引用格式:周孟卿,夏威. 弹性分布式参数估计算法研究进展[J]. 信息对抗技术,2024, 3(4):34-49. [ZHOU Mengqing, XIA Wei. Progress in the study of resilient distributed parameter estimation algorithms[J]. Information Countermeasure Technology, 2024, 3(4):34-49. (in Chinese)]

弹性分布式参数估计算法研究进展

周孟卿[1],夏　威[1,2*]

(1. 电子科技大学信息与通信工程学院,四川成都 611731;
2. 新疆大学计算机科学与技术学院(网络空间安全学院),新疆乌鲁木齐 830046)

摘　要　基于自适应网络的分布式参数估计近年来受到了日益广泛的关注。现有的分布式参数估计算法尽管在无攻击的安全网络中表现良好,但在遭受如虚假数据注入(false data injection,FDI)攻击的对抗网络中,由攻击者注入的虚假数据(也称恶意数据)会随着节点间的通信和协作在网络中扩散,导致算法估计性能的恶化。若算法不能从攻击中快速恢复估计性能(即算法对攻击不具有弹性),则可能导致严重的后果。为此,简要介绍了弹性分布式参数估计算法所解决的基本问题及基本算法原理;从 FDI 攻击检测和弹性参数估计策略 2 个方面,系统地总结了近年来弹性分布式参数估计算法的研究进展,并分析了其在遭受 FDI 攻击的对抗网络中的性能;最后,探讨了现有弹性分布式参数估计算法的发展趋势和未来潜在的研究方向。

关键词　弹性分布式参数估计;FDI 攻击;扩散最小均方;自适应网络;对抗网络

中图分类号　TP 212.9　　**文章编号**　2097-163X(2024)04-0034-16

文献标志码　A　　**DOI**　10.12399/j.issn.2097-163x.2024.04.003

Progress in the study of resilient distributed parameter estimation algorithms

ZHOU Mengqing[1], XIA Wei[1,2*]

(1. School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China; 2. School of Computer Science and Technology (School of Cyberspace Security), Xinjiang University, Urumqi 830046, China)

Abstract　Distributed parameter estimation based on adaptive networks has received increasing attention in recent years. Although existing distributed parameter estimation algorithms perform well in secure networks without attacks, in adversarial networks subjected to attacks such as false data injection (FDI), the false data (also known as malicious data) injected by attackers will spread throughout the network through node communication and collaboration, leading to a deterioration of the algorithm's estimation performance. If the algorithm cannot quickly recover its estimation performance from the attack (i.e., the algorithm is not resilient to the attack), it may lead to serious consequences. To this end, this paper first briefly introduced the basic problems and principles of resilient distributed parameter estimation algorithms; then, it systematically summarized the research progress of resilient distributed parameter estimation algorithms in recent years from two aspects: FDI attack detection and

收稿日期:2023-10-18　　**修回日期**:2024-04-13
通信作者:夏威,E-mail:wx@uestc.edu.cn
基金项目:国家自然科学基金资助项目(61871104)

elastic parameter estimation strategies, and analyzed their performance in adversarial networks subjected to FDI attacks; finally, it discussed the development trend and potential future research directions of the existing resilient distributed parameter estimation algorithms.

Keywords　resilient distributed parameter estimation; FDI attacks; diffusion least mean square; adaptive networks; adversarial networks

0　引言

随着传感器技术和无线通信技术的发展，基于自适应网络(adaptive networks)的分布式参数估计(distributed parameter estimation)受到了日益广泛的关注[1-3]。自适应网络由一组相互连接，且具有传感、计算和通信能力的智能体(agent)节点组成。这些节点独立观测、处理数据，并通过相互协作完成对未知参数向量的估计，而无须配备专门的数据处理中心。与经典的集中式策略不同，分布式策略可靠性更高，并具有良好的可扩展性[4-6]，已在无线传感器网络[7]、电力系统监控[8]以及无人机目标跟踪[9]等领域中得到广泛应用。与增量(incremental)[10-11]、共识(consensus)[12-13]等其他著名的分布式策略相比，扩散(diffusion)[4,6,14]策略通常表现更稳健，已被成功应用于解决参数估计[4]和目标跟踪[15-16]等问题。基于分布式扩散策略的扩散最小均方(diffusion least mean squares，DLMS)算法[4,17]已被证明在一定条件下具有均值和均方稳定性。此外，当节点间存在通信链路噪声[18]或通信时延[19]时，DLMS算法在一定条件下仍具有均值和均方稳定性。

上述 DLMS 算法主要关注节点估计单个参数向量的问题，即单任务估计问题。然而，在许多重要应用中，网络中的节点需协同估计多个未知参数向量，这一类的分布式估计问题被称为多任务估计问题。在多任务估计问题的自适应网络中，每个节点通常只估计多个未知参数中的一个；估计同一参数的节点的集合称之为簇，相互连接的簇之间估计的未知参数向量通常具有相似性。基于分布式扩散策略的多任务扩散最小均方(multitask diffusion least mean squares，M-DLMS)算法可较有效地解决多任务网络中的参数估计问题[20]。基于对 DLMS 算法在多任务网络中的性能分析，通过最小化估计误差来设置相邻节点的自适应组合权值，是提高多任务网络的参数估计性能的途径之一[21]。

假设网络环境是安全的(即假设不存在针对网络的敌对攻击(adversarial attacks)[22-23]是上述分布式参数估计算法的基本前提。在上述安全环境中和一定条件下，算法对未知参数向量的估计在统计意义下将收敛到真实值[4]。然而，在实际应用中，自适应网络通常部署在开放环境中，其智能体节点的传感和通信难免会受到外界干扰甚至遭受各种敌对的物理攻击[23]，此时的自适应网络通常被称为对抗网络(adversarial networks)[24]。在对抗网络中，因为节点遭受敌对攻击，分布式算法的性能将明显恶化[23,25]。例如，当网络遭受拜占庭攻击(Byzantine attacks)[26-27]时，受攻击节点可能被重新编程并发送被篡改的数据，以干扰节点间的正常通信，从而导致网络无法准确估计未知参数。而数据伪造攻击(data falsification attacks)[22]的攻击者则直接向节点发送伪造数据，以干扰节点的观测和通信数据。不过，利用残差测试[28-29]，节点能检测到上述 2 种典型的物理攻击。

此外，攻击者还可窃取节点数据，并借此向节点观测值注入符合特定模型的恶意数据[30-31]，以实施虚假数据注入(false data injection，FDI)攻击[28-31]。FDI 攻击是一种特殊的欺骗攻击(spoofing attacks)[25]，能绕过基于残差测试的经典检测方法[23-25,28-31]。因此，在遭受 FDI 攻击的对抗网络中，经典的分布式参数估计算法[4,17,20-21]无法检测是否遭受 FDI 攻击。而遭受攻击的节点使用 FDI 攻击者篡改的恶意观测值，完成局部自适应迭代，将得到恶意中间估计值(因遭受攻击而被篡改的中间估计值)。随着节点间的通信和协作，恶意中间估计值会在网络中扩散，导致网络整体估计性能的恶化。若算法对 FDI 攻击不具有弹性，即算法不能从攻击中快速恢复估计性能，则可能带来严重后果。例如，在电力系统中[31-32]，错误的状态估计引发的不适当操作，可能威胁电网安全；而对于协同作战的无人机集群[33-34]，不准确的甚至错误的估计结果可能对集群

行动带来灾难性的后果。因此，为了减小 FDI 攻击对算法估计性能的负面影响，研究能够从攻击中快速恢复的弹性分布式参数估计算法具有重要意义。

目前，弹性分布式参数估计算法的研究尚处于起步阶段。本文将系统地总结近年来对抗网络中针对 FDI 攻击的弹性分布式参数估计算法的研究进展，探讨现有算法的原理、性能差异以及适用条件，并展望未来的研究趋势，为相关领域的进一步研究提供参考。

1 弹性分布式参数估计基本原理

考虑一个由 N 个节点组成的自适应网络，其中每个节点具有探测感知、计算和通信的能力，如图 1 所示，其中，节点 $k=8$ 的邻域和度分别为 $N_k=\{5,11,17,k\}$ 和 $n_k=4$。若网络中的 2 个节点能够彼此通信，则称它们互为邻居节点[4-5]。通常假设每个节点是其自身的邻居节点。邻域 N_k 表示节点 k 的邻居节点集合(包括节点 k 自身)，度 $n_k=|N_k|$ 表示节点 k 的邻居数目，N_k^- 表示邻域 N_k 中不包含节点 k 自身的子集。

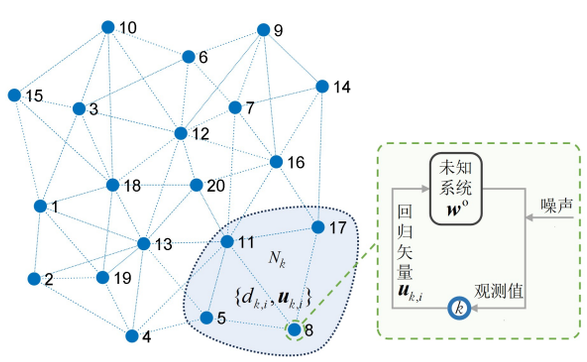


图 1 自适应网络的拓扑结构($N=20$)

Fig. 1 Topology of adaptive network($N=20$)

为了简化讨论，在本文所考虑的自适应网络中，各节点将协同估计单个未知参数向量 $\boldsymbol{w}^o\in\mathbf{R}^{M\times 1}$。例如，在电网状态估计中，$\boldsymbol{w}^o$ 表示网络中所有母线的电压和相位角[35]；而对于协同作战的无人机集群，$\boldsymbol{w}^o$ 可表示无人机集群质心的位置和速度[36]。在 i 时刻，每个节点 k 都可以探测感知一个实值时间广义平稳过程$\{d_{k,i},\boldsymbol{u}_{k,i}\}$，其中 $d_{k,i}$ 是标量观测值，$\boldsymbol{u}_{k,i}\in\mathbf{R}^{M\times 1}$ 是零均值，时间和空间独立的回归矢量，其协方差矩阵为 $\boldsymbol{R}_{u,k}\triangleq E\{\boldsymbol{u}_{k,i}\boldsymbol{u}_{k,i}^{\mathrm{T}}\}$。每个节点 k 的观测值 $d_{k,i}$ 和回归矢量 $\boldsymbol{u}_{k,i}$ 满足以下线性模型[1,4-5]：

$$d_{k,i}=\boldsymbol{u}_{k,i}^{\mathrm{T}}\boldsymbol{w}^o+v_{k,i} \tag{1}$$

式中，$(\cdot)^{\mathrm{T}}$ 表示矩阵或向量的转置，$v_{k,i}$ 表示均值为 0、方差为 $\sigma_{v,k}^2$，在时间和空间上独立同分布的高斯白噪声。不失一般性，假设在任意时刻 i，任意节点 k 处的噪声 $v_{k,i}$ 与任意节点 l 处在任意时刻 j 的回归矢量 $\boldsymbol{u}_{l,j}$ 无关，$k\neq l$。

1.1 安全网络中的扩散最小均方算法

在未遭受 FDI 攻击的安全网络中，DLMS 算法[4]能够以扩散分布式的形式估计未知参数向量。特别地，在基于自适应-组合(adapt-then-combine，ATC)扩散策略的 DLMS 算法中，各节点首先根据其观测值更新自身的中间估计值，再对其邻域内的中间估计值加权组合，实现估计值的更新。具体地，基于 ATC 扩散策略的 DLMS 算法可总结为：

$$\begin{cases}\boldsymbol{\varphi}_{k,i}=\boldsymbol{w}_{k,i-1}+\mu_k\sum\limits_{l\in N_k}a_{l,k}\boldsymbol{u}_{l,i}(d_{l,i}-\boldsymbol{u}_{l,i}^{\mathrm{T}}\boldsymbol{w}_{k,i-1})\\ \boldsymbol{w}_{k,i}=\sum\limits_{l\in N_k}c_{l,k}\boldsymbol{\varphi}_{l,i}\end{cases} \tag{2}$$

式中，$\mu_k>0$ 表示节点 k 处的步长参数，$\boldsymbol{w}_{k,i}$ 表示节点 k 在 i 时刻对 $\boldsymbol{w}^o$ 的估计，$\boldsymbol{\varphi}_{k,i}\in\mathbf{R}^{M\times 1}$ 表示中间估计值。非负实数 $a_{l,k}$ 和 $c_{l,k}$ 分别为组合系数矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{C}$ 第 l 行、第 k 列的元素，表示节点 l 在节点 k 处的组合权重(也称组合系数)，且满足[4]：

$$\begin{cases}\sum\limits_{l\in N_k}a_{l,k}=1,\text{若 } l\notin N_k,\text{则 } a_{l,k}=0\\ \sum\limits_{l\in N_k}c_{l,k}=1,\text{若 } l\notin N_k,\text{则 } c_{l,k}=0\end{cases} \tag{3}$$

式(2)分别对应基于 ATC 策略的 DLMS 算法的自适应步骤和组合步骤，若交换 2 个步骤的顺序，则可以推导得到组合-自适应(combine-then-adapt，CTA)扩散策略。本文主要关注基于 ATC 策略的 DLMS 算法，因为它通常比 CTA 策略估计性能更好[4]。

值得注意的是，当组合系数矩阵 $\boldsymbol{A}\neq\boldsymbol{I}$ 时($\boldsymbol{I}$ 表示单位矩阵)，邻居节点间交换所有向量 $\boldsymbol{u}_{l,i}$、$\boldsymbol{\varphi}_{l,i}$ 和标量 $d_{l,i}$；而当 $\boldsymbol{A}=\boldsymbol{I}$ 时，邻居节点间只交换向量 $\boldsymbol{\varphi}_{l,i}$。对于后者，一方面节省了交换 $\boldsymbol{u}_{l,i}$ 和 $d_{l,i}$ 所需的通信成本；另一方面，从安全角度考虑，交换较少的数据有助于提升算法的安全性[23]。因此，本文所讨论的弹性分布式参数估计算法，通常考虑 $\boldsymbol{A}=\boldsymbol{I}$ 的情况。此外，当 $\boldsymbol{A}=\boldsymbol{C}=\boldsymbol{I}$ 时，网络中邻居节点之间不交换任何数据，此时

DLMS 算法退化为无协作的 LMS（noncooperative LMS，NC-LMS）算法。

1.2　FDI 攻击模型

在安全网络环境中，DLMS 算法[4]能够实现对未知参数的精确估计。然而，在对抗网络中，由于缺乏攻击检测和防御机制，因此一旦节点遭受 FDI 攻击，DLMS 算法的估计性能将显著恶化。

FDI 攻击者入侵网络中的节点，窃取节点数据并借此篡改节点的观测，能够绕过基于经典的 ℓ_2 范数残差测试方法的攻击检测[30-32]。具体地，考虑受攻击节点集合 A_i，FDI 攻击者在节点 $k\in A_i$ 探测未知参数向量 $\boldsymbol{w}^{\mathrm{o}}$ 时，监听并窃取回归矢量 $\boldsymbol{u}_{k,i}$，并按照以下模型设计恶意观测数据[30-32]：

$$\rho_{k,i}=\boldsymbol{u}_{k,i}^{\mathrm{T}}\boldsymbol{w}_{k,i}^{\mathrm{a}} \tag{4}$$

式中，$\boldsymbol{w}_{k,i}^{\mathrm{a}}\in\mathbf{R}^{M\times 1}$ 是 i 时刻节点 k 处的注入误差向量（injected error vector）。通常假设 $\boldsymbol{w}_{k,i}^{\mathrm{a}}$ 服从高斯分布。随后，FDI 攻击者将恶意观测数据 $\rho_{k,i}$ 注入节点的观测值，以扰乱节点对未知参数向量的估计。图 2 给出了自适应网络中 FDI 攻击的示意图。在 i 时刻，每个受攻击节点 $k\in A_i$ 受到篡改后的观测值为：

$$d_{k,i}^{\mathrm{a}}=d_{k,i}+\rho_{k,i} \tag{5}$$

将式(1)和式(4)代入式(5)中，可得到受攻击节点 $k\in A_i$ 处被篡改的观测模型为：

$$d_{k,i}^{\mathrm{a}}=\boldsymbol{u}_{k,i}^{\mathrm{T}}(\boldsymbol{w}^{\mathrm{o}}+\boldsymbol{w}_{k,i}^{\mathrm{a}})+\upsilon_{k,i}=\boldsymbol{u}_{k,i}^{\mathrm{T}}\bar{\boldsymbol{w}}_{k,i}+\upsilon_{k,i} \tag{6}$$

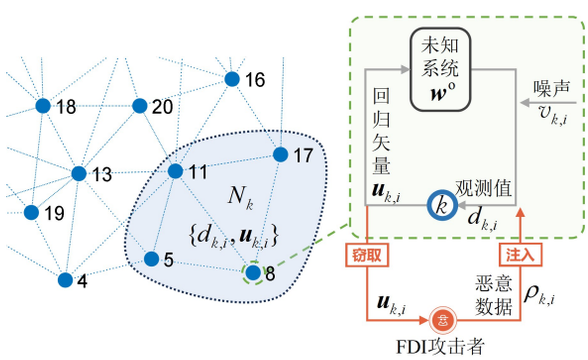


图 2　自适应网络中的 FDI 攻击示意图

Fig. 2　Illustration of FDI attacks in adaptive networks

显然，受攻击节点处被篡改的观测值 $d_{k,i}^{\mathrm{a}}$ 与未遭受 FDI 攻击的安全节点处的真实观测值 $d_{k,i}$ 差异明显。从 FDI 攻击者的角度来看，最有效的攻击是使受攻击节点处的观测产生严重偏离，从而使其对未知参数向量的估计偏离真实值 $\boldsymbol{w}^{\mathrm{o}}$，进而使得整个分布式网络的参数估计性能恶化。

值得注意的是，若使用基于残差的经典方法来检测节点 k 处数据是否遭受 FDI 攻击时，根据式(6)，可得到检测量[23,25]为：

$$\|d_{k,i}^{\mathrm{a}}-\boldsymbol{u}_{k,i}^{\mathrm{T}}\bar{\boldsymbol{w}}_{k,i}\|_2=\|d_{k,i}-\boldsymbol{u}_{k,i}^{\mathrm{T}}\boldsymbol{w}^{\mathrm{o}}\|_2 \tag{7}$$

式中，$\|\cdot\|_2$ 表示 ℓ_2 范数。显然，基于残差的检测方法无法检测到是否存在 FDI 攻击。于是，受攻击节点处的恶意中间估计值，将通过 DLMS 算法的扩散策略，随节点间的数据交互扩散到整个网络，从而导致未直接遭受攻击的节点估计性能恶化，以及网络整体估计性能的恶化。

为了简化表达，可将受攻击节点和安全节点的观测模型统一表示为：

$$d_{k,i}=\boldsymbol{u}_{k,i}^{\mathrm{T}}\bar{\boldsymbol{w}}_{k,i}+\upsilon_{k,i} \tag{8}$$

$$\bar{\boldsymbol{w}}_{k,i}=\begin{cases}\boldsymbol{w}^{\mathrm{o}}+\boldsymbol{w}_{k,i}^{\mathrm{a}}, & k\in A_i\\ \boldsymbol{w}^{\mathrm{o}}, & k\notin A_i\end{cases} \tag{9}$$

式中，当存在 FDI 攻击时，受攻击节点 $k\in A_i$ 处的注入误差向量 $\boldsymbol{w}_{k,i}^{\mathrm{a}}\neq 0$。

1.3　弹性分布式参数估计算法

在未遭受 FDI 攻击的安全环境中，在一定条件下，网络中各节点 k 对未知参数向量的估计是渐进无偏的，即满足[4]：

$$\lim_{i\to\infty}E\{\boldsymbol{w}_{k,i}\}=\boldsymbol{w}^{\mathrm{o}} \tag{10}$$

在对抗网络中，若节点能从攻击中快速恢复，且参数估计性能接近甚至达到在安全环境中的估计性能，则节点对 FDI 攻击具有弹性。类似地，在对抗网络中，若所有节点都对 FDI 攻击具有弹性，则该网络对 FDI 攻击具有弹性；相应地，在该网络所应用的分布式参数估计算法为弹性分布式参数估计算法。

值得注意的是，若网络中邻居节点之间不相互协作，即邻居节点不交换数据（如 NC-LMS 算法），则恶意中间估计值将无法在网络中传播扩散，攻击者也就无法破坏安全节点的估计结果。因此，采用无协作参数估计算法（如 NC-LMS 算法）的网络，尽管各节点无法通过与其邻居的数据分享和协作，提升网络整体的参数估计性能，但其对 FDI 攻击却具有弹性。本文所讨论的弹性分布式参数估计算法，即对 FDI 攻击具有弹性的分布式参数估计算法，在将遭受 FDI 攻击的情况下，通过邻居节点间的数据交换和协作，尽可能提升网络整体的估计性能。

从式(2)的结构可以看出，当 $\boldsymbol{A}=\boldsymbol{I}$ 时，采用 ATC 策略的 DLMS 算法共包含 3 个步骤：自适

应、通信以及组合。然而，为了能在遭受 FDI 攻击的对抗网络中实现对未知参数的估计，通常会避免直接组合邻域内的中间估计值，以免使用恶意中间估计值。因此，在组合之前，各节点通常基于邻域内数据进行攻击检测，以判断自身是否遭受 FDI 攻击；并进一步采取包括组合系数优化在内的弹性参数估计策略，以抑制恶意中间估计值扩散，并完成组合，从而实现对未知参数的弹性分布式估计。弹性分布式参数估计算法的典型过程如图 3 所示。

值得注意的是，除了图 3 所示的弹性分布式参数估计算法典型过程外，不同算法可能还包含其他步骤[25,37-38]。此外，从系统的角度来看，弹性分布式参数估计算法既可以 DLMS 算法作为主体，也可能是由 NC-LMS 算法子系统和 DLMS 算法子系统构成的混合系统[23,37,39-40]。NC-LMS 子系统完成攻击检测，而 DLMS 子系统实现分布式参数估计。

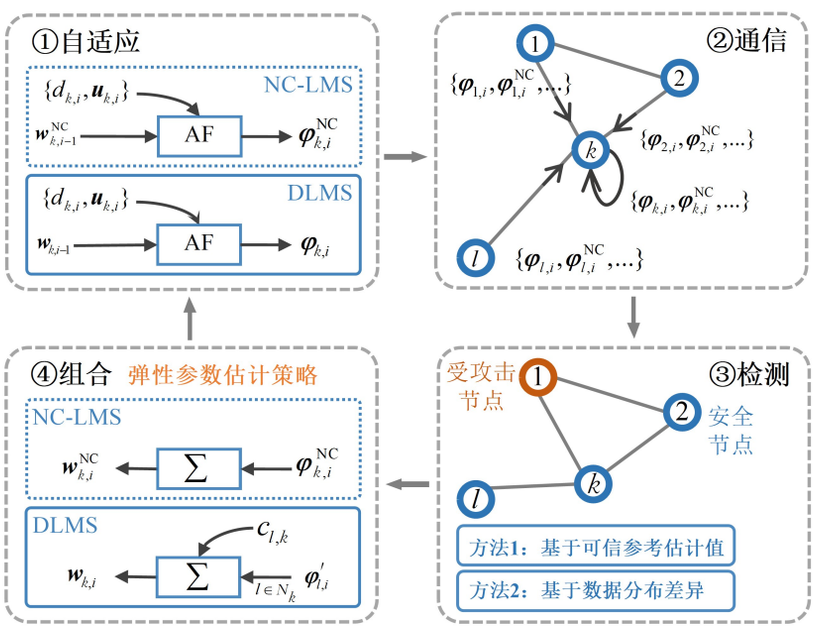


图 3 弹性分布式参数估计算法示意图

Fig. 3 Illustration of resilient distributed parameter estimation algorithms

为了实现对抗网络中对未知参数的弹性估计，不失一般性，现有文献对自适应网络、网络中各节点邻域内受攻击节点的数目以及 FDI 攻击者，通常有如下假设[23-25,37-41]。

假设 1 由 FDI 攻击者决定是否发起攻击，网络无法预知在何时何处会遭受攻击[25]。

假设 2 网络中受攻击节点的数目比网络节点总数少[41]。

假设 3 网络中受攻击节点的数目远小于网络节点总数，且至少存在 1 个节点，其邻域内所有节点都是安全的[24]。

假设 4 在 i 时刻，对于网络中的每个节点 k，其邻域内受攻击节点的数目不超过其节点的度（即节点邻居数目）的 $1/2$[23,25,37-40]。

假设 5 在 i 时刻，对于网络中的每个节点 k，其邻域内受攻击节点的数目不超过其节点的度[24]。

假设 6 FDI 攻击者无法获取自适应网络的任何先验信息，故只能对网络进行无差别攻击[40]。

假设 7 FDI 攻击者无法获取关于未知参数向量 $\boldsymbol{w}^{\circ}$ 的全部信息，故无法构造对网络最具危害的注入误差向量[23-25,39]。

其中，针对网络的假设 1、假设 2、假设 3 以及针对各节点邻域内受攻击节点的数目的假设 4、假设 5，其合理性源于自适应网络通常具备物理保护机制，且 FDI 攻击者对网络的攻击是有代价的[37-38,40]，因此 FDI 攻击者仅能对网络中有限数目的节点发起攻击。值得注意的是，如果某些度较小的节点的多数邻居节点遭受 FDI 攻击，那么基于假设 4 构造的弹性分布式参数估计算法可能会失效。此外，FDI 攻击者无法基于分布式参数估计短暂的暂态过程准确推断未知参数，且无法直接获取自适应网络的先验信息[23]，因此针对

FDI 攻击者的假设 6 和假设 7 也有其合理性。

基于上述不同假设，下文将从 FDI 攻击检测方法与弹性参数估计策略 2 方面，系统地总结近年来弹性分布式参数估计算法的研究进展。

2　算法研究进展

近年来，将 FDI 攻击检测与抑制恶意中间估计值扩散相结合的弹性分布式参数估计策略已被证明是应对 FDI 攻击的可行方法之一。为了在对抗网络环境中实现对未知参数的弹性估计，网络中的各节点需要在判断自身是否遭受 FDI 攻击的基础上，采取弹性估计策略以抑制恶意中间估计值的扩散。

2.1　FDI 攻击检测的方法

对抗网络中现有的 FDI 攻击检测方法通常可分为基于可信参考估计值的检测方法和基于数据分布差异的检测方法。其中，前一类方法[23,37,41-42]利用邻域内中间估计值确定可信赖的参考估计值，并通过比较各节点中间估计值与参考估计值之间差异程度，实现对 FDI 攻击的检测；而后一类方法[24-25,38-40]通常包括节点划分与节点状态感知 2 个步骤，即各节点首先利用观测值或中间估计值的分布差异将邻域划分为 2 个集合，再通过感知节点的受攻击状态来实现 FDI 攻击检测。

2.1.1　基于可信参考估计值的检测方法

网络中各节点可利用其邻域内的中间估计值，确定可信赖的参考估计值。基于这一可信参考估计值，可检测邻域内的节点是否遭受 FDI 攻击。

基于假设 2 和信誉机制的分布式扩散最小均方(reputation-based DLMS，R-DLMS)算法[41]可实现对未知参数向量的弹性估计。在该算法中，每个节点 k 将其邻域内的第 i 时刻的中间估计(向量)中的每一个元素按升序排列，得到已排序的序列 $\Phi_{k,i}^{(m)}$，其中，$m=1,2,\cdots,M$。FDI 攻击将使受攻击节点对未知参数向量的估计偏离其真实值。因此，若 N_k 内有节点遭受 FDI 攻击，则受到恶意数据影响的估计量出现在序列 $\Phi_{k,i}^{(m)}$ 左右两端的概率较大，而出现在序列 $\Phi_{k,i}^{(m)}$ 中间的概率较小。R-DLMS 算法将序列 $\Phi_{k,i}^{(m)}$ 中间$\lceil n_k/2 \rceil$个数据的均值视为可信参考估计值 $\bar{\boldsymbol{\varphi}}_{k,i}^{\mathrm{ref}}$，$\lceil\cdot\rceil$表示向上取整。进一步地，节点 k 依据邻居节点中间估计值 $\boldsymbol{\varphi}_{l,i}$ 与此参考估计值之间欧氏距离的平方 $\|\boldsymbol{\varphi}_{l,i}-\bar{\boldsymbol{\varphi}}_{k,i}^{\mathrm{ref}}\|_2^2$ 的大小来判断邻居节点是否遭受攻击：$\|\boldsymbol{\varphi}_{l,i}-\bar{\boldsymbol{\varphi}}_{k,i}^{\mathrm{ref}}\|_2^2$ 越大，则节点遭受 FDI 攻击的可能性越大。值得注意的是，R-DLMS 算法[41]并不区分受攻击节点和安全节点。此外，恶意中间估计值会随着节点之间数据的交互在网络中扩散，影响安全节点的估计，而参考估计值可能不再可靠，进而影响算法的参数估计性能。

由 NC-LMS 子系统和 DLMS 子系统组成的混合结构是基于可信参考估计值检测方法的弹性分布式参数估计算法的典型构造方式[23,37,42]。NC-LMS 算法子系统实现攻击检测；DLMS 算法子系统实现分布式参数估计。因为不同节点间的 NC-LMS 子系统相互独立，受攻击节点处的恶意中间估计值无法在节点间的 NC-LMS 子系统中扩散，各节点能够基于邻域内节点 NC-LMS 子系统的无协作中间估计值获得可信参考估计值。而在 DLMS 子系统中，恶意中间估计值仍会随节点间的数据交互在网络中扩散，导致安全节点处的估计值不再可信。

基于上述混合系统结构，安全扩散最小均方(secure DLMS，S-DLMS)算法[23]可持续获得可信的参考估计。具体地，在 i 时刻，每个节点 k 将其邻域内的 NC-LMS 子系统的无协作中间估计值(向量)中的每一个元素按升序排序，得到已排序的序列 $\Phi_{k,i}^{\mathrm{NC}(m)}$。与 R-DLMS 算法不同，在假设 4 的条件下，S-DLMS 将选取序列 $\Phi_{k,i}^{\mathrm{NC}(m)}$ 的第$\lceil n_k/2 \rceil$项估计作为可信参考估计值。此外，可以证明，在假设 4 的前提下，当 FDI 攻击的强度较弱，以至于序列 $\Phi_{k,i}^{\mathrm{NC}(m)}$ 的第$\lceil n_k/2 \rceil$项对应的节点恰为受攻击节点时，该估计值仍是真实未知参数向量 $\boldsymbol{w}^{\circ}$ 的无偏估计[23]。

对于邻域 N_k 内的安全节点 l，其 NC-LMS 子系统的无协作中间估计值 $\boldsymbol{\varphi}_{l,i}^{\mathrm{NC}}$ 和 DLMS 子系统的中间估计值 $\boldsymbol{\varphi}_{l,i}$ 都应该近似于节点 k 处的可信参考估计值。于是，通过评估接收到的邻居节点的估计值$\{\boldsymbol{\varphi}_{l,i}^{\mathrm{NC}},\boldsymbol{\varphi}_{l,i}\}$和可信参考估计值 $\boldsymbol{\varphi}_{k,i}^{\mathrm{ref}}$ 各个元素之间的差异，节点 k 可通过下述二元假设检验，判断其邻居节点是否遭受 FDI 攻击：

$$\max\Big(\max(\|\boldsymbol{\varphi}_{l,i}^{\mathrm{NC}(m)}-\boldsymbol{\varphi}_{k,i}^{\mathrm{ref}(m)}\|_2),\ \max(\|\boldsymbol{\varphi}_{l,i}^{(m)}-\boldsymbol{\varphi}_{k,i}^{\mathrm{ref}(m)}\|_2)\Big)^2 \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \theta_{k,i},\ l\in N_k \tag{11}$$

式中，$\boldsymbol{\varphi}_{k,i}^{\mathrm{ref}(m)}$ 和 $\boldsymbol{\varphi}_{l,i}^{(m)}$ 分别表示 i 时刻节点 k 处可信参考估计值(向量)$\boldsymbol{\varphi}_{k,i}^{\mathrm{ref}}\in\mathbf{R}^{M\times 1}$ 中的第 m 个元

素和节点 $l\in N_k$ 的 DLMS 子系统中间估计值(向量)$\boldsymbol{\varphi}_{l,i}\in\mathbf{R}^{M\times 1}$ 中的第 m 个元素,$m=1,2,\cdots,M$。门限 $\theta_{k,i}$ 根据可信参考估计值自适应地确定。

同样在假设 4 的条件下,基于校正机制的安全 DLMS(correction-based secure DLMS,CS-DLMS)算法[42]在 DLMS 算法的自适应和组合步骤之间引入校正(correction)步骤,以提高算法的稳态估计性能。在假设 4 以及不同簇之间估计参数相似性已知的额外假设条件下,安全多任务 DLMS(safe multi-task DLMS,SM-DLMS)算法[37]可有效地检测到多任务网络中遭受 FDI 攻击的节点。该算法对于可信参考估计值的确定方法与 S-DLMS 算法[23]类似,但需要利用未知参数向量的部分先验信息初始化自适应门限。

2.1.2 基于数据分布差异的检测方法

在遭受 FDI 攻击的对抗网络中,恶意数据的注入会导致受攻击节点与安全节点观测值之间存在显著差异。进一步地,利用恶意观测值,受攻击节点局部自适应迭代得到的中间估计值(恶意中间估计值),将与安全节点处的中间估计值存在较大差异。因此,在对抗网络中,可以基于节点间观测值或中间估计值的分布差异,检测节点是否遭受 FDI 攻击。与基于可信参考估计值的检测方法不同,基于数据分布差异的检测方法通常包含节点划分与状态感知 2 个步骤。

2.1.2.1 节点划分

在 i 时刻,每个节点 k 将首先根据自身与邻居节点之间观测值的分布差异或中间估计值的分布差异,将邻域内与自身差异较小的邻居节点划分至集合 $S_{k,i}^{\mathrm{S}}$,而将剩余的与自身差异较大的邻居节点划分至集合 $S_{k,i}^{\mathrm{D}}$。不失一般性,属于同一集合的节点状态是一致的,即要么都是安全的,要么均遭受 FDI 攻击。本小节将概述现有文献中基于数据分布差异的 FDI 攻击检测方法中的节点划分方法的研究进展。

1) 基于 KL 散度的节点划分方法。KL 散度(Kullback-Leibler divergence,KLD)也称相对熵(relative entropy),可衡量 2 个概率分布之间的差异程度。KL 散度越大,2 个概率分布之间的差异也就越大;反之,则差异越小。基于 KL 散度的 DLMS(DLMS with KLD,DLMSKL)算法[25]使用 KL 散度衡量节点间观测值的差异,并据此将每个节点 k 的邻域划分为 $S_{k,i}^{\mathrm{S}}$ 和 $S_{k,i}^{\mathrm{D}}$ 2 个集合。

在 DLMSKL 算法中,在 i 时刻,每个节点 k 将构造一个历史观测值集合,其中存储了 L 个连续时刻的历史观测值。随后,每个节点 k 基于直方图方法来近似历史观测值的概率密度函数[43],从而得到与其邻居观测值分布之间的 KL 散度的估计 $\hat{D}_i(k\parallel l)$[25]。得到与所有邻居节点 $l\in N_k^-$ 观测值分布之间的 KL 散度估计后,每个节点 k 将其邻域内的 KL 散度估计按降序排序,得到已排序的序列 $Q_{k,i}^{\mathrm{KL}}$。

由于受攻击节点与安全节点的观测值之间通常存在较大差异,故相应的 KL 散度也相对较大;而不同安全节点的观测数据之间的 KL 散度则相对较小。用 $V_{k,i}^{\mathrm{KL}}(\beta)$ 表示 $Q_{k,i}^{\mathrm{KL}}$ 剔除前 $\beta-1$ 个邻居节点的 KL 散度估计后,剩余 $n_k-\beta$ 个 KL 散度估计 $\hat{D}_i(k\parallel l_{(\beta)}),\cdots,\hat{D}_i(k\parallel l_{(n_k-1)})$ 的方差,其中,$\beta=1,2,\cdots,n_k-2$。在 i 时刻,每个节点 k 构建下述二元假设检验:

$$\frac{V_{k,i}^{\mathrm{KL}}(\beta)}{V_{k,i}^{\mathrm{KL}}(\beta+1)}\underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}}\theta_{k,i},\ \beta=1,2,\cdots,n_k-3 \tag{12}$$

式中,$\theta_{k,i}$ 表示门限。随着 β 值的增加,若存在 β 使得假设 H_1 为真,则节点 k 认为前 β 个邻居节点的观测值与其自身观测值的分布差异较大。于是,节点 k 将其邻域划分为集合 $S_{k,i}^{\mathrm{D}}=\{l_{(1)},\cdots,l_{(\beta)}\}$ 和 $S_{k,i}^{\mathrm{S}}=\{l_{(\beta+1)},\cdots,l_{(n_k-1)}\}$。若所有 β 都使得假设 H_0 为真,则节点 k 认为所有邻居节点的观测值与其自身观测值的分布差异较小,并将其邻域划分为集合 $S_{k,i}^{\mathrm{D}}=\varnothing$ 和 $S_{k,i}^{\mathrm{S}}=\{l_{(1)},\cdots,l_{(n_k-1)}\}$。

2) 基于相关熵的节点划分方法。相关熵(correntropy)是一种基于高斯核(Gaussian kernel)函数的非线性度量,同样能够评价 2 个随机变量之间的差异程度[44]。利用相关熵的性质,基于相关熵的节点划分和状态感知(correntropy-based state perception,CSP)算法[24]可有效地检测并识别对抗网络中遭受 FDI 攻击的节点。

在实际应用中,可利用观测值的多个样本估计相关熵 $\hat{v}_i(k,l)$[44]。与 DLMSKL 算法[25]不同,在 i 时刻,每个节点 k 将其与邻居节点 l 之间的相关熵估计按升序排序,得到已排序的序列 $Q_{k,i}^{\mathrm{C}}$。

类似地,用 $V_{k,i}^{\mathrm{C}}(\beta)$ 表示 $Q_{k,i}^{\mathrm{C}}$ 剔除前 $\beta-1$ 个邻居节点的相关熵估计后,剩余 $n_k-\beta$ 个相关熵估计 $\hat{v}_i(k,l_{(\beta)}),\cdots,\hat{v}_i(k,l_{(n_k-1)})$ 的方差,$\beta=1,2,\cdots,n_k-2$,其计算方法与 $V_{k,i}^{\mathrm{KL}}(\beta)$ 类似。随后,每个节点 k 构建类似式(12)的二元假设检验,将

其邻域划分为 $S_{k,i}^{\mathrm{S}}$ 和 $S_{k,i}^{\mathrm{D}}$ 2 个集合。与 DLMSKL 算法[25]不同，若存在 β 使得假设 H_0 为真，则前 β 个节点被划分至集合 $S_{k,i}^{\mathrm{S}}=\{l_{(1)},\cdots,l_{(\beta)}\}$ 且 $S_{k,i}^{\mathrm{D}}=\varnothing$。逐步增大 β，直到使得假设 H_1 为真或 $\beta=n_k-3$。当假设 H_1 为真时，节点 k 的邻域被划分为集合 $S_{k,i}^{\mathrm{S}}=\{l_{(1)},\cdots,l_{(\beta)}\}$ 和 $S_{k,i}^{\mathrm{D}}=\{l_{(\beta+1)},\cdots,l_{(n_k-1)}\}$。否则，当 $\beta=n_k-3$ 时，节点 k 的所有邻居节点都划分至集合 $S_{k,i}^{\mathrm{S}}$，且集合 $S_{k,i}^{\mathrm{D}}=\varnothing$。

3）基于交叉检验的节点划分方法。与上述 2 种基于观测值分布差异的节点划分方法[24-25]不同，在经典的 ℓ_2 范数残差测试方法的基础上，具有交叉检验（cross-verification，CV）机制的 DLMS（DLMS with cross-verification，DLMS-CV）算法[39]利用节点观测值与邻居节点无协作中间估计值之间的相关性，将 CV 机制与自适应门限相结合，以将各节点的邻域内划分为集合 $S_{k,i}^{\mathrm{S}}$ 和 $S_{k,i}^{\mathrm{D}}$。

DLMS-CV 算法基于混合系统结构，借助节点间 NC-LMS 子系统的无协作中间估计值来检测 FDI 攻击。具体地，由于每个节点 k 的观测值 $d_{k,i}$ 和回归矢量 $\boldsymbol{u}_{k,i}$ 满足观测模型式（8），而 NC-LMS 子系统的无协作中间估计值 $\boldsymbol{\varphi}_{k,i}^{\mathrm{NC}}$ 是对 $\bar{\boldsymbol{w}}_{k,i}$ 的估计，因此，每个节点 k 的观测值 $d_{k,i}$ 和无协作中间估计值 $\boldsymbol{\varphi}_{k,i}^{\mathrm{NC}}$ 之间通常具有一定的相关性。考虑到不同的安全节点间（或不同的受攻击节点间）的中间估计值差异较小，而受攻击节点与安全节点间的中间估计值差异较大。因此，节点 k 可利用自身观测值和邻居节点 l 的 NC-LMS 子系统无协作中间估计值 $\boldsymbol{\varphi}_{l,i}^{\mathrm{NC}}$ 之间的相关性，构建以下基于 CV 机制的二元假设检验：

$$\| d_{k,i}-\boldsymbol{u}_{k,i}^{\mathrm{T}}\boldsymbol{\varphi}_{l,i}^{\mathrm{NC}}\|_2 \underset{\mathrm{H}_0}{\overset{\mathrm{H}_1}{\gtrless}} \theta_{k,i},\ l\in N_k \tag{13}$$

式中，$\theta_{k,i}$ 表示由回归矢量和观测噪声共同确定的自适应门限。值得注意的是，无论节点 k 自身是否遭受 FDI 攻击，假设 H_0 均为真。

进一步地，每个节点 k 使用信任参数 $t_i(l,k)=\lambda t_{i-1}(l,k)+(1-\lambda)b_i(l,k)$ 判断邻居节点 l 与节点 k 在 i 时刻中间估计值之间的差异大小，$\lambda\in(0,1]$ 表示遗忘因子；$b_i(l,k)$ 表示二元假设检验（13）的结果：若 H_0 为真，则 $b_i(l,k)=1$，反之则 $b_i(l,k)=0$。信任参数 $t_i(l,k)$ 越大，表示节点 l 与节点 k 的状态越相似。对于邻居节点 l，当 $t_i(l,k)$ 超过预设门限 $\xi\in(0,1)$ 时，节点 k 认为其状态与自身一致并将其划分至集合 $S_{k,i}^{\mathrm{S}}$，其他信任参数未达到门限 ξ 的节点则被划分至集合 $S_{k,i}^{\mathrm{D}}$。

4）基于局部离群因子的节点划分方法。局部离群因子（local outlier factor，LOF）策略[45]通过给数据集中的每个数据分配一个由邻域密度决定的数值，即 LOF，以反映每个数据的异常程度。在不同簇之间估计参数的相似性已知的额外假设条件下，基于邻域内 LOF 的节点划分方法[41]可将多任务网络中每个节点 k 的邻域划分为 $S_{k,i}^{\mathrm{S}}$ 和 $S_{k,i}^{\mathrm{D}}$ 2 个集合。其中，每个节点 k 分别计算其邻居节点经过伪移位（pseudo moving position）操作[41]后的中间估计值的 LOF。节点的 LOF 越大，代表其遭受 FDI 攻击的概率越大。基于邻域内的 LOF，每个节点 k 构建二元假设检验将邻域划分为集合 $S_{k,i}^{\mathrm{S}}$ 和 $S_{k,i}^{\mathrm{D}}$：

$$\begin{cases} l\in S_{k,i}^{\mathrm{S}}, & \text{若 } \mathrm{lof}_m(\boldsymbol{\varphi}_{l,i}^{\mathrm{p}})\leqslant\theta_{k,i} \\ l\in S_{k,i}^{\mathrm{D}}, & \text{若 } \mathrm{lof}_m(\boldsymbol{\varphi}_{l,i}^{\mathrm{p}})>\theta_{k,i} \end{cases} \tag{14}$$

式中，$\boldsymbol{\varphi}_{l,i}^{\mathrm{p}}$ 表示 i 时刻邻居节点 $l\in N_k$ 经过伪移位操作后的中间估计值，$m=\lfloor n_k/2\rfloor$，$\lfloor\cdot\rfloor$ 表示向下取整，$\mathrm{lof}_m(\boldsymbol{\varphi}_{l,i}^{\mathrm{p}})$ 表示 $\boldsymbol{\varphi}_{l,i}^{\mathrm{p}}$ 的 LOF（文献[41]给出了其计算方法），门限 $\theta_{k,i}$ 由 K-median 聚类方法[46]确定。

2.1.2.2　状态感知

当网络中每个节点 k 将其邻域划分为 $S_{k,i}^{\mathrm{S}}$ 和 $S_{k,i}^{\mathrm{D}}$ 2 个集合后，还需进一步感知自身状态，以判断自身是否遭受 FDI 攻击。

1）基于邻域内受攻击节点数目的状态感知方法。基于数据分布差异的 FDI 攻击检测方法通常是在假设 4 这一关键假设条件下，即在 i 时刻，对于网络中的每个节点 k，其邻域内受攻击节点的数目不超过其节点度的 1/2[25,38-39]。

具体地，在 i 时刻，对于每个节点 k，与其状态一致的邻居节点集合 $S_{k,i}^{\mathrm{S}}$ 中的节点数 n_k^{S} 共有 3 种可能的情况。第 1 种情况：$n_k^{\mathrm{S}}=n_k$，此时节点 k 的所有邻居都与其状态一致，这意味着邻域 N_k 内所有节点都是安全的。第 2 种情况：$(n_k/2)\leqslant n_k^{\mathrm{S}}<n_k$，超过半数的邻居节点的状态与节点 k 一致，这意味着节点 k 以及集合 $S_{k,i}^{\mathrm{S}}$ 中的节点都是安全的，而集合 $S_{k,i}^{\mathrm{D}}$ 中的节点遭受 FDI 攻击。第 3 种情况：$n_k^{\mathrm{S}}<(n_k/2)$，意味着集合 $S_{k,i}^{\mathrm{S}}$ 中的节点均为受攻击节点，而集合 $S_{k,i}^{\mathrm{D}}$ 中的节点是安全的。

2）基于多数投票机制的状态感知方法。当节点的邻居相对较少时，遭受攻击的邻居节点的

数目很容易超过该节点的度的 1/2。基于多数投票(majority voting)机制的状态感知算法[24],能够在更为宽松的假设 5 条件下,实现节点状态的感知。

具体地,在 i 时刻,每个节点 k 将认为自身处于下列 3 种状态中的一种:处于安全状态 $\tau_{k,i}=1$;处于受攻击状态 $\tau_{k,i}=-1$;处于不确定状态 $\tau_{k,i}=0$。在基于多数投票机制的状态感知过程中,每个节点 k 按照下式实现状态感知:

$$\hat{\tau}_{k\to l,i}=\mathrm{sgn}\Big(\sum_{l}\tau_{l,i-1}\Big)\ ,\ l\in S_{k,i}^{\mathrm{S}}\text{或}\ l\in S_{k,i}^{\mathrm{D}} \tag{15}$$

式中,sgn(·)为符号函数。由式(15)可以看出,每个节点 k 通过聚合来自节点 $l\in S_{k,i}^{\mathrm{S}}$ 或 $l\in S_{k,i}^{\mathrm{D}}$ 上一时刻的状态 $\tau_{l,i-1}$,来推测当前时刻集合 $S_{k,i}^{\mathrm{S}}$ 或 $S_{k,i}^{\mathrm{D}}$ 中节点 l 的状态 $\hat{\tau}_{k\to l,i}$。当集合 $S_{k,i}^{\mathrm{S}}$ 或 $S_{k,i}^{\mathrm{D}}$ 中大多数节点处于相同状态时,节点 k 便推测该集合中所有节点都处于相同的状态。

不失一般性,在初始时刻 $i=0$,由于缺乏关于 FDI 攻击的先验知识,由假设 1 网络中所有节点 k 均不确定自身状态,即 $\tau_{k,0}=0$,故节点无法实现进一步的状态感知。事实上,若节点 k 所有邻居节点都属于集合 $S_{k,i}^{\mathrm{S}}$,即 $S_{k,i}^{\mathrm{D}}=\varnothing$,且邻域 N_k 内的节点均处于不确定状态,基于假设 3,则推测节点 k 邻居节点均处于安全状态[24]:

$$\hat{\tau}_{k\to l,i}=1\ ,\ l\in N_k,\quad \text{若}\ S_{k,i}^{\mathrm{D}}=\varnothing\ \text{且}\ \{\tau_{l,i-1}\}_{l\in S_{k,i}^{\mathrm{S}}}=\{0\} \tag{16}$$

进一步地,每个节点 k 将再次采用多数投票机制,通过对自身状态的感知,判断自身是否遭受 FDI 攻击。具体地,在 i 时刻,每个节点 k 与其邻居节点 l 分享所推测的状态 $\hat{\tau}_{k\to l,i}$,并聚合邻居节点对节点 k 状态的推断:

$$\tau_{k,i}=\mathrm{sgn}\Big(\sum_{l\in N_k^-}\hat{\tau}_{l\to k,i}\Big) \tag{17}$$

值得注意的是,尽管集合 $\{\hat{\tau}_{l\to k,i}\}_{l\in N_k^-}$ 仅包含了节点 k 的单跳邻居节点 $l\in N_k^-$ 的状态推断;而根据式(15),由节点 l 所推断的状态 $\hat{\tau}_{l\to k,i}$ 又与节点 l 的邻居(即节点 k 的多跳邻居 $\{m\in N_l\}_{l\in N_k^-}$)有关。故上述基于多数投票机制的状态感知算法实际上以一种扩散分布式的方式融合了来自多跳邻居的状态推断。这种方式将有助于增强对遭受 FDI 攻击节点的检测性能。

3) 基于朴素贝叶斯准则的状态感知方法。上述 2 种方法均是在划分集合 $S_{k,i}^{\mathrm{S}}$ 和 $S_{k,i}^{\mathrm{D}}$ 的基础上,实现对节点状态的感知。与之不同的是,基于贝叶斯的 DLMS(DLMS based on Bayes,BDLMS)算法[40]无须划分节点,而是通过评估节点 k 的邻居节点 l 和 u 之间状态的一致性,并通过朴素贝叶斯准则(naive Bayesian rule)实现对节点状态的感知。

BDLMS 算法采用混合系统结构,基于假设 4、6,并进一步额外假设不同簇之间估计参数的相似性已知。每个节点 k 首先计算与其邻居节点 l 无协作中间估计值之间的估计误差 $e_i(l,k)$(文献[40]给出了其计算方法)。进一步地,基于与邻居节点的估计误差,节点 k 通过下式来评估邻居节点 l 和 u 的状态是否一致:

$$\gamma_i(l,u)=\begin{cases}1, & \text{若}\ f_i(l,u)\leqslant\theta_{k,i}\\ 0, & \text{若}\ f_i(l,u)>\theta_{k,i}\end{cases} \tag{18}$$

式中,$f_i(l,u)=|e_i(l,k)-e_i(u,k)|$ 表示邻居节点 l 和 u 的估计误差之间的差异,其中,$l,u\in N_k$ 且 $l\neq u$。$\theta_{k,i}$ 是检测门限。$\gamma_i(l,u)=1$ 表示节点 k 认为其邻居节点 l 和 u 的状态一致,即同时安全或同时遭受攻击;$\gamma_i(l,u)=0$ 表示认为其状态不一致。在 i 时刻,节点 k 检测其邻居节点 l 与其他邻居节点状态是否一致的结果为 $\gamma_i(l,N_k\backslash\{l\})=\{\gamma_i(l,l_{(1)}),\gamma_i(l,l_{(2)}),\cdots,\gamma_i(l,l_{(n_k-1)})\}$,其中 $N_k\backslash\{l\}$ 表示邻域 N_k 中不包含节点 l 的子集。

为了有效检测网络中的受攻击节点,该算法进一步额外假设节点被攻击的先验概率已知;根据节点间状态是否一致的结果 $\gamma_i(l,N_k\backslash\{l\})$,并基于朴素贝叶斯准则,通过计算自身以及邻居节点遭受 FDI 攻击的后验概率,以确认各节点是否遭受 FDI 攻击。对于节点 k 的邻居节点 l,若其遭受 FDI 攻击的后验概率 $p(l\,|\,\gamma_i(l,N_k\backslash\{l\}))$ 小于门限 p_t,节点 l 则处于安全状态;反之,则遭受 FDI 攻击。其中,$p(l\,|\,\gamma_i(l,N_k\backslash\{l\}))$ 由节点被攻击的先验概率和 $\gamma_i(l,N_k\backslash\{l\})$ 共同确定(文献[40]给出了其计算方法)。

至此,基于上述不同方法,对抗网络中的各节点可实现对 FDI 攻击的检测。基于可信参考估计值的检测方法在假设 4 条件下,通常要求网络中每个节点 k 邻域内受攻击节点的数目不超过其节点度的 1/2。而基于数据分布差异的检测方法,通过使用基于多数投票机制的状态感知方法,能在更为宽松的假设 5 条件下感知节点状态,实现对 FDI 攻击的检测。下文将进一步讨论弹性参数估计策略的研究进展。

2.2　弹性参数估计策略

基于 2.1 节所介绍的 FDI 攻击检测方法，自适应网络中各节点能够借助其邻域内的数据感知自身状态，从而将网络中节点划分为安全节点和受攻击节点的不同集合。进一步地，为了精确估计未知参数向量，各节点需采取弹性参数估计策略，抑制恶意中间估计值在网络中的扩散。目前弹性参数估计策略主要可分为组合系数优化策略和数据替换策略 2 类。其中，组合系数优化策略[22-23,25,38,41]通过优化组合步骤各节点的组合系数，以减少或抑制受攻击节点处恶意中间估计值的扩散；数据替换策略[24-25,37,39]则将受攻击节点处的恶意数据替换为安全节点处未受攻击影响的安全数据来抑制恶意数据在网络中的扩散。

2.2.1　组合系数优化策略

在遭受 FDI 攻击的对抗网络中，节点 k 通过为安全的邻居节点分配较大的组合系数，而为遭受 FDI 攻击的邻居节点分配较小的组合系数，以抑制恶意中间估计值的扩散。特别地，当组合系数 $c_{l,k}$（见式(3)）等于 0 时，则不组合遭受攻击的节点 l 的数据。

在 R-DLMS 算法[41]中，每个节点 k 将设置其邻居节点的信誉值，该信誉值与参考估计值和邻居节点中间估计值之间欧氏距离的平方 $\|\boldsymbol{\varphi}_{l,i}-\overline{\boldsymbol{\varphi}}_{k,i}^{\mathrm{ref}}\|_2^2$ 成反比，也就是 $\|\boldsymbol{\varphi}_{l,i}-\overline{\boldsymbol{\varphi}}_{k,i}^{\mathrm{ref}}\|_2^2$ 越大，该邻居节点的信誉值也越小，该节点遭受 FDI 攻击的可能性则越大。进一步地，各节点根据邻居节点的信誉值成比例地分配邻居节点的组合系数，通过给信誉值较低的节点分配较小的组合系数以减少恶意中间估计值的扩散，在一定程度上可减小 FDI 攻击对算法估计精度的影响。

不同于 R-DLMS 算法，S-DLMS 算法[23]并不组合来自所有邻居的中间估计值。在 S-DLMS 算法中，得到安全节点集合后，各节点的 DLMS 子系统仅组合自身以及安全邻居的中间估计值。然而，在某些特定情况下，例如遭受攻击的节点的邻居较少时，S-DLMS 算法使用 Metropolis 组合系数可能会不恰当地赋予该受攻击节点较大的组合系数，导致算法估计性能的恶化。

删除权重的 DLMSKL（DLMSKL by deleting weights，DLMSKL-DW）算法（DLMSKL 算法[25]的一个特例），通过移除网络中的受攻击节点，即不考虑受攻击节点处的估计，同时也不组合受攻击节点的数据，以抑制恶意中间估计值的扩散。尽管移除受攻击节点能有效地抑制恶意中间估计值的扩散，但在某些特殊情况下，例如网络中有较多节点遭受攻击时，可能会影响自适应网络的整体参数估计性能。

与 S-DLMS 算法类似，在适用于多任务网络的弹性分布式参数估计算法[38]中，每个节点仅组合自身以及安全邻居的中间估计值。该算法考虑了 2 种组合策略：一种是平均组合策略，即赋予邻域内所有参与组合的节点相同的权重；另一种则是基于 LOF 的组合策略，其中各节点为邻居节点分配的组合系数与该邻居节点的 LOF 值成反比。与平均组合策略相比，基于 LOF 的组合策略有助于提升算法的估计性能和鲁棒性，但同时又会导致算法收敛速度变慢，增加算法的计算复杂度[38]。

2.2.2　数据替换策略

在遭受 FDI 攻击的对抗网络中，通过选择参考邻居，并将受攻击节点处的恶意观测值或恶意中间估计值替换为参考邻居处的观测值或中间估计值，在参考邻居选择适当的情况下，同样有利于抑制恶意中间估计值在网络中的扩散。

作为 DLMSKL 算法[25]的另外 2 个特例，DLMSKL-RM（DLMSKL by replacing the measurement data）和 DLMSKL-RI（DLMSKL by replacing the intermediate data）算法分别采取了替换受攻击节点处的观测值和中间估计值的策略。具体地，在 DLMSKL-RM 算法中，受攻击节点将邻域内 KLD 中位值所对应的节点视为可信赖的参考邻居，并将其恶意观测值替换为该参考邻居的观测值，然后重新计算自身的中间估计值并发送给邻居节点。最后，每个节点组合邻域内所有邻居的中间估计值。DLMSKL-RI 算法则是将受攻击节点处的中间估计值替换为参考邻居的中间估计值，然后每个节点再组合其邻域内所有邻居的中间估计值。与基于设计组合系数策略的 DLMSKL-DW 算法相比，DLMSKL-RM 和 DLMSKL-RI 算法的流程更复杂，节点间需多次通信才能完成 1 次估计值的迭代计算。

DLMS-CV 算法[39]同样使用参考邻居的中间估计值替换受攻击节点的恶意中间估计值，并采用了一种启发式方法选取参考邻居。具体地，对于每个节点 k，若其自身以及所有邻居都是安全的，则不需要选取参考邻居节点替换中间估计值；若节点 k 为安全节点，但其邻域内存在受攻击节点，则选取节点 k 作为参考邻居；若节点 k

为受攻击节点，且其邻域内可能还存在其他受攻击节点，则选取节点 k 邻域内的任意安全节点作为参考邻居。

此外，针对多任务网络的弹性分布式参数估计算法[37,40]中，每个受攻击节点将与自身具有最小相关匹配误差的邻居视为参考邻居，利用其无协作估计值的关联值重新计算自身 DLMS 子系统的中间估计值后，每个节点再组合邻域内所有邻居的中间估计值。

安全数据替换恶意数据的弹性参数估计策略取决于是否选择了适当的参考邻居。启发式的参考邻居选择方法[25,37,39-40]通常不能保证所选择的参考邻居一定能优化网络的参数估计性能。事实上，有可能通过选择参考邻居，优化网络整体的参数估计性能[24]。在构建关于参考邻居的约束优化问题的基础上，通过最小化（近似的）稳态网络均方偏差的上界，文献[24]得到了一种最优参考邻居选择方法。仿真实验结果表明，使用最优参考邻居的中间估计值替换受攻击节点处的恶意中间估计值，能够提高对抗网络中的参数估计精度[24]。

上述弹性参数估计策略有助于减少或抑制恶意中间估计值在网络中的扩散，提升在对抗网络中分布式参数估计算法的性能。对于组合系数优化策略，设计适当的组合系数有助于减少恶意中间估计值的扩散。然而，当节点 k 仅组合邻域内安全节点的中间估计值时，尽管能抑制其受攻击邻居处恶意中间估计值的扩散，但也阻碍了网络中其他安全中间估计值的扩散，进而影响网络的整体估计性能。而对于数据替换策略，若能选择适当的参考邻居，则有利于抑制恶意中间估计值的扩散，且不影响其他安全中间估计值在网络中的扩散。然而，受攻击节点处的数据替换与再次扩散，将增加算法的通信负担。

3 弹性分布式参数估计算法的总结分析

3.1 现有算法总结

按照网络任务数、算法结构是否为混合系统、基于不同的假设、FDI 攻击检测方法以及弹性参数估计策略，表 1 分类总结了现有的弹性分布式参数估计算法。其中，CSP-H 和 CSP-O 分别是采用启发式方法和采用最优参考邻居选择方法的 CSP 算法[24]；DLMS-LOF1 与 DLMS-LOF2 分别是文献[38]提出的采用平均组合策略和采用 LOF 组合策略的算法。

表 1 弹性分布式参数估计算法研究总结

Tab. 1 Summary of the researches on resilient distributed parameter estimation algorithms

弹性分布式参数估计算法	网络任务数	是否为混合系统	基于假设	FDI 攻击检测方法			弹性参数估计策略	
				可信参考估计值	数据分布差异		组合系数优化	数据替换
					节点划分	状态感知		
R-DLMS[38]	单任务	×	2	√	—	—	√	—
S-DLMS[23]		√	4、7	√			√	
DLMSKL-RM[25]				—			—	√
DLMSKL-RI[25]		×	1、4、7		KL 散度	邻域内受攻击节点的数目		√
DLMSKL-DW[25]							√	—
DLMS-CV[37]		√	4、7		交叉检验		—	√
CSP-H[24]		×	3、5、7		相关熵	多数投票	—	√
CSP-O[24]								√
SM-DLMS[39]		√	4	√	—	—	—	√
DLMS-LOF1[41]	多任务	×	4	—	LOF	邻域内受攻击节点的数目	√	—
DLMS-LOF2[41]								
BDLMS[40]		√	4、6	朴素贝叶斯准则			—	√

值得注意的是，FDI 攻击可能是固定不变的[37-38,40-41]，即在整个攻击过程中攻击者采用相同的攻击方式对相同的节点持续发动 FDI 攻击；FDI 攻击也可能是时变的[23-25,39]，例如攻击

者可间歇性地发起 FDI 攻击[23,25,39]。在上述假设条件下，S-DLMS 算法[23]、DLMSKL 算法[25]以及 DLMS-CV 算法[39]对时变的 FDI 攻击具有弹性。此外，仿真实验表明，在上述假设条件下，FDI 攻击强度和受攻击节点的数目均随时间变化时，CSP 算法[24]依然能保持较高的参数估计精度，且明显优于 S-DLMS 算法[23]、DLMSKL 算法[25]以及 DLMS-CV 算法[39]。

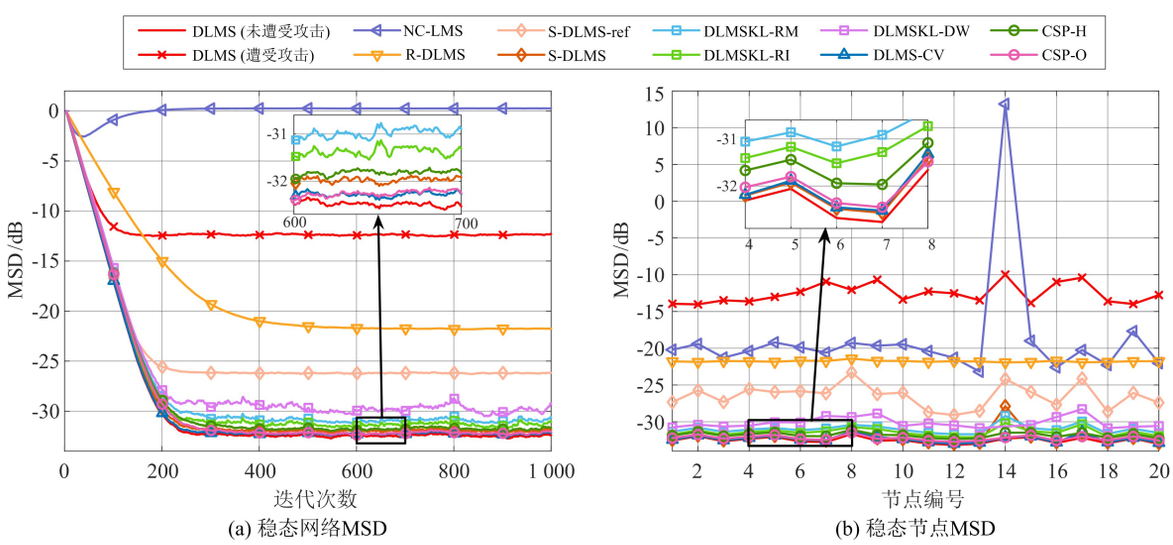
3.2　性能分析

本文设计了一组仿真实验，以综合评估不同场景下弹性分布式参数估计算法的性能。为了简化讨论，仅考虑单任务网络中的参数估计问题[23-25,39,41]。具体地，考虑一个如图 1 所示的包含 $N=20$ 个节点的分布式自适应网络，未知参数向量 $\boldsymbol{w}^{\circ}=[0.5,0.5,-0.5,-0.5]^{\mathrm{T}}$。每个节点 k 处的步长均设置为 $\mu_k=0.02$，回归矢量 $\boldsymbol{u}_{k,i}$ 由方差为 1 的零均值高斯随机过程产生，高斯白噪声的方差满足 $\sigma_{v,k}^2\in[0.1,0.4]$，受攻击节点 $k\in A_i$ 处的注入误差向量 $\boldsymbol{w}_{k,i}^{\mathrm{a}}\in(0,6]$。DLMSKL 算法[25]、DLMS-CV 算法[39]及 CSP 算法[24]的其他参数设置与文献[24-25,39]一致。在仿真实验中，DLMS(未遭受攻击)和 DLMS(遭受攻击)分别表示安全网络中或遭受 FDI 攻击的对抗网络中的 DLMS 算法。除 R-DLMS 算法之外，其他算法均使用 Metropolis 规则[23-25,39]设计组合系数。

不失一般性，本文采用均方偏差(mean-square deviation，MSD)μ[4,23-25,37-42]作为指标来评价算法的参数估计精度。在 i 时刻，每个节点 k 处的均方偏差为 $\mu_{k,i}\triangleq\frac{1}{Z}\sum_{\zeta=1}^{Z}\|\boldsymbol{w}_{k,i,\zeta}-\boldsymbol{w}^{\circ}\|_2^2$，其中，$\boldsymbol{w}_{k,i,\zeta}$ 表示在第 ζ 次独立重复实验中，节点 k 在 i 时刻对未知参数向量 $\boldsymbol{w}^{\circ}$ 的估计值。定义暂态网络均方偏差为 $\mu_i^{\mathrm{net}}\triangleq\frac{1}{N}\sum_{k=1}^{N}\mu_{k,i}$。稳态网络 MSD 与稳态节点 MSD 分别通过平均最后 200 个时刻的网络 MSD 和节点的 MSD 得到。所有仿真实验结果均是 $Z=500$ 次独立重复实验的平均结果。

首先考虑受攻击节点数量较少的情况。随机选择网络中的一个节点(本实验中，选取图 1 中的节点 14)遭受 FDI 攻击，以验证单任务网络中弹性分布式参数估计算法的估计性能。在这种情况下，网络中各节点的受攻击邻居数目均少于其节点度的 1/2，即满足假设 4。

如图 4 所示，在遭受 FDI 攻击的对抗网络中，多数弹性分布式参数估计算法均表现出优越的参数估计性能。具体地，CSP 算法、DLMS-CV 算法、S-DLMS 算法以及 DLMSKL 算法在收敛后的稳态 MSD 均接近于安全网络中的 DLMS 算法。这是因为这些算法的 FDI 攻击检测机制，能够相对有效地检测到受攻击节点，并通过弹性参数估计策略抑制恶意中间估计值在网络中的扩散，从而减小网络估计性能的损失。然而，由于 R-DLMS 无法有效地区分受攻击节点和安全节点，其估计性能的损失较显著。



(a) 稳态网络MSD　　(b) 稳态节点MSD

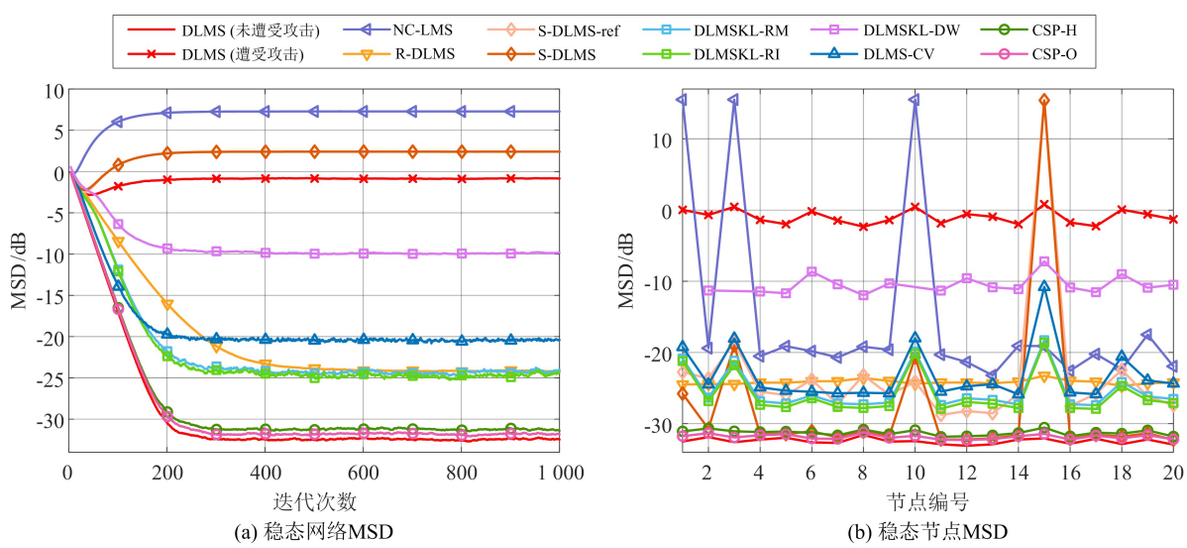
图 4　受攻击节点数较少情况下不同弹性分布式参数估计算法的估计性能

Fig. 4　Estimation performance of different resilient distributed parameter estimation algorithms with a relatively small number of compromised nodes

此外，由于 DLMS 算法缺乏 FDI 攻击检测机制，恶意中间估计值会随着节点间的数据交互在网络中扩散，并影响原本未遭受攻击的节点，从而导致整个网络的参数估计性能的严重恶化。值得注意的是，对于 NC-LMS 算法，受攻击节点 14 处的稳态估计性能显著恶化，但并未影响其他节点。因此，从网络整体来看，NC-LMS 算法无法对未知参数向量进行有效的估计。此外，因为假设 4 成立，S-DLMS-ref，即各节点处 S-DLMS 算法的参考估计值的稳态 MSD 均较为合理，这表明 S-DLMS 算法基于 NC-LMS 子系统选取了可靠的可信参考估计值。

现在考虑较多节点遭受攻击的情况，其中节点 1、节点 3 以及节点 10 遭受了 FDI 攻击。特别地，对于节点 15，其受攻击的邻居节点数量已超过了其度的 1/2。

值得注意的是，该场景不再满足 S-DLMS 算法、DLMSKL 算法以及 DLMS-CV 算法中的重要假设 4，即网络中各节点的受攻击邻居数目少于其节点度的 1/2。图 5 为受攻击节点数较多情况下不同弹性分布式参数估计算法的估计性能，可以观察到 S-DLMS 算法及其可信参考估计值 S-DLMS-ref 在节点 15 处的稳态 MSD 均显著恶化。这是由于节点 15 错误地选择了其受攻击邻居的中间估计值作为参考估计值，从而无法有效地限制恶意中间估计值的扩散，导致 S-DLMS 算法无法准确估计未知参数向量。此外，对于基于假设 4 和邻域内受攻击节点的数目来实现状态感知的 DLMSKL 算法和 DLMS-CV 算法，节点 15 会错误地将受攻击邻居误判为安全节点，从而导致算法参数估计性能的恶化。



(a) 稳态网络MSD (b) 稳态节点MSD

图 5 受攻击节点数较多情况下不同弹性分布式参数估计算法的估计性能

Fig. 5 Estimation performance of different resilient distributed parameter estimation algorithms with a relatively large number of compromised nodes

另外，由于基于多数投票的状态感知方法不受假设 4 的限制，CSP 算法的参数估计性能明显优于其他算法，且其稳态 MSD 几乎与安全网络环境中的 DLMS 算法保持一致。此外，CSP 算法中选择最优参考邻居的 CSP-O 算法性能要优于采用启发式选择参考邻居的 CSP-H 算法。

4 未来研究展望

结合 FDI 攻击检测和抑制恶意中间估计值扩散的弹性分布式参数估计策略已被证明是应对 FDI 攻击的可行方法之一。本文系统总结了近年来弹性分布式参数估计算法的研究进展，探讨了现有算法的设计原理、性能差异以及适用条件。尽管目前弹性分布式参数估计算法的研究已取得部分进展，但仍有不少问题值得进一步深入研究：

1）现有的弹性分布式参数估计算法主要关注网络中节点遭受 FDI 攻击的情况。然而，在复杂的对抗网络中，还可能遭受包括拜占庭攻击、拒绝服务(denial of service)攻击[47]、稀疏传感器(sparse sensor)攻击[48]、重放攻击(replay attack)[49]等不同类型的网络攻击。鉴于不同类型

攻击具有独特的特性和攻击机制，因此需要研究如何在网络遭受多种类型甚至混合攻击的情况下，更好地实现攻击检测以及弹性分布式参数估计。

2）现有的弹性分布式参数估计算法仅考虑了观测噪声为高斯白噪声的情况。然而，在实际环境中还存在多种复杂的噪声，例如脉冲噪声、有色噪声等。如何在存在复杂噪声的对抗网络环境中实现弹性分布式参数估计，有待深入研究。

3）现有的弹性分布式参数估计算法通常对网络中遭受攻击的节点数目设有一定限制。然而，在某些情况下，例如复杂的战场环境或大规模自然灾害受灾区，网络中的节点可能会受到大面积攻击或瘫痪，导致算法对未知参数估计精度的下降甚至恶化。因此，需要进一步研究在这类情况下实现对未知参数的相对可靠的估计。

4）在分布式参数估计问题中，自适应网络中的各个节点之间需要协同工作。在实际中，由于每个智能体节点的计算资源有限，且节点部署的物理环境可能复杂多变，节点之间可能存在通信延迟。然而，分布式参数估计通常涉及迭代优化过程，需经历多轮信息迭代更新以逐步收敛到参数的估计值。通信延迟可能导致算法无法在实时性要求较高的应用中提供即时的参数估计，且延迟还可能导致节点之间信息的不同步或不完整传输，进而影响网络整体估计的一致性。因此，在存在通信延迟的对抗网络中实现对未知参数的弹性分布式估计，是一个值得研究的方向。

5）现有的弹性分布式参数估计算法通常要求邻居节点之间始终以协作的方式分享中间估计值。在实际工程应用中，由于自适应网络中智能体节点的载荷有限，通常需要考虑节点间的通信成本，以控制能耗，延长节点使用寿命。因此，研究低通信成本的弹性分布式估计算法很有意义。

6）随着人工智能技术的不断发展，以深度学习为代表的人工智能算法在图像识别、目标跟踪等诸多领域得到了广泛应用。与传统的算法不同，人工智能算法通过学习大量样本数据并分析数据的统计性质和规律关系，构建一个能够对未知数据进行泛化的模型，在解决特殊复杂问题时通常更具优势。因此，针对特殊对抗网络环境，将人工智能技术与现有弹性分布式参数估计算法相结合，以实现对未知参数的弹性估计，是一个有待深入研究的方向，同时也具有重要的应用价值。

参 考 文 献

[1] SAYED A H. Adaptive networks[J]. Proceedings of the IEEE, 2014, 102(4): 460-497.

[2] HE S M, SHIN H-S, XU S Y, et al. Distributed estimation over a low-cost sensor network: a review of state-of-the-art[J]. Information Fusion, 2020, 54: 21-43.

[3] ZAYYANI H. Robust minimum disturbance diffusion LMS for distributed estimation[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68(1): 521-525.

[4] CATTIVELLI F S, SAYED A H. Diffusion LMS strategies for distributed estimation[J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1035-1048.

[5] CHEN J S, SAYED A H. Diffusion adaptation strategies for distributed optimization and learning over networks[J]. IEEE Transactions on Signal Processing, 2012, 60(8): 4289-4305.

[6] TU S Y, SAYED A H. Diffusion strategies outperform consensus strategies for distributed estimation over adaptive networks[J]. IEEE Transactions on Signal Processing, 2012, 60(12): 6217-6234.

[7] LILHORE U K, KHALAF O I, SIMAIYA S, et al. A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks[J]. International Journal of Distributed Sensor Networks, 2022, 18(9): 1-16.

[8] PASQUALETTI F, CARLI R, BULLO F. Distributed estimation via iterative projections with application to power network monitoring[J]. Automatica, 2012, 48(5): 747-758.

[9] DOOSTMOHAMMADIAN M, TAGHIEH A, ZARRABI H. Distributed estimation approach for tracking a mobile target via formation of UAVs[J]. IEEE Transactions on Automation Science and Engineering, 2022, 19(4): 3765-3776.

[10] DO PRADO R A, GUEDES R M, HENRIQUES F D R, et al. On the analysis of the incremental ℓ_0-LMS algorithm for distributed systems[J]. Circuits, Systems, and Signal Processing, 2021, 40(2): 845-871.

[11] SAEED M O B, PASHA S A, ZERGUINE A. A variable step-size incremental LMS solution for low SNR applications [J]. Signal Processing, 2021, 178: 107730.

[12] SCHIZAS I D, MATEOS G, GIANNAKIS G B. Dis-

tributed LMS for consensus-based in-network adaptive processing[J]. IEEE Transactions on Signal Processing, 2009, 57(6): 2365-2382.

[13] NAKAI-KASAI A, HAYASHI K. Optimal combination weight for sparse diffusion least-mean-square based on consensus propagation[C]//Proceedings of 2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference. [S. l.: s. n.]:IEEE, 2020: 228-235.

[14] ZAYYANI H, JAVAHERI A. A robust generalized proportionate diffusion LMS algorithm for distributed estimation[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68(4): 1552-1556.

[15] XIA W, SUN M Q, WANG Q. Direct target tracking by distributed Gaussian particle filtering for heterogeneous networks[J]. IEEE Transactions on Signal Processing, 2020, 68: 1361-1373.

[16] LI W L, XIONG K, JIA Y M, et al. Distributed Kalman filter for multitarget tracking systems with coupled measurements[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51(10):6599-6604.

[17] LOPES C G, SAYED A H. Diffusion least-mean squares over adaptive networks: formulation and performance analysis[J]. IEEE Transactions on Signal Processing, 2008, 56(7): 3122-3136.

[18] KHALILI A, TINATI M A, RASTEGARNIA A, et al. Steady-state analysis of diffusion LMS adaptive networks with noisy links[J]. IEEE Transactions on Signal Processing, 2012, 60(2): 974-979.

[19] HUA F, NASSIF R, RICHARD C, et al. Diffusion LMS with communication delays: stability and performance analysis[J]. IEEE Signal Processing Letters, 2020, 27: 730-734.

[20] CHEN J, RICHARD C, SAYED A H. Multitask diffusion adaptation over networks[J]. IEEE Transactions on Signal Processing, 2014, 62(16): 4129-4144.

[21] CHEN J, RICHARD C, SAYED A H. Diffusion LMS over multitask networks[J]. IEEE Transactions on Signal Processing, 2015, 63(11): 2733-2748.

[22] HUA Y, HU L M, CHEN F. An adaptive malicious punishment over secure distributed estimation under attacks[C]//Proceedings of 2018 IEEE International Conference on Computer and Communications. [S. l.]: IEEE, 2018: 2195-2199.

[23] LIU Y, LI C G. Secure distributed estimation over wireless sensor networks under attacks[J]. IEEE Transactions on Aerospace and Electronic Systems, 2018, 54(4): 1815-1831.

[24] XIA W, ZHANG Y H. Resilient distributed estimation against FDI attacks:a correntropy-based approach[J]. Information Sciences, 2023, 635: 236-256.

[25] HUA Y, CHEN F, DENG S, et al. Secure distributed estimation against false data injection attack[J]. Information Sciences, 2020, 515: 248-262.

[26] WAN F Y, MA T, HUA Y, et al. Secure distributed estimation under Byzantine attack and manipulation attack[J]. Engineering Applications of Artificial Intelligence, 2022, 116: 105384.

[27] YU T, DE LAMARE R C, YU Y. Robust resilient diffusion over multi-task networks against Byzantine attacks: design, analysis and applications[J]. IEEE Transactions on Signal Processing, 2022, 70: 2826-2841.

[28] MUSLEH A S, CHEN G, DONG Z Y. A survey on the detection algorithms for false data injection attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2020, 11(3): 2218-2234.

[29] DRAYER E, ROUTTENBERG T. Detection of false data injection attacks in smart grids based on graph signal processing[J]. IEEE Systems Journal, 2020, 14(2): 1886-1896.

[30] LIU L C, ESMALIFALAK M, DING Q F, et al. Detecting false data injection attacks on power grid by sparse optimization[J]. IEEE Transactions on Smart Grid, 2014, 5(2): 612-621.

[31] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security, 2011, 14(1): 1-33.

[32] KIM T T, POOR H V. Strategic protection against data injection attacks on power grids[J]. IEEE Transactions on Smart Grid, 2011, 2(2): 326-333.

[33] GU Y P, YU X, GUO K X, et al. Detection, estimation, and compensation of false data injection attack for UAVs[J]. Information Sciences, 2021, 546: 723-741.

[34] LIN H, SUN P, CAI C X, et al. Secure LQG control for a Quadrotor under false data injection attacks[J]. IET Control Theory & Applications, 2022, 16(9): 925-934.

[35] CHEN Y, KAR S, MOURA J M F. Resilient distributed estimation through adversary detection[J]. IEEE Transactions on Signal Processing, 2018, 66(9): 2455-2469.

[36] XIA W, ZHOU Z Y, JIANG W Y, et al. Dynamic UAV swarm confrontation: an imitation based on mobile adaptive networks[J]. IEEE Transactions on

Aerospace and Electronic Systems, 2023, 59(5): 7183-7202.

[37] SHI Q, FENG M Y, LI X Y, et al. A secure distributed information sharing algorithm based on attack detection in multi-task networks[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67(12): 5125-5138.

[38] LIU Q X, YE M, CHEN F. Secure distributed estimation over multitask networks against multiple attacks[J]. IEEE Transactions on Aerospace and Electronic Systems, 2023, 59(3): 2480-2493.

[39] HUA Y, WAN F Y, GAN H P, et al. Distributed estimation with cross-verification under false data-injection attacks[J]. IEEE Transactions on Cybernetics, 2023, 53(9): 5840-5853.

[40] WANG T T, LI Y H, CHEN F, et al. Bayes-based distributed estimation in adversarial multitask networks[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(5): 4004-4019.

[41] 卢光跃，陈文晓，黄庆东. 基于信誉机制的分布式扩散最小均方算法[J]. 电子与信息学报，2015，37(5)：1234-1240.
LU Guangyue, CHEN Wenxiao, HUANG Qingdong. Distributed diffusion least mean square algorithm based on the reputation mechanism[J]. Journal of Electronics and Information Technology, 2015, 37(5): 1234-1240. (in Chinese)

[42] CHANG H N, LI W L. Correction-based diffusion LMS algorithms for secure distributed estimation under attacks[J]. Digital Signal Processing, 2020, 102: 102735.

[43] DO M N, VETTERLI M. Wavelet-based texture retrieval using generalized Gaussian density and Kullback-Leibler distance[J]. IEEE Transactions on Image Processing, 2002, 11(2): 146-158.

[44] SANTAMARÍA I, POKHAREL P P, PRINCIPE J C. Generalized correlation function: definition, properties, and application to blind equalization[J]. IEEE Transactions on Signal Processing, 2006, 54(6): 2187-2197.

[45] BREUNIG M M, KRIEGEL H P, NG R T, et al. LOF: identifying density-based local outliers[C]// Proceedings of 2000 ACM SIGMOD International Conference on Management of Data. [S. l.]: ACM, 2000: 93-104.

[46] MOSHKOVITZ M, DASGUPTA S, RASHTCHIAN C, et al. Explainable k-means and k-medians clustering[C]//Proceedings of International Conference on Machine Learning. [S. l.: s. n.], 2020: 7055-7065.

[47] DENG C. Distributed resilient control for cyber-physical systems under denial-of-service attacks[C]//Proceedings of the 23rd International Conference on Mechatronics Technology. [S. l.]: IEEE, 2019: 1-5.

[48] AN L W, YANG G H. Distributed sparse undetectable attacks against state estimation[J]. IEEE Transactions on Control of Network Systems, 2022, 9(1): 463-473.

[49] HUANG J H, YANG W, HO D W C, et al. Security analysis of distributed consensus filtering under replay attacks[J]. IEEE Transactions on Cybernetics, 2024, 54(6): 3526-3539.

作 者 简 介

周孟卿

男，2001 年生，硕士研究生，研究方向为分布式信号处理

E-mail：mqz@std.uestc.edu.cn

夏　威

男，1980 年生，博士，副教授，博士研究生导师，研究方向为统计信号处理和阵列信号处理

E-mail：wx@uestc.edu.cn

责任编辑　安　蓓