控制与决策
Control and Decision

DoS攻击下一类二阶多智能体系统的安全分组一致性研究

纪良浩, 邢子正, 杨莎莎, 肖云鹏, 李华青

引用本文:
纪良浩,邢子正,杨莎莎,肖云鹏,李华青. DoS攻击下一类二阶多智能体系统的安全分组一致性研究[J]. 控制与决策, 2022, 37(11): 2887–2896.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2021.0495

DoS攻击下一类二阶多智能体系统的安全分组一致性研究

纪良浩[1†], 邢子正[1], 杨莎莎[1], 肖云鹏[1], 李华青[2]

(1. 重庆邮电大学 图像认知重庆市重点实验室，重庆 400065；
2. 西南大学 电子与信息工程学院，重庆 400715)

摘 要: 针对拒绝服务(denial-of-service, DoS)攻击下一类二阶多智能体系统的安全分组一致性协同控制问题,区别于同类工作,在非周期性多信道独立的攻击场景下,基于复杂系统中智能体间的合作与竞争交互,提出一种新的带有状态估计器的安全分组一致性控制协议. 在该协议的作用下,首先,给出DoS攻击持续时间的约束条件,通过设计合适的李雅普诺夫函数,结合求解代数黎卡提方程得到不同攻击模式下信道的衰减率;然后,通过引入与各个信道对应的等效衰减率,克服所得衰减率与信道难以匹配的问题,并给出系统的稳定性判据;最后,通过数值实验验证理论分析所得结论的正确性和有效性.

关键词: 多智能体系统；合作-竞争交互；状态估计器；多信道；安全分组一致性

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2021.0495 **开放科学(资源服务)标识码(OSID):**

引用格式: 纪良浩,邢子正,杨莎莎,等. DoS攻击下一类二阶多智能体系统的安全分组一致性研究[J]. 控制与决策, 2022, 37(11): 2887-2896.

Security group consensus for second-order multi-agent systems with cooperative-competitive interactions subject to DoS attacks

JI Liang-hao[1†], *XING Zi-zheng*[1], *YANG Sha-sha*[1], *XIAO Yun-peng*[1], *LI Hua-qing*[2]

(1. Chongqing Key Laboratory of Image Cognition，Chongqing University of Posts and Telecommunications，Chongqing 400065，China；2. College of Electronic and Information Engineering，Southwest University，Chongqing 400715，China)

Abstract: This paper investigates the problem of security couple-group consensus for second-order multi-agent systems under DoS attacks. Different from the related studies, more complex non-periodic multi-channel independent DoS attacks are considered in our work. Comprehensively considering the cooperative and competitive interactions among the agents, a novel protocol with a state estimator for realizing security couple-group consensus is proposed. On basis of the protocol, the constraint condition for the duration of DoS attacks is given. Meanwhile, the decay rates under different attack modes are obtained by designing appropriate Lyapunov functions and solving the algebraic Riccati equations. To solve the problem that the decay rate is difficult to match with the channel, the equivalent decay rate corresponding to each channel is introduced. In addition, the stability criterion of the system is also given. Finally, several numerical simulations are designed to illustrate the correctness and effectiveness of the results.

Keywords: multi-agent systems；cooperative-competitive interaction；state estimator；multiple channels；security consensus

0 引 言

分组一致性问题是多智能体系统协同控制的根本问题,具有重要的理论研究意义和实际应用价值[1]. 近年来,随着多智能体系统在飞行器编队、智能电网以及智慧交通等领域应用的不断深入,复杂系统的安全控制问题逐渐引起了众多研究者的广泛关注[2].

在多智能体系统的安全控制中,针对信道的攻击主要包括欺骗攻击和DoS攻击. 欺骗攻击主要是将伪造数据注入信道,并替换正常信息,最终导致系统发散[3]. 与节点攻击和欺骗攻击不同,DoS攻击主要是通过恶意占用通信网络,致使节点之间缺少必要的

收稿日期: 2021-03-25；**录用日期:** 2021-07-30.

基金项目: 国家自然科学基金项目(61876200, 62072066, 62006031)；重庆市基础研究与前沿探索项目(cstc2018jcyjAX0112, cstc2019jcyj-msxmX0545)；重庆市教委科学技术研究项目重大项目(KJZD-M202100602).

†通讯作者. E-mail: jilh@cqupt.edu.cn.

交互信息[4]. 然而, 多智能体系统的控制协议正是基于节点间的交互信息设计的,因此DoS攻击会造成更大破坏. 基于以上分析可知,研究DoS攻击下多智能体系统的安全分组一致性问题更加具有实际意义.

近年来,针对DoS攻击下多智能体系统的安全一致性问题已取得了一系列的研究成果. 如针对周期性DoS攻击,文献[5]通过建立基于切换拓扑的系统模型,并结合事件触发机制设计了相应的控制方案. 文献[6]设计了基于事件触发的弹性控制方案,并准确地描述了DoS攻击周期与采样周期以及触发参数的关系. 对于非周期性DoS攻击,文献[7]设计了相应的过滤器,通过引入不断切换的过滤器应对DoS攻击造成状态信息不可用的问题. 文献[8]引入领导者-跟随者模型并提出了一种弹性协作事件触发控制方案. 对于多信道同步实施DoS攻击,文献[9-10]在此基础上分别就周期采样和非周期采样进行了较为全面的讨论. 对于多信道独立DoS攻击,文献[11-14]就此问题进行了深入讨论, 并结合事件触发机制,输出反馈机制以及估计器分别设计了相应的安全控制方案. 文献[15]根据多信道独立DoS攻击对系统拓扑连通性的影响,分别设计了两种基于观测器的弹性算法,能够有效减弱DoS攻击带来的不良影响. 文献[16]提出了一种基于事件触发通信策略的切换观测器方案,通过估计系统的网络状态,有效地调度网络中信息传输. 文献[17]对于多个攻击者独立攻击每条信道的情况,设计了不依赖于拉普拉斯矩阵特征值的动态事件触发控制协议.

针对现有研究工作,不难发现其主要存在以下几方面问题: 1) 大多数相关工作所针对的周期或非周期DoS攻击,均属于多信道同步实施攻击,针对更加灵活的多信道独立DoS攻击的相关研究工作较少[11-17]. 理论上,多信道同步DoS攻击是多信道独立DoS攻击的一种特殊形式. 针对多信道同步攻击提出的控制协议并不适用于多变的多信道独立DoS攻击. 因此,研究多信道独立DoS攻击问题显得尤为重要. 2) 已有文献中所设计的安全控制协议仅考虑了系统的整体一致性,但单一的群体一致能够解决的问题是有限的. 更多情况下,需将系统中的智能体分为多个小组,可通过组间合作完成不同的任务[18]. 如无人机编队协同攻击多个目标时,可将整个编队进行分组,每个分组针对不同目标采用不同队形,最终实现协同攻击的目的. 因此,研究分组一致安全控制协议更加具有实际意义. 3) 相关工作主要研究基于单一合作或竞争交互的多智能体系统,较少涉及多智能体之间更为普遍的合作-竞争交互[19-25]. 如铁路运输系统中,轨道资源是有限的. 火车之间即竞争轨道的使用权,同时又合作将货物运送到目的地,这都是合作-竞争在实际应用中的体现[26]. 因此,研究智能体间合作-竞争关系更加具有现实意义.

受相关研究工作的启发,本文主要研究多信道独立DoS攻击下一类二阶多智能体系统的安全分组一致性问题. 主要内容如下:

1) 相比文献[9-10]中常见的多信道同步攻击,本文采用更加灵活的多信道独立攻击. 此外, 与文献[11-17]相比,所提出安全控制协议考虑了在多信道独立DoS攻击下的二阶多智能体系统,并引入二分组机制和合作-竞争交互机制. 因此,所提出安全控制协议更具有适用性.

2) 受文献[27]的启发,本文引入状态估计器,目的是使得智能体及其所使用的估计器即使在DoS攻击的极端情况下也可以优先实现系统的局部状态一致,从而避免在DoS攻击期间智能体状态的过度偏移.

3) 由于在DoS攻击下的二阶线性系统中引入了时变拓扑,基于固定拓扑的分析方法不再适用. 本文设计时变矩阵$E(t)$替换拉普拉斯矩阵,简化系统分析.

1 预备知识

1.1 图论知识

假设多智能体系统由N个智能体组成,其拓扑关系可用一个时变的无向图$\mathcal{G}(t)=\{\mathcal{V},\mathcal{E}(t)\}$表示. 其中: $\mathcal{V}=\{1,2,\dots,N\}$为节点集,$\mathcal{E}(t)\subseteq\mathcal{V}\times\mathcal{V}$为$t$时的边集. 在无向图中,智能体$i$到$j$间传递信息的边$(i,j)\in\mathcal{E}(t)$与智能体$j$到$i$传递信息的边$(j,i)\in\mathcal{E}(t)$等价,即$(i,j)=(j,i)$. 节点$i$的相邻节点集合可表示为$N_i=\{j\in\mathcal{V}|(i,j)\in\mathcal{E}(t)\}$. $\mathcal{A}(t)=[a_{ij}(t)]\in\boldsymbol{R}^{N\times N}$为$t$时刻各节点之间连接关系的邻接矩阵,其中$a_{ij}(t)>0$为边$(i,j)$的权重. 若$(i,j)\in\mathcal{E}(t)$,则$a_{ij}(t)=1$;否则$a_{ij}(t)=0$. 本文规定$a_{ii}(t)=0$,即系统拓扑中不存在自环. t时刻无向图$\mathcal{G}(t)$的拉普拉斯矩阵定义为$L(t)=[l_{ij}(t)]\in\boldsymbol{R}^{N\times N}$,其中$l_{ii}(t)=\sum\limits_{j=1}^{N}a_{ij}(t)$,且当$i\neq j$时,$l_{ij}(t)=-a_{ij}(t)$. 考虑到系统拓扑是时变的,初始拉普拉斯矩阵定义为$L=\{L(t)|t=0\}$,初始图定义为$\mathcal{G}=\{\mathcal{V},\mathcal{E}\}$,其中$\mathcal{E}=\{\mathcal{E}(t)|t=0\}$为初始边集.

假设1 初始图$\mathcal{G}$是无向连通图.

与文献[11-12]相同,文中假设系统拓扑图是一个无向连通图. 此外,规定v_i为初始拉普拉斯矩阵L对应于特征值λ_i的特征向量,显而易见特征值满足

$0=\lambda_1\leqslant\lambda_2\leqslant\ldots\leqslant\lambda_N$.

1.2 DoS攻击模型

DoS攻击和欺骗攻击是信道攻击中常见的两种攻击方式. 与欺骗攻击在信道中注入虚假数据以此破坏数据的完整性不同, DoS攻击通过大量占用信道中的通信资源, 致使智能体之间的必要交互信息无法正常传输, 系统中的部分或全部智能体之间无法相互访问. 本文假设传输信道受到攻击, 即无法从相邻智能体处获取相关信息, 且每个信道所遭受的攻击是相互独立的. 假设1中设定系统拓扑图为无向图, 因此可合理认为, 当信道 $(i,j)\in\mathcal{E}(t)$ 受到攻击时, 信道 $(j,i)\in\mathcal{E}(t)$ 也遭受到攻击.

与文献[15]相似, 本文对于每个传输信道 $(i,j)\in\mathcal{E}(t)$ 给出以下关于DoS攻击持续时间的假设.

假设2　存在正标量 γ_{ij} 和 $\varpi_{ij}<1$ 满足如下关系:

$$\text{len}(\Lambda_{ij}(t_1,t_2))\leqslant\gamma_{ij}+\varpi_{ij}(t_2-t_1). \tag{1}$$

其中: $\Lambda_{ij}(t_1,t_2)$ 为在时间段 $[t_1,t_2)$ 内, 信道 $(i,j)\in\mathcal{E}$ 所遭受DoS攻击时间段的集合; $\text{len}(\Lambda_{ij}(t_1,t_2))$ 为在时间段 $[t_1,t_2)$ 内, 信道 $(i,j)\in\mathcal{E}$ 所遭受DoS攻击的时间总和; ϖ_{ij} 为攻击强度的大小; $\gamma_{ij}>0$ 为每条信道遭受DoS攻击的基础时间.

注1　正如文献[14]所讨论的, DoS攻击是受到限制的, 不可以无限制地持续下去, 需要在资源耗尽时终止攻击活动并休眠一段时间, 以便为下一次攻击提供能量. 因此, 式(1)中的参数 $\varpi_{ij}<1$ 是必然的, 且 ϖ_{ij} 越大, 攻击强度便越大. 此外, 大多数文献仅对信道全部遭受攻击或全部正常通信两种情况进行讨论[5-10], 本文综合考虑了各种攻击模式(相较于前者还需要考虑部分信道遭受攻击的种种情况), 此类多信道独立DoS攻击更为灵活, 这在系统安全控制上增加了难度.

对于不同的攻击模式, 定义

$$\zeta(t)=\{(i,j)\in\mathcal{E}\backslash\mathcal{E}(t)|t\in\text{len}(\Lambda_{ij}(0,\infty))\}, \tag{2}$$

作为在 t 时刻遭受攻击的信道的集合, $\mathcal{E}\backslash\mathcal{E}(t)$ 表示属于集合 $\mathcal{E}$ 而不属于集合 $\mathcal{E}(t)$.

注2　初始通信拓扑图已知, 且总信道的个数有限, 因此DoS攻击模式亦是有限的. 当某时刻部分信道遭受攻击时, 只要此时遭受攻击的信道个数或信道的组合与之前时刻已有的攻击不同, 便认为是一种新的攻击模式. 因此, 在边 $(i,j)\in\mathcal{E}$ 等价于边 $(j,i)\in\mathcal{E}$ 的前提下, 总的攻击模式为 $2^{\frac{|\mathcal{E}|}{2}}$ 种.

1.3 系统描述

假设多智能体系统由 N 个二阶智能体组成, 系统的动力学模型描述如下:

$$\begin{cases}\dot{x}_i(t)=v_i(t),\\ \dot{v}_i(t)=u_i(t),\end{cases} \tag{3}$$

其中 $x_i(t)\in\boldsymbol{R}$、$v_i(t)\in\boldsymbol{R}$ 和 $u_i(t)\in\boldsymbol{R}$ 分别为智能体 i 的位置、速度和控制输入.

为了便于分析, 对系统的模型进行转换. 令转换向量 $W_i(t)=[x_i(t),v_i(t)]^{\mathrm{T}}$, 则式(3)中的动力学模型可重写为

$$\dot{W}_i(t)=AW_i(t)+Bu_i(t). \tag{4}$$

其中: 系统矩阵 $A=\begin{bmatrix}0&1\\0&0\end{bmatrix}$, 输入矩阵 $B=\begin{bmatrix}0\\1\end{bmatrix}$. 令 $W(t)=[W_1(t),W_2(t),\ldots,W_N(t)]^{\mathrm{T}}$, 且 $u(t)=[u_1(t),u_2(t),\ldots,u_N(t)]^{\mathrm{T}}$, 由式(4), 有

$$\dot{W}(t)=(I_N\otimes A)W(t)+(I_N\otimes B)u(t). \tag{5}$$

定义1　对于任意的初始状态, 当满足下式时, 称基于合作-竞争的多智能体系统(3)可渐近实现二分组一致:

$$\begin{cases}\lim\limits_{t\to\infty}\|x_i(t)-x_j(t)\|=0,\ \varsigma_i=\varsigma_j;\\ \lim\limits_{t\to\infty}\|x_i(t)+x_j(t)\|=0,\ \varsigma_i\neq\varsigma_j.\end{cases} \tag{6}$$

$$\begin{cases}\lim\limits_{t\to\infty}\|v_i(t)-v_j(t)\|=0,\ \varsigma_i=\varsigma_j;\\ \lim\limits_{t\to\infty}\|v_i(t)+v_j(t)\|=0,\ \varsigma_i\neq\varsigma_j.\end{cases} \tag{7}$$

其中: ς_i 为第 i 个智能体所在的分组. 二分组机制确保多智能体系统在最终稳定的状态下, 两个组位置和速度值的符号是相反的.

若系统在DoS攻击下仍能够实现二分组一致, 则称多智能体系统(3)可渐近实现安全二分组一致.

2 分布式控制协议设计

本节分别从单一的分布式状态反馈控制器和基于估计器的分布式控制器两方面探讨系统在不同攻击模式下的衰减率, 以便分析系统在DoS攻击下的稳定性问题.

2.1 单一的分布式状态反馈控制器

类似于文献[12]中的状态反馈控制器, 设计如下分布式状态反馈控制器:

$$\begin{aligned}u_i(t)=c_1\Big\{&\sum_{j\in N_{S_i},(i,j)\notin\zeta(t)}a_{ij}(x_j(t)-x_i(t))-\\&\sum_{j\in N_{D_i},(i,j)\notin\zeta(t)}a_{ij}(x_j(t)+x_i(t))\Big\}+\\c_2\Big\{&\sum_{j\in N_{S_i},(i,j)\notin\zeta(t)}a_{ij}(v_j(t)-v_i(t))-\\&\sum_{j\in N_{D_i},(i,j)\notin\zeta(t)}a_{ij}(v_j(t)+v_i(t))\Big\}.\end{aligned} \tag{8}$$

其中: c_1 和 c_2 分别为关于位置和速度的耦合强度, N_{S_i} 和 N_{D_i} 分别为与节点 i 属于同一组或不同组的相邻节点集合. 控制器(8)与文献[14]中的控制器不同之处在于控制器(8)考虑了合作-竞争交互关系、二分组机制. 安全控制的基本思想是控制输入协议 $u_i(t)$ 在DoS攻击期间不进行更新.

注3 合作-竞争交互机制在多智能体系统中的表现为: 同一组中的智能体之间存在合作关系, 不同组之间的智能体是竞争关系. 智能体 i 的相邻节点只能在 N_{S_i} 或 N_{D_i} 中, 所以 $N_i = N_{S_i} \bigcup N_{D_i}$. 此外, 为降低分析难度, 本文暂且考虑二分组情况. 前 M 个节点为一组, 后 $N-M$ 个节点为一组. 由于在控制协议中同时考虑了二分组机制与合作-竞争交互关系, 所提出控制协议相较于同类工作[11-17]更具有一般性.

将式(8)代入(5), 得到

$$\dot{W}(t) = (I_N \otimes A - (E - E_{\zeta(t)}) \otimes BK)W(t). \quad (9)$$

其中: 矩阵 $K = [c_1 \ \ c_2]$; 矩阵 E 是初始拉普拉斯矩阵 L 的变换矩阵, 变换规则为

$$E = \begin{bmatrix} L_{M\times M} & -L_{M\times(N-M)} \\ -L_{(N-M)\times M} & L_{(N-M)\times(N-M)} \end{bmatrix},$$

$L_{M\times M}$ 为矩阵 L 中 M 行 M 列的子矩阵, $-L_{M\times(N-M)}$ 为将矩阵 L 中 M 行 $N-M$ 列将元素取反的子矩阵; 矩阵 $E_{\zeta(t)}$ 由矩阵 $L_{\zeta(t)}$ 变换后得到, 变换规则同上, $L_{\zeta(t)}$ 为不可通信智能体间的拉普拉斯矩阵.

定义误差向量为

$$\delta_i(t) = \begin{cases} W_i(t) - \dfrac{\bar{W}_M - \bar{W}_{N-M}}{N}, \ i = 1, 2, \ldots, M; \\ W_i(t) - \dfrac{\bar{W}_{N-M} - \bar{W}_M}{N}, \\ \quad i = M+1, M+2, \ldots, N. \end{cases} \quad (10)$$

其中: $\bar{W}_M = \sum_{i=1}^{M} W_i(t)$ 为编号从1到 M 的智能体所对应转换向量的和, $\bar{W}_{N-M} = \sum_{i=M+1}^{N} W_i(t)$ 为编号从 $M+1$ 到 N 的智能体所对应转换向量的和. 令 $\delta(t) = [\delta_1(t), \delta_2(t), \ldots, \delta_N(t)]^{\mathrm{T}}$, 由式(10), $\delta(t)$ 可通过 $W(t)$ 表达为

$$\delta(t) = (H \otimes I_n)W(t), \quad (11)$$

其中 $H = I_N - \left(\begin{bmatrix} 1_{M\times M} & -1_{M\times(N-M)} \\ -1_{(N-M)\times M} & 1_{(N-M)\times(N-M)} \end{bmatrix} / N \right)$, $1_{M\times M}$ 表示元素全为1的 M 行 M 列的子矩阵, $-1_{M\times(N-M)}$ 表示元素全为 -1 的 M 行 $N-M$ 列的子矩阵. 定义特征向量矩阵 $\Omega(t) = [\beta_1(t), \beta_2(t), \ldots, \beta_N(t)] \in \boldsymbol{R}^{N\times N}$, $\beta_i(t)$ 为与特征值 $\lambda_i(t)(i = 1, 2, \ldots, N)$ 对应的特征向量. 令 $E(t) = E - E_{\zeta(t)}$, 时变拓扑包含如下属性:

$$\Omega(t)\Omega^{\mathrm{T}}(t) = \Omega^{\mathrm{T}}(t)\Omega(t) = I_N, \quad (12)$$

$$\Omega^{\mathrm{T}}(t)E(t)\Omega(t) = \mathrm{diag}\{0, \lambda_2(t), \ldots, \lambda_N(t)\}, \quad (13)$$

$$HE(t) = E(t)H = E(t),$$

$$HE_{\zeta(t)} = E_{\zeta(t)}H = E_{\zeta(t)}. \quad (14)$$

结合式(9)~(11), 可得到 $\delta(t)$ 的导数为

$$\dot{\delta}(t) = (H \otimes I_n)\dot{W}(t) = (I_N \otimes A - E(t) \otimes BK)\delta(t). \quad (15)$$

注4 本文考虑的攻击模型为多信道独立DoS攻击, 因此系统拓扑会随着DoS攻击模式的改变而改变. 此外, 大多数文献中用于系统分析的拉普拉斯矩阵并不适用于时变拓扑. 因此, 本文综合考虑时变拓扑和合作-竞争交互机制, 设计了时变矩阵 $E(t)$ 替换拉普拉斯矩阵, 简化了系统分析.

接下来, 将使用以下定理分析在控制器(8)的作用下, 系统(9)在不同攻击模式下的衰减率.

定理1 考虑含有 N 个节点的连通无向图, 对于系统矩阵 A、输入矩阵 B 以及给定对称正定矩阵 Q 和 R, 存在正标量 $\widehat{\alpha}_2 > 0$、标量 $\widehat{\alpha}_3$ 以及对称正定矩阵 P 使得

$$A^{\mathrm{T}}P + PA - PBR^{-1}B^{\mathrm{T}}P = -Q, \quad (16)$$

$$PA + A^{\mathrm{T}}P - \widehat{\alpha}_2 P < 0, \quad (17)$$

$$PA + A^{\mathrm{T}}P - \widehat{\alpha}_3 P < 0 \quad (18)$$

成立, 则有如下不等式成立:

$$\dot{V}(t) \leqslant \alpha_{\zeta(t)}V(t), \quad (19)$$

其中 $V(t)$ 为系统(9)的李雅普诺夫函数, 且有

$$V(t) = \delta^{\mathrm{T}}(t)(I_N \otimes P)\delta(t). \quad (20)$$

证明 由式(20)可知

$$\dot{V}(t) = \dot{\delta}^{\mathrm{T}}(t)(I_N \otimes P)\delta(t) + \delta^{\mathrm{T}}(t)(I_N \otimes P)\dot{\delta}(t). \quad (21)$$

令 $\tilde{\delta}(t) = (\Omega^{\mathrm{T}}(t) \otimes I_n)\delta(t) = [\tilde{\delta}_1(t), \tilde{\delta}_2(t), \ldots, \tilde{\delta}_N(t)]^{\mathrm{T}}$, 易得 $\tilde{\delta}_1(t) = (v_1(t) \otimes I_n)(H \otimes I_n)W(t) = 0$. 根据不同的攻击模式, 分别讨论以下3种情况: 1) 在DoS攻击下系统拓扑仍能够保持连通; 2) 在DoS攻击下系统拓扑分为几个连通分支; 3) 所有信道均被攻击, 导致整个系统通信瘫痪.

1) 当 $\lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t)) \neq 0$ 时, 虽有部分信道被攻击, 但整个系统拓扑仍保持连通(初始拓扑完整, 没有DoS攻击情况也归于此类). 令 $K = \mu R^{-1}B^{\mathrm{T}}P$,

$\mu \geqslant 1/2\underline{\lambda}$,根据假设1、式(21)和(16),得到

$$\begin{aligned}&\dot{V}(t)=\\&\delta^{\mathrm{T}}(t)(I_N\otimes(A^{\mathrm{T}}P+PA)-2E(t)\otimes PBK)\delta(t)=\\&\tilde{\delta}^{\mathrm{T}}(t)(I_N\otimes(A^{\mathrm{T}}P+PA))\tilde{\delta}(t)-\\&2\tilde{\delta}(t)((\Omega^{\mathrm{T}}(t)E(t)\Omega(t))\otimes PBK)\tilde{\delta}(t)\leqslant\\&\tilde{\delta}^{\mathrm{T}}_{2:N}(t)(I_{N-1}\otimes(A^{\mathrm{T}}P+PA))\tilde{\delta}_{2:N}(t)-\\&2\tilde{\delta}^{\mathrm{T}}_{2:N}(t)\underline{\lambda}(I_{N-1}\otimes PBK)\tilde{\delta}_{2:N}(t)\leqslant\\&\tilde{\delta}^{\mathrm{T}}_{2:N}(t)(I_{N-1}\otimes(A^{\mathrm{T}}P+PA-\\&PBR^{-1}B^{\mathrm{T}}P))\tilde{\delta}_{2:N}(t)=-\sum_{i=2}^{N}\tilde{\delta}_i^{\mathrm{T}}Q\tilde{\delta}_i\leqslant\\&-\lambda_{\min}(Q)\sum_{i=1}^{N}\tilde{\delta}_i^{\mathrm{T}}\tilde{\delta}_i=\alpha_1V(t).\end{aligned}\tag{22}$$

其中

$$\underline{\lambda}=\{\lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))|\lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))>0\},$$

$$\alpha_1=\frac{-\lambda_{\min}(Q)}{\lambda_{\max}(P)},\tilde{\delta}_{2:N}(t)=[\tilde{\delta}_2(t),\tilde{\delta}_3(t),\ldots,\tilde{\delta}_N(t)]^{\mathrm{T}}.$$

2) 当$\lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))=0$时,系统拓扑在DoS攻击下不再连通,由式(22),得到

$$\dot{V}(t)\leqslant\tilde{\delta}^{\mathrm{T}}_{2:N}(t)(I_{N-1}\otimes(A^{\mathrm{T}}P+PA))\tilde{\delta}_{2:N}(t).\tag{23}$$

当存在正标量$\widehat{\alpha}_2>0$满足式(17)时,有

$$\dot{V}(t)\leqslant\widehat{\alpha}_2\lambda_{\min}(P)\sum_{i=1}^{N}\tilde{\delta}_i^{\mathrm{T}}\tilde{\delta}_i=\alpha_2V(t),\tag{24}$$

其中$\alpha_2=\dfrac{\widehat{\alpha}_2\lambda_{\min}(P)}{\lambda_{\max}(P)}$.

3) 当$E(t)=0$时,DoS攻击危害系统拓扑中的每条信道,致使整个系统通信瘫痪. 由式(21),得到

$$\dot{V}(t)=\delta^{\mathrm{T}}(t)(I_N\otimes(PA+A^{\mathrm{T}}P))\delta(t).\tag{25}$$

当存在标量$\widehat{\alpha}_3$满足式(18)时,有

$$\dot{V}(t)\leqslant\alpha_3V(t),\tag{26}$$

其中$\alpha_3=\widehat{\alpha}_3$. □

注5　不同攻击模式下衰减率α_1、α_2以及α_3的选择应使得定理1中的式(16)～(18)对于所有$\zeta(t)\subseteq\mathcal{E}$均是可行的. 由于存在$2^{\frac{|\mathcal{E}|}{2}}$种不同的攻击模式,由$\zeta(t)\subseteq\mathcal{E}$求解式(16)～(18)会有$2^{\frac{|\mathcal{E}|}{2}}$种衰减率. 随着系统规模的扩大,计算量呈几何倍增. 为此,在计算时采取了适当的放缩方法, 根据系统在DoS攻击下连通度的不同,将所有攻击模式分为3类: 1)攻击少量信道,系统拓扑仍能够保持连通的DoS攻击模式; 2)攻击部分信道,系统拓扑分为几个连通分支的DoS攻击模式; 3)所有信道均被攻击,导致整个系统通信瘫痪的DoS攻击模式. 并分别求解这3种情况下的衰减率. 这种方式虽然存在一定的保守性,但是极大地简化了计算的复杂程度.

2.2　基于估计器的分布式控制器

设计基于估计器的分布式控制器,即

$$\begin{aligned}u_i(t)=c_1\Big\{&\sum_{j\in N_{S_i},(i,j)\notin\zeta(t)}a_{ij}(x_j(t)-x_i(t))-\\&\sum_{j\in N_{D_i},(i,j)\notin\zeta(t)}a_{ij}(x_j(t)+x_i(t))+\\&\sum_{j\in N_{S_i},(i,j)\in\zeta(t)}a_{ij}(\hat{x}_j^i(t)-x_i(t))-\\&\sum_{j\in N_{D_i},(i,j)\in\zeta(t)}a_{ij}(\hat{x}_j^i(t)+x_i(t))\Big\}+\\c_2\Big\{&\sum_{j\in N_{S_i},(i,j)\notin\zeta(t)}a_{ij}(v_j(t)-v_i(t))-\\&\sum_{j\in N_{D_i},(i,j)\notin\zeta(t)}a_{ij}(v_j(t)+v_i(t))+\\&\sum_{j\in N_{Si},(i,j)\in\zeta(t)}a_{ij}(\hat{v}_j^i(t)-v_i(t))-\\&\sum_{j\in N_{D_i},(i,j)\in\zeta(t)}a_{ij}(\hat{x}_j^i(t)+x_i(t))\Big\}.\end{aligned}\tag{27}$$

其中: $\hat{x}_j^i(t)$和$\hat{v}_j^i(t)$分别为在信道因DoS攻击瘫痪时智能体i对相邻智能体j位置和速度的估计值,其余参数均与式(8)中参数的含义一致.

注6　由于发生DoS攻击时最坏的情况是某些节点与其相邻节点完全中断信息交互,成为孤立节点. 设计估计器的目的是使得孤立节点的速度值可以在估计器的辅助下合理更新,不再是保持信道断开前最后一次通信得到的固定速度值,避免了信道瘫痪期间节点位置过度偏移. 当通信再次恢复时,整个系统不会因为某些节点位置过度偏移而加长收敛时间,从而实现加速系统收敛的目的. 值得说明的是,每条信道每次由正常通信转换为被攻击的状态时,其所涉及的估计器均会将上次DoS攻击期间的估计值舍弃,以估计器所对应的节点最后一次传输的状态值为初始估计值. 在本次DoS攻击期间开始迭代更新,并重新计算误差,由此避免了全局估计误差的累积.

当DoS攻击发生时,节点i的估计器的初始位置和速度分别为$\hat{x}_j^i(t_{d_0})=x_j(t_l)$和$\hat{v}_j^i(t_{d_0})=v_j(t_l)$, t_{d_0}和t_l分别为本次DoS攻击开始的时刻以及本次攻击发生前节点i与邻居节点j最后一次通信的时刻. 在此次DoS攻击期间位置估计值$\hat{x}_j^i(t)$和速度估计值$\hat{v}_j^i(t)$的更新规则如下:

$$\begin{cases}\dot{\hat{x}}_j^i(t)=\hat{v}_j^i(t),\\\dot{\hat{v}}_j^i(t)=\hat{u}_i(t).\end{cases}$$

$$\hat{u}_i(t)=\begin{cases}c_1(x_i(t)-\hat{x}_j^i(t))+c_2(v_i(t)-\hat{v}_j^i(t)),\ j\in N_i;\\ -c_1(x_i(t)+\hat{x}_j^i(t))-c_2(v_i(t)+\hat{v}_j^i(t)),\ j\notin N_i.\end{cases}\tag{28}$$

其中: c_1 和 c_2 分别为关于位置和速度的耦合强度, N_i 为节点 i 的邻居节点, $\hat{u}_i(t)$ 为控制输入. 与式(4)相似, 令节点 i 对邻居节点 j 的估计转换向量 $\hat{W}_j^i(t)=[\hat{x}_j^i(t),\hat{v}_j^i(t)]^{\mathrm{T}}$, 则相应的估计误差向量为

$$e_j^i(t)=\begin{cases}\hat{W}_j^i(t)-W_i(t),\ j\in N_i;\\ \hat{W}_j^i(t)+W_i(t),\ j\notin N_i.\end{cases}\tag{29}$$

节点 i 的估计误差向量为 $e^i=[e_1^i,e_2^i,\dots,e_N^i]^{\mathrm{T}}$, 系统的估计误差向量为 $e(t)=[e^1,e^2,\dots,e^N]^{\mathrm{T}}$. 将矩阵 $E_{\zeta(t)}$ 的主对角线元素全部替换为0, 并将其定义为矩阵 $A_{\zeta(t)}$. $A_{\zeta(t)}^i$ 表示矩阵 $A_{\zeta(t)}$ 的第 i 行, 则 $A_{\zeta(t)}=[A_{\zeta(t)}^1,A_{\zeta(t)}^2,\dots,A_{\zeta(t)}^N]^{\mathrm{T}}$. 由式(27), 可将式(5)中的 $(I_N\otimes B)u(t)$ 重写为

$$\begin{aligned}(I_N\otimes B)u(t)=&-((E-E_{\zeta(t)})\otimes BK)W(t)-\\&(O_{\zeta(t)}\otimes BK)e(t),\end{aligned}\tag{30}$$

其中 $O_{\zeta(t)}=\mathrm{diag}[A_{\zeta(t)},N]\in\boldsymbol{R}^{N\times N^2}$, 表示将矩阵 $A_{\zeta(t)}$ 以行为单位对角化. 则式(9)可重写为

$$\begin{aligned}\dot{W}(t)=&(I_N\otimes A-(E-E_{\zeta(t)})\otimes BK)W(t)-\\&(O_{\zeta(t)}\otimes BK)e(t).\end{aligned}\tag{31}$$

由式(30), 可将误差向量 $\delta(t)$ 的导数重写为

$$\begin{aligned}&\dot{\delta}(t)=(H\otimes I_n)\dot{W}(t)=\\&(H\otimes I_n)((I_N\otimes A-(E-E_{\zeta(t)})\otimes BK)W(t)-\\&(O_{\zeta(t)}\otimes BK)e(t))=\\&(I_N\otimes A-(E-E_{\zeta(t)})\otimes BK)\delta(t)-\\&(H_O\otimes BK)e(t).\end{aligned}\tag{32}$$

其中: I_n 为适当维度的单位阵, 矩阵 $H_O=H\times O_{\zeta(t)}$.

定理2 考虑含有 N 个节点连通无向图, 对于系统矩阵 A、输入矩阵 B 以及给定对称正定矩阵 Q 和 R, 存在正标量 $\breve{\alpha}_2>0$、标量 $\breve{\alpha}_3$ 以及对称正定矩阵 P, 使得

$$A^{\mathrm{T}}P+PA-PBR^{-1}B^{\mathrm{T}}P=-Q,\tag{33}$$

$$A^{\mathrm{T}}P+PA-\breve{\alpha}_2P<0,\tag{34}$$

$$A^{\mathrm{T}}P+PA-\breve{\alpha}_3P<0\tag{35}$$

成立, 则有如下不等式成立:

$$\dot{V}(t)\leqslant\alpha_{\zeta(t)}V(t)-\Phi(t).\tag{36}$$

其中: $V(t)=\delta^{\mathrm{T}}(t)(I_N\otimes P)\delta(t)$, $\Phi(t)=\dfrac{\kappa_0}{\rho}\displaystyle\sum_{i=1}^{N}e_i^{\mathrm{T}}e_i$, $\kappa_0=\|PBK\|$, $\eta=\lambda_{\max}^2$, $0<\rho<\dfrac{\lambda_{\min}(Q)}{\kappa_0\eta}$.

证明 由式(32), $V(t)$ 的导数可重写为

$$\begin{aligned}&\dot{V}(t)=\\&\dot{\delta}^{\mathrm{T}}(t)(I_N\otimes P)\delta(t)+\delta^{\mathrm{T}}(t)(I_N\otimes P)\dot{\delta}(t)=\\&\dot{V}_1(t)-\dot{V}_2(t).\end{aligned}\tag{37}$$

其中

$$\begin{aligned}\dot{V}_1(t)=&\delta^{\mathrm{T}}(t)(I_N\otimes(A^{\mathrm{T}}P+PA)-\\&2E(t)\otimes PBK)\delta(t),\\ \dot{V}_2(t)=&2\delta^{\mathrm{T}}(t)(H_O\otimes PBK)e(t).\end{aligned}$$

与第2.1节相似, 根据攻击模式的不同将分为以下3种情况讨论系统的衰减率.

1) 当 $\lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))\neq0$ 时, 意味着系统未遭受攻击或在DoS攻击下的系统拓扑仍是连通的. 对于 $\dot{V}_1(t)$, 当存在矩阵 P 满足式(33)时, 有

$$\begin{aligned}\dot{V}_1(t)\leqslant&\tilde{\delta}_{2:N}^{\mathrm{T}}(t)(I_{N-1}\otimes(A^{\mathrm{T}}P+PA-\\&PBR^{-1}B^{\mathrm{T}}P))\tilde{\delta}_{2:N}(t)\leqslant\\&-\lambda_{\min}(Q)\sum_{i=1}^{N}\tilde{\delta}_i^{\mathrm{T}}\tilde{\delta}_i.\end{aligned}\tag{38}$$

对于 $\dot{V}_2(t)$, 有

$$\begin{aligned}\dot{V}_2(t)=&2\delta^{\mathrm{T}}(t)(H_O\otimes PBK)e(t)\leqslant\\&2\|PBK\|\|H_O\|\|\delta^{\mathrm{T}}(t)\|\|e(t)\|.\end{aligned}\tag{39}$$

利用不等式 $ab\leqslant\dfrac{\rho}{2}a^2+\dfrac{1}{2\rho}b^2$, 得到

$$\begin{aligned}&\dot{V}_2(t)\leqslant\\&2\|PBK\|\sum_{i=1}^{N}\left(\lambda_{\max}^2(H_O)\frac{\rho}{2}\delta_i^{\mathrm{T}}\delta_i+\frac{1}{2\rho}e_i^{\mathrm{T}}e_i\right)\leqslant\\&\kappa_0\sum_{i=1}^{N}\left(\eta\rho\delta_i^{\mathrm{T}}\delta_i+\frac{1}{\rho}e_i^{\mathrm{T}}e_i\right).\end{aligned}\tag{40}$$

结合式(38)和(40), 式(37)可改写为

$$\begin{aligned}&\dot{V}(t)\leqslant\\&-\lambda_{\min}(Q)\sum_{i=1}^{N}\tilde{\delta}_i^{\mathrm{T}}\tilde{\delta}_i-\kappa_0\sum_{i=1}^{N}\left(\eta\rho\delta_i^{\mathrm{T}}\delta_i+\frac{1}{\rho}e_i^{\mathrm{T}}e_i\right)\leqslant\\&-(\lambda_{\min}(Q)+\kappa_0\eta\rho)\sum_{i=1}^{N}\tilde{\delta}_i^{\mathrm{T}}\tilde{\delta}_i-\frac{\kappa_0}{\rho}\sum_{i=1}^{N}e_i^{\mathrm{T}}e_i=\\&\alpha_1V(t)-\Phi(t),\end{aligned}\tag{41}$$

其中 $\alpha_1=-\dfrac{\lambda_{\min}(Q)+\kappa_0\eta\rho}{\lambda_{\max}(P)}$.

2) 当 $\lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))=0$ 时, 此时在DoS攻击下的系统拓扑是不连通的, 对于 $\dot{V}_1(t)$, 当存在正标量 $\breve{\alpha}_2$ 满足式(34)时, 有

$$\dot{V}_1(t)\leqslant\tilde{\delta}_{2:N}^{\mathrm{T}}(t)(I_{N-1}\otimes(A^{\mathrm{T}}P+PA))\tilde{\delta}_{2:N}(t)\leqslant$$

$$\breve{\alpha}_2\lambda_{\min}(P)\sum_{i=1}^{N}\tilde{\delta}_i^{\mathrm{T}}\tilde{\delta}_i. \tag{42}$$

由式(40)和(42),得到

$$\dot{V}(t)\leqslant\alpha_2V(t)-\Phi(t), \tag{43}$$

其中$\alpha_2=\dfrac{\breve{\alpha}_2\lambda_{\min}(P)-\kappa_0\eta\rho}{\lambda_{\max}(P)}$.

3) 当$E(t)=0$时,在DoS攻击下所有的信道均是瘫痪的,对于$\dot{V}_1(t)$,当存在标量$\breve{\alpha}_3$满足式(35)时,有

$$\dot{V}_1(t)=$$
$$\delta^{\mathrm{T}}(t)(I_N\otimes(PA+A^{\mathrm{T}}P))\delta(t)\leqslant\breve{\alpha}_3V(t). \tag{44}$$

由式(40)和(44),得到

$$\dot{V}(t)\leqslant\alpha_3V(t)-\Phi(t), \tag{45}$$

其中$\alpha_3=\breve{\alpha}_3-\dfrac{\kappa_0\eta\rho}{\lambda_{\max}(P)}$. □

根据是否含有估计器可得到$\dot{V}(t)$的两种表达形式

$$\begin{cases}\dot{V}(t)\leqslant\alpha_{\zeta(t)}V(t),\\ \dot{V}(t)\leqslant\alpha_{\zeta(t)}V(t)-\Phi(t).\end{cases} \tag{46}$$

其中: 式(46)第1式为不含有估计器的情况,第2式为含有估计器的情况. 衰减率$\alpha_{\zeta(t)}$包含以下3种情况:

$$\alpha_{\zeta(t)}=\begin{cases}\alpha_1,\ E(t)\neq0,\ \lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))\neq0;\\ \alpha_2,\ E(t)\neq0,\ \lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))=0;\\ \alpha_3,\ E(t)=0.\end{cases} \tag{47}$$

注 7　当节点与其所有邻居节点的通信均被DoS攻击中断时,该节点的估计器数量最大. 因此,当所有信道遭受DoS攻击时,系统中估计器的个数最大为$2|\mathcal{E}|$. 由于每个节点使用估计器的个数随着其被中断通信的邻居节点个数的增加而增加,相应的计算成本也会变得更大. 因此,对于规模过大的系统,控制器(27)不太适用.

3　稳定性分析

基于获得的衰减率$\alpha_{\zeta(t)}$,本节重点分析系统在DoS攻击下的稳定性问题.

定理3　基于假设1,多智能体系统(3)在控制器(27)作用下,若存在标量φ_{ij}^1、φ_{ij}^2以及函数$\Delta(\theta,t)$,使得

$$\omega=\sum_{(i,j)\in\mathcal{E}}(\varphi_{ij}^1\varpi_{ij}-\varphi_{ij}^2(1-\varpi_{ij}))<0, \tag{48}$$

$$\varphi_{ij}^1-\varphi_{ij}^2\geqslant0, \tag{49}$$

$$\alpha_{\zeta(t)}-\Big(\sum_{(i,j)\in\zeta(t)}\varphi_{ij}^1-\sum_{(i,j)\in\mathcal{E}\backslash\zeta(t)}\varphi_{ij}^2\Big)\leqslant0 \tag{50}$$

成立,则多智能体系统能够渐近实现安全分组一致.

证明　假设ϕ_k是DoS攻击从一种攻击模式转换为另一种模式的时刻,则对于$t\in[\varphi_k,\varphi_{k+1})$,由式(19)中$\dot{V}(t)\leqslant\alpha_{\zeta(t)}V(t)-\Phi(t)$,有

$$\mathrm{e}^{-\alpha_{\zeta(t)}t}\dot{V}(t)-\mathrm{e}^{-\alpha_{\zeta(t)}t}\alpha_{\zeta(t)}V(t)\leqslant-\mathrm{e}^{-\alpha_{\zeta(t)}t}\Phi(t). \tag{51}$$

经过推导可知

$$\begin{aligned}&V(t)\leqslant\mathrm{e}^{\alpha_{\zeta(t)}(t-\phi_k)}V(\phi_k)-\int_{\phi_k}^{t}\mathrm{e}^{\alpha_{\zeta(t)}(t-\theta)}\Phi(\theta)\mathrm{d}\theta\leqslant\\ &\mathrm{e}^{\Delta_k}V(\varphi_0)-\int_{\varphi_0}^{t}\mathrm{e}^{\Delta(\theta,t)}\Phi(\theta)\mathrm{d}\theta=\\ &\mathrm{e}^{\Delta(0,t)}V(0)-\int_0^t\mathrm{e}^{\Delta(\theta,t)}\Phi(\theta)\mathrm{d}\theta=F_1-F_2.\end{aligned} \tag{52}$$

其中

$$\Delta_k=\alpha_{\zeta(\phi_k)}(t-\phi_k)+\sum_{s=1}^{k}\alpha_{\zeta(\phi_{s-1})}(\phi_s-\phi_{s-1}),$$
$$\Delta(0,t)=\sum\nolimits_{\zeta(t)\in\mathcal{E}}\alpha_{\zeta(t)}\mathrm{len}(\Lambda_{ij}(0,t)),$$
$$F_1=\mathrm{e}^{\Delta(0,t)}V(0),$$
$$F_2=\int_0^t\mathrm{e}^{\Delta(\theta,t)}\Phi(\theta)\mathrm{d}\theta.$$

由式(50)和(1),得到

$$\begin{aligned}&\Delta(0,t)\leqslant\\ &\sum_{\zeta(t)\in\mathcal{E}}\Big(\sum_{(i,j)\in\zeta(t)}\varphi_{ij}^1+\sum_{(i,j)\in\mathcal{E}\backslash\zeta(t)}\varphi_{ij}^2\Big)\mathrm{len}(\Lambda_{ij}(0,t))=\\ &\sum_{(i,j)\in\mathcal{E}}\Big((\varphi_{ij}^1-\varphi_{ij}^2)\sum_{\zeta(t)\in\mathcal{E},(i,j)\in\zeta(t)}\mathrm{len}(\Lambda_{ij}(0,t))+\\ &\varphi_{ij}^2t\Big)\leqslant\omega t+\bar{\gamma},\end{aligned} \tag{53}$$

其中$\bar{\gamma}=\sum\limits_{(i,j)\in\mathcal{E}}(\varphi_{ij}^1-\varphi_{ij}^2)\gamma_{ij}$.

由式(53),对于F_1有$\lim\limits_{t\to\infty}F_1=0$. 由于DoS攻击是受限且非持续的,根据注5中估计器的更新特性,估计误差不是全局累积的,所以$e(t)$和$\Phi(t)$均是有界的. 有

$$\begin{aligned}F_2=\int_0^t\mathrm{e}^{\Delta(\theta,t)}\Phi(\theta)\mathrm{d}\theta\leqslant\\ \mathrm{e}^{\Delta(\theta_{\max},t)}\Phi(\theta_{\max})t\leqslant\\ \mathrm{e}^{\omega(t-\theta_{\max})+\bar{\gamma}}\Phi(\theta_{\max})t.\end{aligned} \tag{54}$$

其中: $\mathrm{e}^{\Delta(\theta_{\max},t)}\Phi(\theta_{\max})$为$\theta\in(0,t)$时$\mathrm{e}^{\Delta(\theta,t)}\Phi(\theta)$的最大值,$\bar{\gamma}=\sum\limits_{(i,j)\in\mathcal{E}}(\varphi_{ij}^1-\varphi_{ij}^2)\gamma_{ij}$. 由式(48)和(54),有$\lim\limits_{t\to\infty}F_2=0$,可得$\lim\limits_{t\to\infty}V(t)=\lim\limits_{t\to\infty}F_1-\lim\limits_{t\to\infty}F_2=0$,即

$$\lim_{t\to\infty}\|\delta(t)\|=0. \tag{55}$$

式(55)表明(6)和(7)是成立的(以上分析过程同样适用于式(46)中$\dot{V}(t)\leqslant\alpha_{\zeta(t)}V(t)$的情况),即在DoS攻击下多智能体系统实现了安全分组一致. □

注 8　虽然在第2节中给出了不同攻击模式下的衰减率,但是不同攻击模式所对应符号不同的

衰减率不利于稳定性分析. 为此在定理3中引入1组等价参数φ_{ij}^1和φ_{ij}^2, 其中φ_{ij}^1对应被攻击的信道$(i,j)\in\mathcal{E}$, φ_{ij}^2对应不被攻击的信道$(i,j)\in\mathcal{E}$.

4 数值仿真

考虑一个由5个智能体组成的多智能体系统,通信拓扑如图1所示. 其中节点v_1、v_2、v_3以及节点v_4、v_5分别隶属于两个分组. 不失一般性,随机选择各智能体的初始状态如下: $x(0)=[1,2,3,4,5]^{\mathrm{T}}$, $v(0)=[0.3,0.5,0.7,0.2,0.6]^{\mathrm{T}}$. 由图1可见,通信拓扑图共有6条边. 因此,攻击模式共存在$2^6=64$种,此处不再一一列出. 设定每条信道DoS攻击的攻击强度为$\varpi_{ij}=0.4, i,j=1,2,3,4,5, i\neq j$.

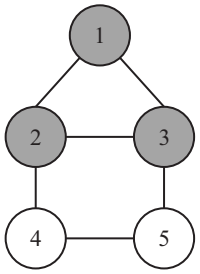


图1 系统通信拓扑图

仿真1 选择$R=0.5, Q=\begin{pmatrix}1.8 & 0.4\\ 0.4 & 5.64\end{pmatrix}$. 基于以上参数设定,可得到不同攻击条件下不同控制器的衰减率$\alpha_{\zeta(t)}$,结果如表1所示.

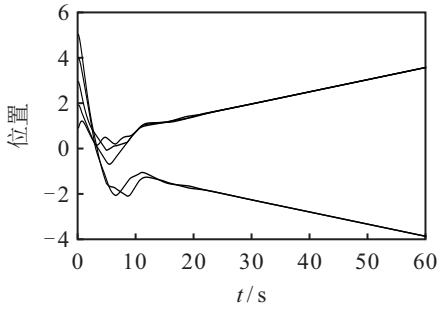
表1 不同控制器下的衰减率$\alpha_{\zeta(t)}$

$\alpha_{\zeta(t)}$	$\lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))\neq 0$	$\lambda_{\min}(\Omega^{\mathrm{T}}(t)E(t)\Omega(t))=0$	$E(t)=0$
控制器(8)	−0.46	0.54	1.4
控制器(27)	−0.7	0.3	1.17

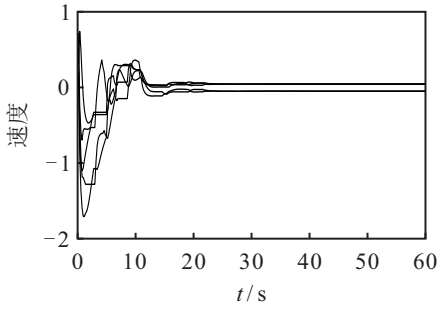
由表1可见,系统在同一控制器下的衰减率$\alpha_{\zeta(t)}$随着DoS攻击边数的增加而增加,这表明DoS攻击程度越大,通讯信息衰减越严重. 估计器在DoS攻击期间可以估计邻居节点的状态,这意味着即使所有的通信信道被攻击时,控制器(27)仍然可以保证各个节点的状态总是朝着最终一致状态更新. 然而,控制器(8)却将节点的速度值固定在某一个特定值上,因此,在理论上,基于控制器(27)的系统收敛得更快.

根据以上分析,选择参数$c_1=0.43, c_2=0.88$进行验证. 仿真结果如下.

图2(a)和图2(b)分别为控制器(8)下各个智能体

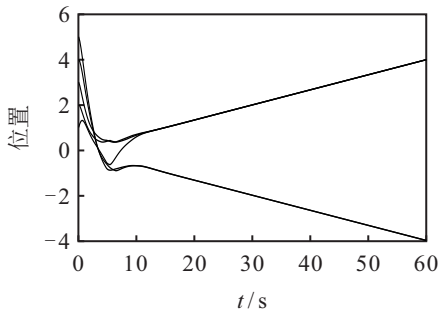


(a) 位置收敛

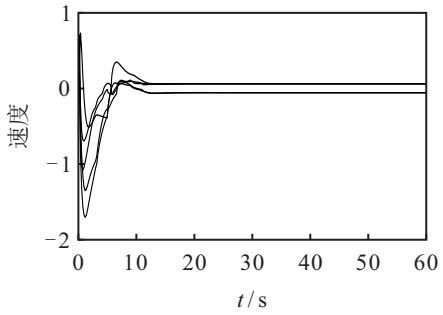


(b) 速度收敛

图2 基于控制器(8)的状态收敛



(a) 位置收敛



(b) 速度收敛

图3 基于控制器(27)的状态收敛

位置和速度的收敛图. 图3(a)和图3(b)分别为控制器(27)下各个智能体位置和速度的收敛图. 当系统实现安全分组一致时,图2中,控制器(8)的2组智能体的速度分别收敛至± 0.0449; 图3中,控制器(27)的2组智能体速度分别收敛至± 0.0609; 图2中,控制器(8)的2组智能体最终分别以± 0.0449的速度匀速运动,在46.92时间单位2组智能体位置分别到达± 2.5925; 图3中,控制器(27)下的2组智能体最终分别以± 0.0609的速度运动,在29.44时间单位2组智能体的位置分别到达± 1.7648. 通过对比,可以看出

含有控制器(27)的系统其状态收敛得更快.

仿真 2　对于同样的攻击强度,控制器(27)中估计器对系统收敛的加速效果应更具有一般性. 因此,仿真2引入文献[12]中不含估计器的控制器进行对比. 选择参数$c_1=1.0936, c_2=0.5199$进行实验, 仿真结果如下.

图4为在控制器(27)的作用下各个智能体的位置收敛图,图5为在文献[12]中不含估计器的控制器下位置的收敛图. 如图4和图5所示,控制器(27)在19.47时间单位使得2组智能体的位置分别达到± 5.36,文献[12]的控制器在46.15时间单位使得2组智能体的位置分别达到± 3.50. 通过对比,可以看出在攻击强度相同的情况下,控制器(27)中的估计器的确可以加速系统的收敛.

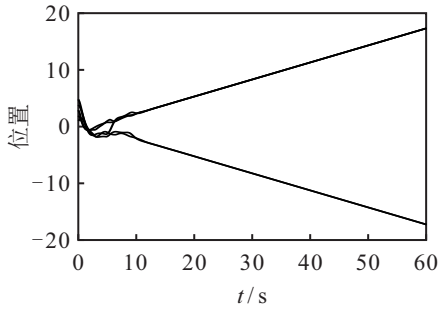


图 4　基于控制器(27)的位置收敛

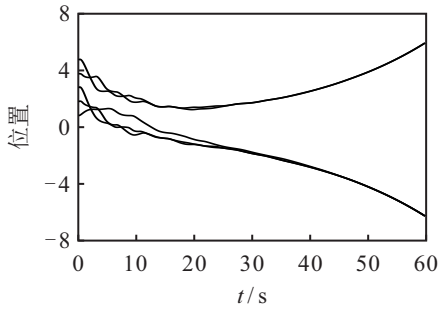


图 5　基于文献[12]中控制器的位置收敛

5　结　论

本文针对在DoS攻击下一类二阶多智能体系统安全分组一致性问题进行了研究. 对于更为灵活的多信道独立DoS攻击,设计了状态反馈控制器和基于估计器的控制器,通过求解代数黎卡提方程和线性矩阵不等式,得到不同攻击模式下不同控制器的衰减率. 然后基于得到的衰减率,通过引入1组等价参数降低了对系统稳定性分析的难度,并给出了系统稳定的条件. 实验结果表明,在所提出状态反馈控制器和基于估计器的控制器下,当满足DoS攻击持续时间的充分条件时,系统可渐近实现安全分组一致. 此外,通过实验结果发现,系统在基于估计器的控制器下的状态收敛速度更快,且更加稳定,从而验证了估计器加速系统收敛的有效性. 所提出控制器仅适用于同质系统和无向拓扑中. 因此,未来将考虑解决包含有向拓扑的异质多智能体系统在DoS攻击下的安全一致性问题.

参考文献(References)

[1] 侯健, 郑荣濠. 随机分组策略下的分布式多智能体一致性[J]. 控制理论与应用, 2018, 35(4): 517-522.
(Hou J, Zheng R H. Distributed multi-agent consensus via a novel randomized group partition approach[J]. Control Theory & Applications, 2018, 35(4): 517-522.)

[2] 丁俐夫, 颜钢锋. 多智能体系统安全性问题及防御机制综述[J]. 智能系统学报, 2020, 15(3): 425-434.
(Ding L F, Yan G F. A survey of the security issues and defense mechanisms of multi-agent systems[J]. CAAI Transactions on Intelligent Systems, 2020, 15(3): 425-434.)

[3] 王士贤, 李军毅, 张斌. 欺骗攻击环境下具有执行器故障的跳变耦合信息物理系统的同步控制[J]. 控制理论与应用, 2020, 37(4): 863-870.
(Wang S X, Li J Y, Zhang B. Synchronization control of jumping coupled cyber physical system with actuator failures under deception attacks[J]. Control Theory & Applications, 2020, 37(4): 863-870.)

[4] 李丽, 王夕娟. 拒绝服务攻击下领导-跟随多智能体系统的均方一致性研究[J]. 控制与决策, 2019, 34(11): 2317-2322.
(Li L, Wang X J. Mean Square consensus for leader-following multi-agent systems under denial-of-service attacks[J]. Control and Decision, 2019, 34(11): 2317-2322.)

[5] Cheng Z H, Yue D, Hu S L, et al. Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks[J]. Neurocomputing, 2020, 400: 458-466.

[6] Hu S L, Yue D, Xie X P, et al. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks[J]. IEEE Transactions on Cybernetics, 2019, 49(12): 4271-4281.

[7] Chen X L, Yuan P. Event-triggered generalized dissipative filtering for delayed neural networks under aperiodic DoS jamming attacks[J]. Neurocomputing, 2020, 400: 467-479.

[8] Feng Z, Hu G Q. Secure cooperative event-triggered control of linear multiagent systems under DoS attacks[J]. IEEE Transactions on Control Systems Technology, 2020, 28(3): 741-752.

[9] Chen X L, Wang Y G, Hu S L. Event-based robust stabilization of uncertain networked control systems under quantization and denial-of-service attacks[J].

Information Sciences, 2018, 459: 369-386.

[10] Xu Y, Fang M, Wu Z G, et al. Input-based event-triggering consensus of multiagent systems under denial-of-service attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 50(4): 1455-1464.

[11] Lu A Y, Yang G H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service[J]. IEEE Transactions on Automatic Control, 2018, 63(6): 1813-1820.

[12] Lu A Y, Yang G H. Distributed consensus control for multi-agent systems under denial-of-service[J]. Information Sciences, 2018, 439/440: 95-107.

[13] Lu A Y, Yang G H. Observer-based control for cyber-physical systems under denial-of-service with a decentralized event-triggered scheme[J]. IEEE Transactions on Cybernetics, 2020, 50(12): 4886-4895.

[14] Yang Y, Li Y F, Yue D. Event-trigger-based consensus secure control of linear multi-agent systems under DoS attacks over multiple transmission channels[J]. Science China Information Sciences, 2020, 63(5): 1-14.

[15] Yang H J, Ye D. Observer-based fixed-time secure tracking consensus for networked high-order multiagent systems against DoS attacks[J]. IEEE Transactions on Cybernetics, 2022, 52(4): 2018-2031.

[16] Sun Y C, Yang G H. Event-triggered distributed state estimation for multiagent systems under DoS attacks[J]. IEEE Transactions on Cybernetics, 2020, 4456: 1-10.

[17] Xu W Y, Hu G Q, Ho D W C, et al. Distributed secure cooperative control under denial-of-service attacks from multiple adversaries[J]. IEEE Transactions on Cybernetics, 2020, 50(8): 3458-3467.

[18] 田磊, 王蒙一, 赵启伦, 等. 拓扑切换的集群系统分布式分组时变编队跟踪控制[J]. 中国科学: 信息科学, 2020, 50(3): 408-423.
(Tian L, Wang M Y, Zhao Q L, et al. Distributed time-varying group formation tracking for cluster systems under switching topologies[J]. Scientia Sinica: Informationis, 2020, 50(3): 408-423.)

[19] Wang J N, Lanzon A, Petersen I R. Robust cooperative control of multiple heterogeneous Negative-Imaginary systems[J]. Automatica, 2015, 61: 64-72.

[20] Ji L H, Gao T, Liao X F. Couple-group consensus for cooperative-competitive heterogeneous multiagent systems: Hybrid adaptive and pinning methods[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51(9): 5367-5376.

[21] Zhai S D, Zheng W X. On survival of all agents in a network with cooperative and competitive interactions[J]. IEEE Transactions on Automatic Control, 2019, 64(9): 3853-3860.

[22] Ji L H, Zhang Y, Jiang Y L. Couple-group consensus: A class of delayed heterogeneous multiagent systems in competitive networks[J]. Complexity, 2018, 2018: 7386729.

[23] Li K, Ji L, Yang S, et al. Couple-group consensus of cooperative-competitive heterogeneous multiagent systems: A fully distributed event-triggered and pinning control method[J]. IEEE Transactions on Cybernetics, 2020: 33055047.

[24] Liu J, Li H Y, Ji J C, et al. Group-bipartite consensus in the networks with cooperative-competitive interactions[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(12): 3292-3296.

[25] Zhang H, Chen J, Wang Z P, et al. Distributed event-triggered control for cooperative output regulation of multiagent systems with an online estimation algorithm[J]. IEEE Transactions on Cybernetics, 2022, 52(3): 1911-1923.

[26] Feng F L, Xu Y R, Tang Z W. Research on the charge rate of railway value-guaranteed transportation based on competitive and cooperative relationships[J]. Advances in Mechanical Engineering, 2018, 10(1): 1687814017747691.

[27] Feng Z, Hu G Q. Distributed secure average consensus for linear multi-agent systems under DoS attacks[C]. American Control Conference. Piscataway: IEEE, 2017: 2261-2266.

作者简介

纪良浩 (1977–), 男, 教授, 博士生导师, 从事智能信息处理、复杂系统与复杂网络等研究, E-mail: jilh@cqupt.edu.cn;

邢子正 (1997–), 男, 硕士生, 从事多智能体系统、复杂网络的研究, E-mail: xingzz97@163.com;

杨莎莎 (1987–), 女, 副教授, 博士, 从事多智能体系统协同控制等研究, E-mail: yangss@cqupt.edu.cn;

肖云鹏 (1982–), 男, 教授, 博士, 从事社交网络、复杂网络等研究, E-mail: xiaoyp@cqupt.edu.cn;

李华青 (1987–), 男, 教授, 博士生导师, 从事复杂系统协同控制与优化等研究, E-mail: huaqingli@hotmail.com.

(责任编辑: 魏 冰)