corresponding to $(i,j) \in \digamma$ with and without DoS attack. Then, Theorem 2 is given for stability analysis.

Theorem 2. *For a connected undirected graph with system (1), given decay rates $\beta_{\digamma}$ in (6), if there exist scalars $\theta_1^{ij}, \theta_2^{ij}$ and attack intensity μ_{ij} such that*

$$\theta_1^{ij} - \theta_2^{ij} \geq 0 \tag{9}$$

$$\beta_{\digamma} - \Big(\sum_{(i,j)\in\digamma} \theta_1^{ij} + \sum_{(i,j)\in\mathcal{E}\setminus\digamma} \theta_2^{ij} \Big) \leq 0 \tag{10}$$

$$\bar{\mu} = \sum_{(i,j)\in\mathcal{E}} (\mu_{ij}\theta_1^{ij} + (1-\mu_{ij})\theta_2^{ij}) < 0, \tag{11}$$

the MASs can still achieve formation control under DoS attacks satisfying Assumption 1 and FDI attaks satisfying Assumption 2.

Proof. Assume that $\epsilon_k (\epsilon_0 = 0)$ are the time instants which $\digamma(t)$ changes. When $t \in [\epsilon_k, \epsilon_{k+1})$, according to (7), we get

$$V(t) \leq e^{\mathfrak{D}_k} V(\epsilon_0) = e^{\mathfrak{D}(0,t)} V(0) \tag{12}$$

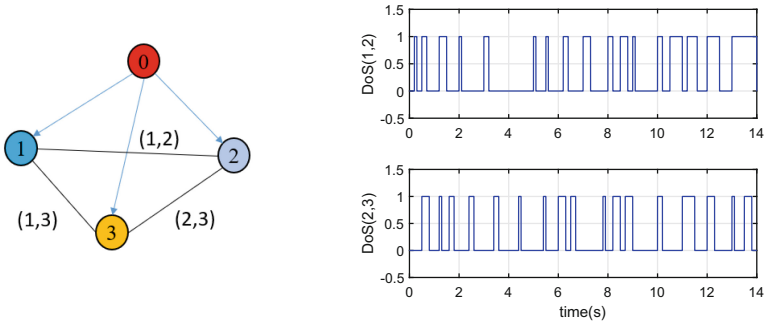
where $\mathfrak{D}_k = \beta_{\digamma(\epsilon_k)}(t-\epsilon_k) + \sum_{p=1}^{k} \beta_{\digamma(\epsilon_p)}(\epsilon_p - \epsilon_{p-1})$, $\mathfrak{D}(0,t) = \sum_{\digamma\in\mathcal{E}} \beta_{\digamma} |\Xi_{\digamma}(0,t)|$. Due to (10), one can obtain

$$\mathfrak{D}(0,t) \leq \bar{\mu} t + \bar{\xi} \tag{13}$$

where $\bar{\xi} = \sum_{(i,j)\in\mathcal{E}} (\theta_1^{ij} - \theta_2^{ij}) \xi_{ij}$. From (12)and (13), it has $\lim_{t\to+\infty} V(t) = 0$, that is,

$$\lim_{t\to+\infty} (\hat{\psi}^T(t)(I_N \otimes P)\hat{\psi}(t) + 2\gamma \sum_{i=1}^{N} (\gamma_{0i} - \omega_{0i}(t)) + \sum_{i=1}^{N}\sum_{j=1}^{N} \frac{(\omega_{ij,0}\omega_{ij}(t) - \omega_{ij,0})^2}{2} |_{(j,i)\notin\digamma(t)}) = 0.$$

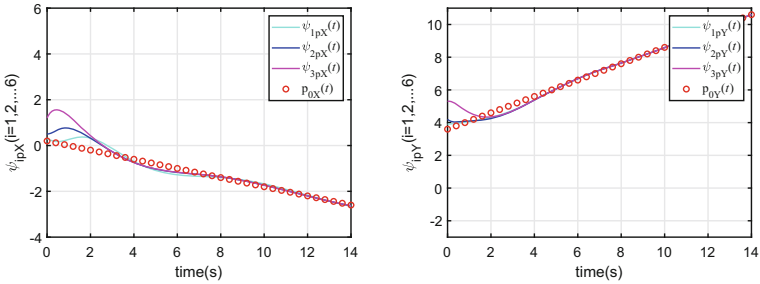
Thus, $\lim_{t\to+\infty} \hat{\psi}^T(t)(I_N \otimes P)\hat{\psi}(t) = 0$, which yields $\lim_{t\to+\infty} \parallel \hat{\psi}(t) \parallel = 0$. Due to $\hat{\psi}_i(t) = \psi_i(t) - \psi_i(0)$, we obtain $\lim_{t\to+\infty}(x_i - f_i - x_0) = 0$, which is our control target.



(a) Communication graph with a leader and three followers.

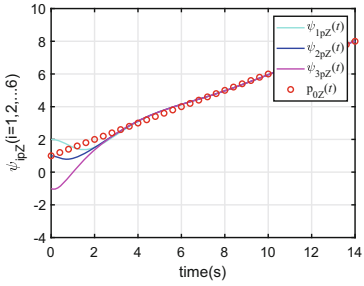
(b) DoS attack signals. 1/0 means there is/is no attack on channel (i, j).

Fig. 1. Velocity state errors between leader and followers under hybrid attacks.



(a) Trajectories of ψ_{ipX} and p_{0X}.

(b) Trajectories of ψ_{ipY} and p_{0Y}.



(c) Trajectories of ψ_{ipZ} and p_{0Z}.

Fig. 2. Position state (p_i) error between leader and followers under hybrid attacks.

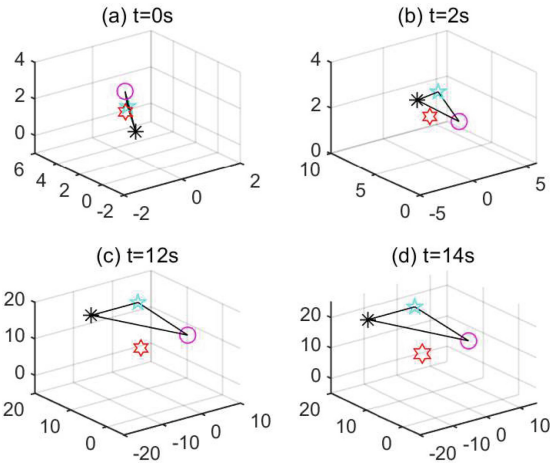
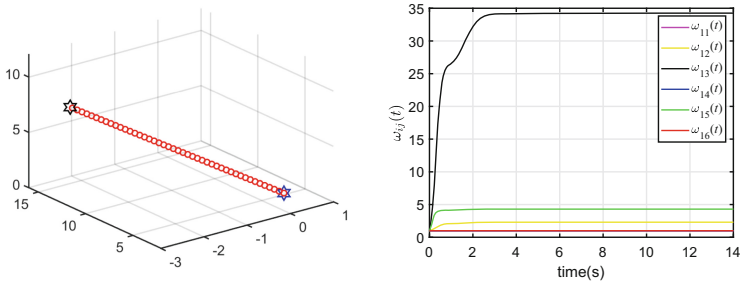


Fig. 3. State snapshots of all the agents at different monments.



(a) Movement track of the leader. (b) Trajectories of weights.

Fig. 4. Movement track of the leader and Trajectories of weights.

5 Analysis of Simulation Results

In this section, a MAS comprises a leader, and three follows, whose communication topology is shown in Fig. 1 (a). The model is considered as $[p_i, v_i] = [p_i, v_i] = [p_{iX}, p_{iY}, p_{iZ}, v_{iX}, v_{iY}, v_{iZ}]^T$. DoS attacks are injected in MASs, which are shown as 1 (b). In the simulation process, given the decay rate β_F where $F = \{(1,2),(2,1),(2,3),(3,2)\}$, β_F are chosen as $-0.5, -0.1, 2$ with $|F| = 0, 2, 4$. By Theorem 1, we get the controller gain under hybrid attacks. Meanwhile, the maximum attack duration is $\mu_{12} = \mu_{13} = \mu_{23} = 0.2213$, respectively. For FDI attack, we choose $G = [0.01, 0.01, 0.01, 0.01, 0.01, 0.01]$, $\zeta(t) = [tanh(0.01 * \psi_1)), 0, 0]^\top$.

For X, Y, and Z directions, the states of all followers converge asymptotically to the leader. Figure 2 describes the position state of the follower converging asymptotically to that of the leader. The follower's velocity state described by Fig. 3 shows the state snapshots of each agent at different moments, where the

three followers and a leader are marked by asterisks, pentagons, circles, hexagrams, respectively. In a time-varying formation, all followers stay formation with the leader, which runs in a straight line and is described as shown in Fig. 4. Figure 4 (a) describes the movement process of the leader, which begins with a blue hexagon and ends with a black one. Figure 4 (b) is the time-varying curve of the adaptive weight change coefficient in the leader-follower case, which converges to a finite value eventually. Therefore, for the leader-follower MASs under DoS attacks and FDI attacks, all the agents achieve the desired formation with control protocol (4).

6 Conclusion

Under hybrid attacks, a new adaptive, resilient formation protocol is proposed for undirected topology leader-follower MASs based on time-varying edge weights. Each channel is attacked independently and randomly. Sufficient conditions for the control protocol and DoS duration are given through LMIs, and the controller gain and DoS duration are obtained by giving the decay rates, and stability is guaranteed. However, the scheme of this article can only deal with the resilient formation of undirected graphs and will extend it to directed graphs in the future.

References

1. Feng, Z., Wen, G., Hu, G.: Distributed secure coordinated control for multiagent systems under strategic attacks. IEEE Trans. Cybernetics **47**(5), 1273–1284 (2017)
2. Wan, Y., Wen, G., Yu, X., Huang, T.: Distributed consensus tracking of networked agent systems under denial-of-service attacks. IEEE Trans. Syst. Man Cybernetics Syst. **51**, 1–14 (2020). https://doi.org/10.1109/TSMC.2019.2960301
3. Gao, R., Huang, J.: Leader-following consensus of uncertain strict feedback multiagent systems subject to sensor and actuator attacks. Int. J. Robust Nonlinear Control **30**(17), 7635–7654 (2020)
4. Zhi, F., Hu, G.: Distributed secure average consensus for linear multi-agent systems under dos attacks. In: 2017 American Control Conference, ACC (2017)
5. Ma, L., Wang, Z., Yuan, Y.: Consensus control for nonlinear multi-agent systems subject to deception attacks. In: International Conference on Automation & Computing (2016)
6. Pasqualetti, F., Dorfler, F., Bullo, F.: Attack detection and identification in cyber-physical systems. IEEE Trans. Autom. Control **58**(11), 2715–2729 (2013)
7. Forti, N., Battistelli, G., Chisci, L., Sinopoli, B.: Secure state estimation of cyber-physical systems under switching attacks. Ifac Papersonline **50**(1), 4979–4986 (2017)
8. Li, X.M., Xiao, W., Zhou, Q., Li, H.: Secure consensus control for time-varying multi-agent systems with mixed types attacks. In: 2019 6th International Conference on Information, Cybernetics, and Computational Social Systems, ICCSS (2019)
9. Mousavinejad, E., Ge, X., Han, Q.L., Yang, F., Vlacic, L.: Detection of cyber attacks on leader-following multi-agent systems. In: IECON 2019–45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal (2019)

10. Kantert, J., Scharf, H., Edenhofer, S., Tomforde, S., Hähner, J., Muller-Schloer, C.: A graph analysis approach to detect attacks in multi-agent systems at runtime. In: 2014 IEEE Eighth International Conference on Self-Adaptive and Self-Organizing Systems, pp. 80–89, London, UK (2014)
11. Fawzi, H., Tabuada, P., Diggavi, S.: Secure state-estimation for dynamical systems under active adversaries. In: Communication, Control, & Computing (2011)
12. Lu, A.Y., Yang, G.H.: Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched luenberger observer. Inf. Sci. **417**, 454–464 (2017)
13. An, L., Yang, G.H.: Secure state estimation against sparse sensor attacks with adaptive switching mechanism. IEEE Trans. Autom. Control **63**(8), 2596–2603 (2018)
14. Yang, Y., Xu, H., Yue, D.: Observer-based distributed secure consensus control of a class of linear multi-agent systems subject to random attacks. IEEE Trans. Circuits Syst. I Regul. Pap. **66**(8), 3089–3099 (2019)
15. Shang, Y.: Resilient consensus of switched multi-agent systems. Syst. Control Lett. **122**, 12–18 (2018)
16. Lu, A.Y., Yang, G.H.: Distributed consensus control for multi-agent systems under denial-of-service. Inf. Sci. **439–440**, 95–107 (2018)
17. De Persis, C., Tesi, P.: Input-to-state stabilizing control under denial-of-service. IEEE Trans. Autom. Control **60**(11), 2930–2944 (2015)
18. Yang, F., Gu, Z., Cheng, J., Liu, J.: Event-driven finite-time control for continuous-time networked switched systems under cyber attacks. J. Franklin Inst. **357**(16), 11690–11709 (2020)