文章编号:1004-9037(2014)04-0516-10

网络化雷达协同抗欺骗式干扰技术研究进展

张林让 赵珊珊 周 宇 刘 楠 张 娟

(西安电子科技大学雷达信号处理国家重点实验室,西安,710071)

摘要:网络化雷达在战场上可以构成全方位、立体化、多层次的战斗体系,因此对欺骗式干扰对抗具有很大的优越性。本文首先简要介绍了网络化雷达概念,并分析了其抗干扰优势。根据网络化雷达融合结构不同,将现有协同抗干扰方法分为数据级融合抗欺骗式干扰和信号级融合抗欺骗式干扰两大类,其中,数据级融合方法进一步分类为点迹关联和航迹关联两类。本文对各类方法进行了详细介绍,在此基础上,比较分析了数据级融合和信号级融合两类方法的抗干扰性能及算法复杂度,为抗干扰措施的选择提供依据。最后,针对现有方法中存在的问题,对网络化雷达协同抗欺骗式干扰的发展趋势进行展望,指出下一步的研究方向。

关键词:网络化雷达;协同抗欺骗式干扰;数据级融合;信号级融合

中图分类号:TN973 **文献标志码**:A

Research Advance on Cooperative Anti-Deception Jamming in Netted Radar

Zhang Linrang, *Zhao Shanshan*, *Zhou Yu*, *Liu Nan*, *Zhang Juan*

(National Lab. of Radar Signal Processing, Xidian Univetsity, Xi′an, 710071, China)

Abstract: Netted radar system can sense the battle field in multiple levels and can gain rider information than a single radar system. Due to these features, netted radar system shows great advantages in anti-deception jamming. Firstly, an introduction to netted radar is given, and its potential cooperative electronic counter-countermeasures (ECCM) abilities against deception jamming are analyzed. According to the difference in the fusion structure, the existing anti-deception jamming approaches are classified as data fusion-based and signal fusion-based anti-jamming methods. Moreover, data fusion-based methods are classified as measurement fusion and track fusion. In this paper, all classes of cooperative anti-deception jamming approaches are presented in detail. Then, the anti-jamming performance and computational complexity of these two classes of methods are analyzed. Finally, based on the analysis of existing methods, this paper highlights the development direction of the cooperative anti-deception jamming, and then points out the future research interests.

Key words: netted radar; cooperative ECCM for deception jamming; data fusion; signal fusion

引 言

随着现代电子战的快速发展,以电子干扰为代表的电子战技术对雷达系统的工作性能和生存能力构成了严峻的挑战和威胁[1,2]。欺骗式干扰是电子干扰的重要干扰样式,主要应用于自卫式干扰和随队干扰中,可利用雷达的匹配滤波增益,以较小功率达到较好的干扰效果,同时更适合于干扰跟踪雷达,故其干扰技术及对抗策略的研究引起国内外学者的广泛关注[3]。尤其是数字射频存储器(Digital radio frequency memory, DRFM)[4]等先进器件的成熟为欺骗式假目标干扰的工程应用提供了有力的技术支持。DRFM 可通过截获、存储、转发敌方雷达信号,瞬时精确模仿雷达波形,在真实目标附近产生时域、频域和空域特征都十分相似

基金项目:国家自然科学基金(61301285,61301281,61001213)资助项目。

收稿日期:2014-06-10;**修订日期**:2014-07-15

的假目标。这种高逼真度假目标可以迷惑和扰乱雷达对真实目标的探测，甚至造成雷达检测、跟踪和识别等处理电路的过载。因此，如何有效对抗这种高度欺骗性假目标是亟待解决的问题，对提高雷达探测和跟踪能力具有重要意义。

针对欺骗式干扰，单部雷达对抗方法的研究发展很快，也有很多好的方法，可利用发射波形分集[5-7]、极化信息[8-11]、运动学信息[12-15]以及 DRFM 量化误差[16-18]对假目标进行鉴别。但是单部雷达视角单一，得到的环境信息有限，所能达到的抗干扰效能是有限的，对于高逼真度的有源假目标，很难达到理想的对抗效果。同时，随着干扰技术不断发展，部分抗干扰方法也将无法奏效，如 DRFM 延时转发时间已经可以达到 ms 量级，可实现在同一个脉冲重复周期对雷达进行欺骗式干扰[12]，此时波形分集的方法将完全失效；随着 DRFM 量化位数不断增大，利用量化误差进行欺骗式干扰对抗的效果也将越来越差。因此，单站雷达已经很难与其所面临的复杂电子干扰相抗衡，急需寻求更好的对抗思路。

Skolnik M. I. 总结了雷达抗干扰的发展，提出网络化雷达是其重要发展趋势，是提高雷达抗干扰能力和生存能力的一种有效方法[19]。网络化雷达在战场上可以构成全方位、立体化、多层次的战斗体系，具有全频段、多体制、多重叠系数等技术性能，因而具有很强的生存能力和抗干扰能力[20]。网络化雷达不但扩展了探测空域，同时实现了多站资源共享，建立灵活的单基地、双/多基地网，充分发挥体制对抗和群体对抗的优势，是适应未来战场环境需求的有效途径，多雷达组网的各种技术措施如多频段，全空域，多发射波形，变极化天线，数据融合，被动工作方式，能量管理等全面提高了雷达系统的“四抗”能力。网络化雷达协同抗欺骗式干扰的理论研究及应用处于起步阶段，仍有很多问题亟待解决，但已得到国内外研究学者的广泛关注，成为雷达抗干扰的重要研究方向。

1　网络化雷达

1.1　概述

网络化雷达是通过对多部不同体制、不同频段、不同工作模式、不同极化方式的雷达适当布站，借助通信手段链接成网，由网络中心站统一调配处理而形成的一个有机整体[20,21]。网络化雷达，又可称为多站雷达[22]，包括组网雷达和多基地雷达。它通过将不同体制、不同工作模式、不同频段的雷达量测信息在融合中心进行融合，可充分发挥雷达集群的优势，取长补短，利用不同雷达得到的回波信息进行协同干扰对抗。网络化雷达可按照作战需要灵活调整网内雷达的工作状态，充分发挥各雷达优势来完成协同对抗的任务，从而形成网络化雷达系统的电磁优势和信息优势，极大提高整体作战能力，特别是在复杂电磁干扰环境下[23]。

1.2　抗欺骗式干扰优势分析

首先，干扰机一般无法对整个网络化雷达进行欺骗式干扰对抗。网内的雷达频段不一致，而干扰机进行干扰是有一定频率范围的，则干扰机只能干扰对应频段的雷达，无法对整个雷达网进行有效的干扰；网内的雷达信号形式多样，若干扰侦察机无法有效识别分选信号，干扰机也很难同时进行干扰，则多假目标干扰无法针对所有雷达同时进行；网内雷达分布位置不同，辐射源数量增加，使信号空间的密度和分布更加复杂，干扰机无法有效的针对所有雷达同时进行干扰，只能对雷达网中的部分雷达进行干扰[24]。

在各雷达均受到欺骗式干扰时，网络化雷达仍然可以利用冗余探测信息有效鉴别出有源假目标，实现欺骗式干扰对抗。欺骗式干扰对抗的本质是在尽量保留真实目标的情况下，对假目标进行剔除，因此，找到真实目标与假目标之间的差异是对抗欺骗式干扰的基础。在网络化雷达中，各雷达从不同方向对目标进行探测、量测和跟踪，通过比较各雷达回波信号、量测值、或者跟踪航迹之间的差异，可以对真假目标进行有效鉴别。

1.3　融合级别

网络化雷达的核心技术是信息融合，也是协同抗干扰的关键。信息融合可以分成不同的级别[25]：检测级融合、位置级融合、目标识别（属性）级融合、态势估计、威胁估计这五级，融合信息量依次下降，融合算法难度也不断下降。网络化雷达协同抗干扰主要利用检测级融合和位置级融合来完成。

检测级融合即是信号级融合，直接利用各雷达的接收回波信号，对目标进行协同探测，也是一个分布式检测问题。位置级融合是直接在传感器的量测点迹或者状态估计上进行融合，即为数据级融合，进一步分为点迹融合和航迹融合。点迹关联一般用于集中式融合结构中，集中式融合结构将各雷达检测到的目标量测值传递到融合中心，在融合中

心进行数据对准、点迹相关、数据关联、航迹滤波、预测与综合跟踪。航迹关联一般用于分布式融合结构中，分布式融合结构中各雷达的检测报告在进入融合中心之前，先由其自己的数据处理器产生局部多目标跟踪航迹，然后把处理过的信息送至融合中心，中心根据各雷达的航迹数据完成航迹关联和航迹融合，形成全局估计。

2 网络化雷达协同抗欺骗式干扰技术

网络化雷达协同抗欺骗式干扰得到国内外研究学者的重视，也取得了较多的研究成果。根据网络化雷达融合中心所采用的融合结构不同，可以将协同抗干扰方法分为数据级融合抗欺骗式干扰和信号融合抗欺骗式干扰两大类。在网络化雷达中，数据级融合通过对各雷达得到的目标量测值进行转换、关联与融合，实现协同抗干扰；信号级融合直接利用各雷达得到的回波信号，通过检测级融合算法完成协同抗干扰。

2.1 数据级协同抗欺骗式干扰

由于回波的物理来源相同，网络化雷达中不同雷达对同一目标的量测值(包括位置量测与速度量测)转换到统一坐标系下是相对“集中”的，存在于一个量测误差决定的误差椭圆内。而相反地，在网络化雷达布站信息没有完全被获知的情况下，转发式干扰机很难对各节点雷达形成协同欺骗，不同雷达对有源假目标的量测转换到同一坐标系下是相对“分散”的。也就是说，对于网络化雷达，真实目标所具有的空间位置相关性，而欺骗式假目标不具备，这就为网络化雷达数据融合进行协同抗欺骗干扰提供了理论依据。

这种不具备空间位置相关性的假目标，称之为非协同假目标，是由干扰机独立的对各雷达进行欺骗产生的。相反地，协同假目标为干扰机针对各雷达进行协同欺骗产生的具备空间位置相关性的假目标，即位置信息吻合、速度信息一致。非协同欺骗与协同欺骗是针对网络化雷达才存在的概念，以非协同距离欺骗式干扰为例，非协同与协同假目标示意图如图 1 所示。产生协同假目标需要两个条件：一是干扰系统中的侦察机能有效确定网络化雷达中所有雷达的位置坐标和工作参数；二是干扰机具有同时针对各雷达进行欺骗干扰的能力，一般可以采用时分复用技术或者利用分布式干扰机来实现。由此可见，协同式干扰对网络化雷达具有更高的欺骗性，同时对干扰系统本身提出了更高的要求。

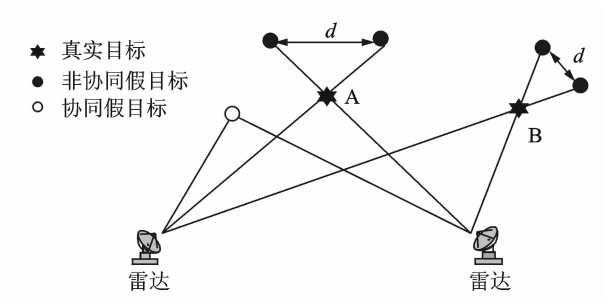

图 1 非协同与协同假目标示意图

Fig. 1 Illustration of uncooperative and cooperative false targets

2.1.1 点迹关联

2.1.1.1 非协同假目标对抗

针对非协同距离欺骗干扰，干扰机对各雷达产生的假目标存在于真实目标与该雷达的延长线上，在同一坐标下是相对分散的，如图 1 中所示。利用非协同假目标不具备空间位置相关性的特点，赵艳丽等人提出一种利用位置信息进行有源假目标鉴别的方法[26,27]，首先对各雷达得到的量测值进行坐标变换，并利用最近邻关联算法进行粗关联，得到关联量测序列，再利用卡方检验进行点检关联，对所有关联量测序列对应的目标进行真假鉴别。该方法的优点是可在保证对真实目标的误判概率的情况下，对有源假目标进行有效鉴别，其对假目标的鉴别能力决定于距离欺骗时间延迟、各雷达的量测误差、网络化雷达布站情况以及目标相对各雷达的位置关系。由于该方法仅利用了目标的位置信息，在距离网络化雷达较远区域，如图 1 中 B 点所示，相比于 A 点，由于各雷达相对目标的角度差异变小，假目标的分散程度明显下降，这将导致网络化雷达对此处假目标的鉴别能力显著降低。此时，提高假目标鉴别性能最直接的方法，就是通过改变网络化雷达布站情况，使得各雷达间的布站间距增大，但是，网络化雷达利用冗余探测信息进行假目标鉴别，必需保证进行数据融合的雷达的威力范围有重合区域，也正是在该重合区域才能对假目标进行鉴别，这将限制了各雷达间的布站间距不能无限增大。

针对较远区域假目标鉴别能力下降的问题，赵珊珊等人提出一种联合利用目标位置信息和速度量测进行有源假目标鉴别的方法[28]，首先利用位置信息进行有源假目标鉴别，与赵艳丽等人提出的方法相同。对通过检验的目标，先根据测得的径向

速度信息计算得到目标真实速度，并进一步利用真实速度信息进行有源假目标鉴别。该方法有效提高了对有源假目标的鉴别能力，尤其是在距网络化雷达较远区域，这都源于融合信息的增加。但是，该方法的融合步骤过于繁琐，可以考虑不利用串行融合方法，而是在一次卡方检验中同步融合位置和速度信息，即并行融合方法。此外，该方法最大问题在于它仅适用于网络化雷达中具有至少三部测速雷达的情况下。

上述两种点迹关联的方法，都认为雷达对目标的检测概率为 1，当网络化雷达中有两个雷达对目标的检测概率较低（如微弱目标、隐身目标等），未能探测到目标时，这两种方法将可能把真实目标误判为假目标，此时将使得漏警概率明显提高。针对这一问题，利用虚假目标量测存在信噪比高，且其他雷达的量测与虚假目标不关联的特点，徐海全等人提出了采用信噪比检验和卡方检验的雷达网抗虚假目标干扰算法[29]，在点迹关联之前，首先进行信噪比检验，对于信噪比高于给定门限的目标才进一步进行点迹关联检验，这样避免了其他雷达由于目标回波信噪比低未检测到此目标，而误将真实目标判断为虚假目标的问题。但是，该方法进行信噪比检验的门限值没有理论依据，且对于信噪比与真实目标接近的假目标，将会被误判为真实目标。笔者认为，对于检测概率小于 1 的情况下，应该将检测概率对点迹关联的影响考虑进去，利用贝叶斯公式重新推导关联检验门限，以及在多雷达情况下优化使用 K/M 准则，设计检测概率小于 1 的情况下的假目标鉴别算法。

对于非协同速度欺骗干扰，赵珊珊等人先计算得到目标真实信息，再利用卡方检验进行假目标鉴别[28]。除此方法外，也可以直接利用各雷达得到的径向速度信息的差异对有源假目标进行鉴别[30]：对于真实目标，网络化雷达中不同雷达测得的多普勒速度一般是不同的；而对于有源速度欺骗干扰，由于它是通过调制频率得到的，各雷达测得的多普勒速度是相同的。文献[30]给出了基于此差异的假目标鉴别流程，包括时间同步、数据对准和多普勒频率比较，并分析了网络化雷达布站对假目标鉴别的影响，但是并没有给出量测误差下欺骗式假目标鉴别的数学模型。这种方法的优点在于算法简单且实时性好，缺点在于应用场景假设过于理想，因为多普勒频率差异只有干扰机静止，目标运动的条件下才成立。对于常采用欺骗式干扰的自卫式干扰机往往是以目标为载体，必然是相同运动的，此时，这种方法将失效。

2.1.1.2　协同假目标对抗

上述方法仅能对非协同假目标进行有效鉴别，对于针对网络化雷达的协同假目标，上述方法均失效，或者鉴别效果较差。针对协同式欺骗干扰，可以通过破坏其两个必备条件进行有效对抗。通过在网络化雷达中设置一个“静默”接收站，是一种行之有效的方法，因为干扰侦察机无法发现接收站的位置，自然无法对整个网络化雷达进行协同欺骗。

杨林等提出一种利用 T/R-R（Transmitter/Receiver-receiver）型多基地雷达系统进行有源假目标鉴别的方法[31,32]，该方法将 T/R 站和 R 站得到的量测值进行点迹关联，选择马氏距离为检验统计量，在保证对真实目标的判定概率的条件下，设立自适应门限进行有源假目标鉴别。这里使用的点迹关联方法与多部单站雷达之间点迹关联算法类似，区别在于 R 站的量测信息与 T/R 站不同，应该为距离和信息与相对 R 站的方位角信息，所以利用 R 站的量测信息得到目标在统一坐标系下的定位坐标以及定位误差协方差矩阵的方法不同，具体算法可参见文献[33]。由于 R 站“静默”，干扰机无法侦察其具体位置，因此无法针对其进行干扰，此时存在两种情况，一种是 R 站没有受到欺骗式干扰，另一种较坏的情况是 R 站也同样接收到欺骗式干扰，但与 T/R 站检测到的假目标是非协同的，以距离欺骗假目标为例，T/R 站与 R 站同时被干扰情况下真假目标信息如图 2 所示，可以看到假目标是相对“分散”的。此外，利用异地配置的主/被动雷达也可以有效对协同假目标进行鉴别，李世忠等人先后提出两种异地配置的主/被动雷达进行假目标对抗的方法[34,35]。由于被动雷达只能对目标的方位角进行量测，对被动雷达而言，自卫式干扰机就相当于一个真实目标，距离欺骗干扰对被动雷达是无效的，如图 3 所示。

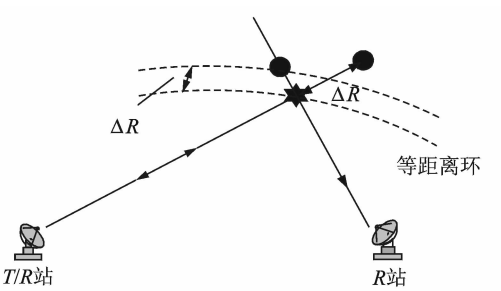

图 2　T/R-R 多基地雷达距离假目标示意图

Fig. 2　Illustration of range deception false targets in T/R-R multistatic radar system

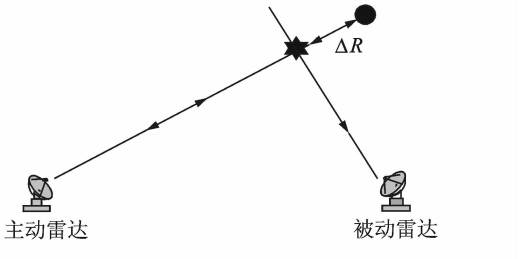

图 3 主/被动雷达距离假目标示意图

Fig. 3 Illustration of range deception false targets in active/passive radar

文献[34]基于角度统计量和距离统计量提出了两种主/被动雷达联合鉴别假目标算法：基于角度统计量的鉴别算法首先利用主动雷达的量测值对目标进行定位，并计算其相对被动雷达的方位角，再与被动雷达测得的方位角信息进行比较，使用卡方检验的方法对假目标进行鉴别；基于距离统计量的鉴别算法首先用交叉定位的方法对目标进行定位，并计算其相对主动雷达的径向距离，再与主动雷达量测得到的径向距离进行比较，使用卡方检验的方法对假目标进行鉴别。但是，基于角度统计量的鉴别算法没有利用被动雷达的俯仰角信息，基于距离统计量的鉴别算法没有利用主动雷达或被动雷达的俯仰角信息，因此，这两种鉴别方法没有充分利用主/被动雷达系统的所有量测信息，得到的鉴别效果并不是最优的。

文献[35]采用基准线最小距离法排除部分虚假目标，再利用三维分配算法进一步进行鉴别。基准线最小距离法是分别利用主动雷达量测值和主/被动雷达交叉定位对目标进行定位，再对得到的两个定位信息进行比较，利用卡方检验的方法对假目标进行鉴别，对通过检验的目标对，进一步利用三维分配算法进行鉴别。该算法与基于角度统计量和距离统计量鉴别虚假目标算法相比，可以得到较高的正确鉴别概率和较低的误鉴别概率。但是，三维分配算法是一个 0-1 优化问题，一般采用贪婪算法进行求解，在目标个数较多时，计算复杂度较高。

2.1.2 航迹关联

对于采用分布式融合结构的网络化雷达，各雷达分别对目标进行跟踪滤波，在存在航迹欺骗干扰的情况下，在融合中心可以利用航迹关联的方法对虚假航迹进行鉴别。真实目标的空间位置相关性反映在雷达滤波航迹上就是：来自于真实目标的航迹对的关联距离小，而来自虚假目标的航迹对关联距离大。利用这种航迹关联距离的差异，赵艳丽提出一种分布式组网雷达抗多假目标欺骗干扰处理方法[36]，首先对各雷达的航迹进行时间对齐与空间对准，再对同一时刻的滤波结果进行点迹关联算法，最后利用 K/M 法则得到最终航迹关联结果。该方法中 K/M 法则的选择具有主观性，另一种航迹关联检验的方法为将航迹对上每个时刻点的关联距离累加起来，作为航迹关联的检验统计量，并利用卡方检验对虚假航迹进行鉴别。由于联合利用了一段时间内的量测信息，航迹关联对虚假航迹的鉴别能力通常比点迹关联对假目标的鉴别能力好。

与协同假目标相似，针对网络化雷达的协同式欺骗也可能产生协同航迹欺骗干扰[37,38]，文献[37]中介绍了一种多机协同控制下的航迹欺骗技术，阐述了通过电子战斗机编队协作来产生具有空间、时间相关的虚假航迹的工作原理。为了在网络化雷达中的多部雷达上形成想定的、具有空间位置相关性的虚假航迹，干扰机需要对各雷达的位置坐标进行精确估计，对于一个设定的虚假航迹，计算相对各部雷达在各个时刻需要加入的假目标信息，然后根据设定好的欺骗参数，不断地对各部雷达同时实施欺骗干扰。在整个过程中，任何一步出错，都将导致协同式欺骗干扰失去应有的效果。因此，多雷达航迹欺骗干扰对干扰机要求比较高，侦察引导设备灵敏度要足以截获到雷达旁瓣信号，并能精确估计各雷达的位置，还能分析各雷达天线的扫描规律并精确测量其参数，干扰机发射功率要足够高，以使干扰信号从雷达天线的副瓣进入，干扰机的辐射功率、假目标的距离、速度和持续时间均可控，以根据设定的欺骗参数对各雷达进行协同欺骗[21]。

可以看出，对网络化雷达进行协同航迹欺骗的条件很苛刻，因此对抗协同航迹欺骗的方法就很简单，如改变网内部分雷达的扫描频率，改变可移动平台上雷达的空间位置，在网络化雷达加入“静默”的接收站或被动雷达等方法都可以破坏协同欺骗干扰产生的条件，对其进行有效地对抗。其中，加入接收站或被动雷达的方法与抗协同假目标干扰的方法相同，在分布式融合结构下，航迹关联的算法都与文献[36]中的方法相同，区别在于不同工作模式的雷达对目标进行跟踪滤波时所采用的目标量测方程不同，接收站可以根据距离和信息与方位角信息独立对目标进行跟踪，被动雷达需要利用主动雷达的量测信息进行航迹起始，再利用角跟踪算法得到目标滤波航迹。

2.1.3　数据级协同抗干扰总结

对现有文献中数据级协同抗干扰方法进行总结，如图 4 所示，协同抗干扰的理论基础均为：真实目标具有位置相关性，而假目标不具备。只是在不同工作模式、不同融合结构下，所采用的关联算法不同，从而产生不同的假目标鉴别算法。对于协同欺骗式干扰，可利用在网络化雷达中加入接收站或者被动雷达来对协同假目标进行有效鉴别。

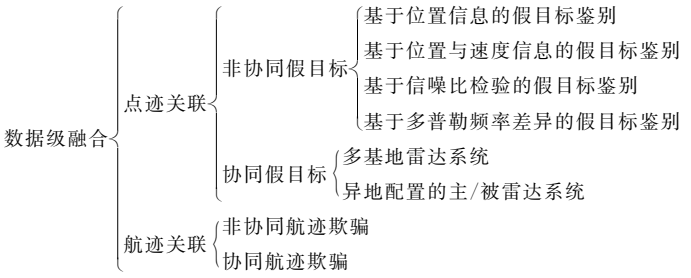

图 4　数据级协同抗欺骗式干扰技术总结

Fig. 4　Summary of data fusion-based cooperative anti-deception jamming technology

点迹关联用于集中式融合结构，通过对各雷达得到的目标量测值进行关联，以鉴别假目标，再对关联成功的真实目标进行点迹融合，最后在融合中心进行跟踪滤波，得到系统航迹，因此集中式融合结构先进行空间融合，再进行时间融合。而航迹关联用于分布式融合结构，在各雷达中独立对目标进行跟踪滤波，再对各雷达得到的跟踪航迹进行关联，以鉴别虚假航迹，并对关联成功的真实航迹进行融合，得到系统航迹，因此分布式融合结构先进行时间融合，再进行空间融合。

从计算量进行比较，集中式融合结构和分布式融合结构相差不大：集中式融合结构中点迹关联的复杂度较高，但是只需在融合中心进行一次跟踪滤波即可形成系统航迹；分布式融合结构中航迹关联的复杂度较低，因为在各雷达跟踪滤波阶段已经剔除部分虚假目标，只保留了可形成稳定航迹的目标，但是需要各个雷达独立地对目标进行跟踪滤波。主要区别在于：集中式融合结构的处理过程都在融合中心进行，而分布式融合结构将部分计算量转移到了各雷达站中，降低了融合中心的计算量。

从假目标鉴别能力上进行比较，由于航迹关联综合利用了一段跟踪时间内的量测信息，航迹关联对虚假航迹的鉴别能力通常比点迹关联的鉴别能力好。然而，在各雷达独立进行跟踪滤波的过程中，会对目标信息造成一定的损失，因此点迹关联所利用的信息更多，所得到的鉴别结果更加可靠。此外，由于集中式融合结构所需要传输的信息量更大，需要更高容量的通信链路。

因此，从抗欺骗式干扰的任务出发，网络化雷达采用集中式或者分布式融合结构都是可行的。但是，需要注意的是：(1)在融合中心处理能力不够，或通信链路容量不足的情况下，网络化雷达应该选择分布式融合结构，利用航迹关联的方法对假目标进行鉴别。(2)在假目标个数较多的情况下，应该先考虑利用集中式融合结构，以避免在各雷达中出现多目标跟踪或起始目标过量的问题，在对真实目标形成稳定航迹后，再考虑采用分布式融合结构。

2.2　信号级协同抗欺骗式干扰

除了空间位置相关性的差异外，目标回波与干扰信号在信号级上也存在差异性，从而为信号级协同抗干扰提供理论基础。对于有源假目标，不管干扰调制方式如何，只要是由同一欺骗干扰信号产生的，其在各雷达中的复幅度是完全相关的。对于真实目标，由于其雷达散射截面积(Radar cross section，RCS)随探测视角的变化而随机起伏，因此，若各雷达站之间足够远，对目标的视角差异足够大的情况下，雷达站得到的目标回波是相互独立的。

为满足目标回波之间相互独立的条件，雷达站之间的间距需满足的条件可以借鉴分布式 MIMO 体制[39-41]下关于目标回波信号相关性的结论。不同雷达接收到的目标回波之间的相关性与两雷达站间的间距 L、工作波长 λ、目标相对雷达的径向距离 R 和目标尺寸 D 有关。文献[39]中给出了一个目标回波之间的独立性条件：$L \geqslant \lambda R/D$，即将目标看成一个天线，则当两个雷达站相对目标的夹角对于目标直径决定的波束宽度时，两个雷达接收到的目标回波相互独立。

在雷达间距满足上述独立性条件时，真实目标

具有各向异性，而有源假目标具有各向同性，注意这里和数据融合所利用的空间位置相关性是不同的，这里真实目标的各向异性体现在信号级上目标回波间的相关性。利用这一差异，可利用信号级融合的方法对有源假目标进行鉴别，定义目标的慢时间复包络序列为脉冲压缩后若干连续脉冲重复周期中目标所在采样点的幅度所构成的序列，得到的目标慢时间复包络序列之间的相关性进行有源假目标鉴别，但该方法无法保证对真实目标的误判概率。在此基础上，文献[42]在有源假目标的复幅度满足高斯分布的假设下，通过对目标慢时间复包络序列间的互相关的概率密度函数进行分析，利用似然比检测对有源假目标进行恒虚警鉴别，并根据奈曼-皮尔逊准则设立门限，保证了有源假目标鉴别过程中对真实目标的误判概率可控。

利用真假目标空间散射特性的差异对欺骗干扰进行协同对抗，并不依赖于欺骗式干扰的信号调制方式，故可用于对不同欺骗式干扰产生的假目标进行鉴别，这是这类方法最大的优点。此外，信号级协同抗欺骗干扰可以与数据级融合算法串联使用，进一步提高网络化雷达对有源假目标的鉴别能力。但是，这类方法有效性的前提是：雷达站之间的布站间距满足目标独立性条件，干扰机可同时干扰到至少两部雷达站，这些都限制了这类方法的可用范围。

2.3 协同抗欺骗式干扰技术总结

雷达在接收到回波信号后，首先进行信号处理、目标检测和参数测量，再利用目标的量测值进行数据处理，得到目标航迹。因此，信号级融合在数据级融合的前端进行，点迹融合在航迹融合的前端进行，融合级别依次下降。

雷达在目标进行参数测量的过程中，将丢弃回波信号中目标的幅度和相位信息，因此，相比于数据级融合方法，信号级融合所利用的信息更多、更全面，可达到的抗干扰能力通常比数据级融合方法要高，对欺骗式假目标的鉴别能力更强。但是，由于所利用信息的复杂度较高，信号级协同抗干扰方法更加复杂，计算量较高。

值得注意的是，在欺骗式干扰下，利用信号级方法协同抗干扰后，对保留的目标可以再次利用数据级融合方法进行假目标鉴别，进一步降低网络化雷达的被欺骗概率。

3 结束语

目前，网络化雷达协同抗欺骗式干扰问题已经渗透到了许多理论和应用研究领域，但仍然存在大量的问题亟待解决，如多种抗干扰措施如何选择，如何将现有研究成果应用到实际中，以及网络化雷达之间的调度问题。从现有研究状况分析，协同抗干扰领域仍处于发展中，下面四个方面值得更多关注。

(1)建立网络化雷达智能抗干扰体系。认知雷达是新一代雷达系统[43,44]，将脑科学和人工智能融入雷达系统，赋予了雷达系统感知环境、理解环境、学习、推理并判断决策的能力，使雷达系统能够适应日益复杂多变的电磁环境。将认知雷达的概念应用到雷达系统中，就构成了智能抗干扰体系[45-47]。对于网络化雷达智能抗干扰体系应该有以下几个方面构成：首先对电磁环境进行感知，提出网络化协同干扰特征提取，并进行自适应干扰识别；根据干扰类型，自适应选择最优的融合算法和抗干扰措施；最后，为了得到更好的干扰对抗效果，对整个网络化雷达进行资源调度，如网络化雷达优化布站，优化控制各雷达工作模式、工作参数和抗干扰措施技术，实现整个系统最佳的抗干扰效能。

(2)数据级协同抗干扰。数据级融合协同抗干扰方法具有一定的可实践性，但是大部分现有方法的理论模型没有考虑时间对齐误差、空间对准误差以及雷达站位置坐标偏差等的关联算法的影响，在存在上述系统误差的情况下，如何更好地通过数据融合进行协同抗干扰，仍然需要对该问题进行进一步研究。此外，数据级协同抗欺骗式干扰方法所能达到的抗干扰性能的极限，即网络化雷达对假目标鉴别概率的理论值也值得深入分析，是数据级协同抗干扰下，对网络化雷达进行优化布站的依据。

(3)信号级协同抗干扰。信号级协同抗干扰方法的研究目前局限在仅利用目标回波幅度信息，更多地利用雷达回波信息将可以得到更好的抗干扰效能，如在目标检测或者参数估计的同时，进行假目标鉴别，使得真正实现信号级融合协同抗干扰。此外，信号级协同抗干扰在实践中仍存在较多难点，其对系统时间对齐，空间同步的精度要求较高。同时，融合算法的信号模型过于理想，如假设各雷达的检测概率为 1、各雷达中真实目标的回波信号相互独立、干扰机可同时对至少两部雷达站进行干扰。

(4)资源管理。网络化雷达是由多部雷达协同构成的一个整体，要想使得网络化雷达发挥出最优的抗干扰能力，融合中心对网络化雷达的控制起到至关重要的作用。资源管理主要包括：选择合适的融合算法，对系统误差进行校正，优化控制各雷达工作模式、工作参数和抗干扰措施技术，可移动雷达的优化布站，以及已布雷达的选择问题等。资源管理直接影响整个网络化雷达系统的整体抗干扰能力，应该从系统的工作任务出发和所受主要干扰的类型出发，对网络化雷达进行优化控制，只有完美的协同调度和统一管理才能使得网络化雷达发挥出最好的抗干扰能力，这与认知雷达的思想不谋而合。

参考文献：

[1] Schleher D C. Electronic warfare in the information age[M]. Norwood MA: Artech House, 2000.

[2] 赵国庆. 雷达对抗原理[M]. 2 版. 西安：西安电子科技大学出版社，2012.
Zhao Guoping. Radar electronic countermeasures theory [M]. second edition. Xi′an: Xidian University Publishing House, 2012.

[3] Li Nengjing, Zhang Yiting. A survey of radar ECM and ECCM[J]. IEEE Trans Aerosp Electron Syst, 1995, 31(3): 1110-1120.

[4] Roome S. Digital radio frequency memory[J]. IEE Electron Commun Engng J, 1990, 2(4): 147-153.

[5] Akhtar J. Orthogonal block coded ECCM schemes against repeat radar jammers[J]. IEEE Trans Aerosp Electron Syst, 2009, 45(3): 1218-1226.

[6] Liu Nan, Zhao Shanshan, Zhang Linrang. A radar ECCM scheme based on full-rate orthogonal pulse block[J]. J Comput Inf Syst, 2013, 9(24): 9771-9779.

[7] Zhang Jindong, Zhu Daiyin, Zhang Gong. New antivelocity deception jamming technique using pulses with adaptive initial phases[J]. IEEE Trans Aerosp Electron Syst, 2013, 49(2): 1290-1300.

[8] 李永祯，肖顺平，王雪松，等. 雷达极化抗干扰技术[M]. 北京：国防工业出版社，2010.
Li Yongzhen, Xiao Shunping, Wang Xuesong, et al. Technology of electronic counter-countermeasures using polarization[M]. Beijing: National Defense Industry Press, 2010.

[9] Song Lizhong, Qiao Xiaolin, Meng Xiande, et al. Study on the method of polarization suppression of cheating jamming in pulse Doppler radar [J]. Journal of Systems Engineering and Electronics, 2005, 16(2): 310-315.

[10] 李永祯，申绪涧，汪连栋，等. 基于辅天线的有源假目标欺骗干扰的极化识别[J]. 信号处理，2008，24(1)：24-27.
Li Yongzhen, Shen Xujian, Wang Liandong, et al. Polarization identification algorithm of active-decoys and radar targets based on sidelobe-canceller antenna [J]. Signal Processing, 2008, 24(1): 24-27.

[11] Huang Can, Chen Zhuming, Duan Rui. Novel discrimination algorithm for deceptive jamming in polarimetric radar [C]//Proc Int Conf on Information Technology and Software Engineering. Berlin, Heidelberg: [s. n.], 2013: 359-365.

[12] 饶彬. 对抗条件下弹道目标的雷达跟踪技术研究[D]. 长沙：国防科技大学，2011.
Rao Bin. Study on radar tracking technologies of ballistic targets in the presence of countermeasures [D]. Changsha: National University of Defense Technology, 2011.

[13] Rao Bin, Zhao Yanli, Xiao Shunping, et al. Discrimination of exo-atmospheric active decoys using acceleration information[J]. IET Radar Sonar Navig, 2010, 4(4): 626-638.

[14] Rao Bin, Xiao Shunping, Wang Xuesong, et al. Maximum likelihood approach to the estimation and discrimination of exoatmospheric active phantom tracks using motion features[J]. IEEE Trans Aerosp Electron Syst, 2012, 48(1): 794-819.

[15] Rao Bin, Xiao Shunping, Wang Xuesong. Joint tracking and discrimination of exoatmospheric active decoys using nine-dimensional parameter-augmented EKF[J]. Signal Process, 2011, 91(10): 2247-2258.

[16] Hill C J, Truffert V. Statistical processing techniques for detecting DRFM repeat-jam radar signals [C]//IEE Colloquium on Signal Processing Techniques for Electronic Warfare. London: [s. n.], 1992: 1-6.

[17] Greco M, Gini F, Farina A. Combined effect of phase and RGPO delay quantization on jamming signal spectrum[C]//IEE Int Radar Conf. Arlington, VA: [s. n.], 2005.

[18] Greco M, Gini F, Farina A. Radar deception and classification of jamming signals belonging to a cone class[J]. IEEE Trans Signal Process, 2008, 56(5): 1984-1993.

[19] Skolnik M I. Radar handbook[M]. second edition.

NewYork: McGraw Hill, 1990.

[20] 姜秋喜. 网络化雷达对抗系统导论[M]. 北京:国防工业出版社, 2011.
Jiang Qiuxi. Introduction to netted radar countermeasures system[M]. Beijing: National Defense Industry Press, 2011.

[21] 兰俊杰, 陈蓓, 徐廷新. 组网雷达发展现状及其干扰技术[J]. 飞航导弹, 2009(12):39-41.
Lan Junjie, Chen Bei, Xu Tingxin. Current development status and its countermeasures to netted radar [J]. Winged Missiles, 2009(12):39-41.

[22] Chenrnyak V S. Fundamentals of multisite radar systems: multistatic radars and multiradar systems [M]. Gordon and Breach, New York: 1998.

[23] 陈永光, 李修和, 沈阳. 组网雷达作战能力分析与评估[M]. 北京: 国防工业出版社, 2006.
Chen Yongguang, Li Xiuhe, Shen Yang. Analysis and evaluation to network radar engagement abilities [M]. Beijing: National Defense Industry Press, 2006.

[24] Stavroulakis P, Farsaris N, Xenos T D. Anti-jamming transmitter independent radar networks[C]// Int Conf on Signal processing, Communications and Networking. Chennai:[s. n.], 2008:269-273.

[25] 何友, 王国宏, 关欣, 等. 信息融合理论及应用[M]. 北京: 电子工业出版社, 2010.
He You, Wang Guohong, Guan Xin, et al. Information fusion theory with application [M]. Beijing: Publishing House of Electronics Industry, 2010.

[26] 赵艳丽. 弹道导弹雷达跟踪与识别研究 [D]. 长沙: 国防科技大学, 2007.
Zhao Yanli. Study on radar tracking and discrimination for ballistic missiles [D]. Changsha: National University of Defense Technology, 2007.

[27] 赵艳丽, 王雪松, 王国玉, 等. 多假目标欺骗干扰下组网雷达跟踪技术 [J]. 电子学报, 2007, 35(3):454-458.
Zhao Yanli, Wang Xuesong, Wang Guoyu, et al. Tracking technique for radar network in the presence of multi-range-false-target deception jamming [J]. Acta Electronic Sinica, 2007, 35(3):454-458.

[28] 赵珊珊, 张林让, 周宇, 等. 组网雷达点迹信息融合抗假目标干扰方法[J]. 电子科技大学学报, 2014, 43(2):865-869.
Zhao Shanshan, Zhang Linrang, Zhou Yu, et al. Measurement fusion method against false-target jamming for radar network [J]. Journal of University of Electronic Science and Technology of China, 2014, 43(2):865-869.

[29] 徐海全, 王国宏, 关成斌. 虚假目标干扰下的雷达网目标跟踪技术 [J]. 电子信息对抗技术, 2012, 27(1):28-31.
Xu Haiquan, Wang Guohong, Guan Chengbin. A tracking technique of radar network with false target jamming [J]. Electronic Information Warfare Technology, 2012, 27(1):28-31.

[30] Lü Bo, Song Yao, Zhou Changyou. Study of multistatic radar against velocity-deception jamming[C]// Int Conf on Electronics, Communication and Control. Ninbo:[s. n.], 2011:1044-1047.

[31] Yang Lin, Sun Zhongkang. Identification of false targets in bistatic radar system[C]//Proc IEEE National Aerospace and Electronics Conf. Dayton, OH: [s. n.], 1997, 2:878-883.

[32] 杨林, 徐晖, 孙仲康. T/R-R 型双基地系统识别欺骗式假目标[J]. 国防科技大学学报, 1997, 19(5):1-7.
Yang Lin, Xu Hui, Sun Zhongkang. Indentification method of false-targets in T/R-R bistatic radar system [J]. Journal of National University of Defense Technology, 1997, 19(5):1-7.

[33] 孙仲康, 周一宇, 何黎星. 单多基地有源无源定位技术[M]. 北京: 国防工业出版社, 1996.
Sun Zhongkang, Zhou Yiyu, He Lixing. Active/Passive location technology by signal/multistatic radar [M]. Beijing: National Defense Industry Press, 1996.

[34] 李世忠, 王国宏, 徐海全, 等. 异地配置的主/被动雷达抗多假目标干扰[J]. 火力与指挥控制, 2013, 38(5): 10-13.
Li Shizhong, Wang Guohong, Xu Haiquan, et al. Study on algorithm against multi-false-target deception jamming for active/passive radar at different sites [J]. Fire Control & Command Control, 2013, 38(5):10-13.

[35] 李世忠, 王国宏, 徐海全, 等. 三维空间主/被动雷达抗多假目标干扰研究[J]. 现代防御技术, 2012, 40(6): 118-124.
Li Shizhong, Wang Guohong, Xu Haiquan, et al. Algorithm against multi-false-target deception jamming for three-dimensional active/passive radar at different sites [J]. Modern Defence Technology, 2012, 40(6): 118-124.

[36] 赵艳丽, 陈永光, 蒙洁, 等. 分布式组网雷达抗多假目标欺骗干扰处理方法[J]. 电光与控制, 2011, 18(3) : 25-30.
Zhao Yanli, Chen Yongguang, Meng Jie, et al. A data

processing method against multi-false-target deception jamming for distributed radar network [J]. Electronics Optics & Control, 2011, 18(3): 25-30.

[37] 范振宇，王磊，陈越，等：组网雷达航迹欺骗技术研究[J]. 中国电子科学研究院学报，2010, 5(2)：179-186.
Fan Zhenyu, Wang Lei, Chen Yue, et al. A technique of track deception against netted radars [J]. Journal of CAEIT, 2010, 5(2): 179-186.

[38] Wu Yuqing, Shen Xiaofeng. A compound interference with distributed interference and false track interference for radar networking[C]//2012 6th Asia-Pacific Conference on Environmental Electromagnetics. Shanghai: [s. n.], 2012: 204-207.

[39] Fishler E, Haimovich A, Blum R, et al. MIMO radar: an idea whose time has come[C]//Radar Conference, Proceedings of the IEEE. Philadelphia: IEEE, 2004: 71-78.

[40] Fishler E, Haimovich A, Blum R S, et al. Spatial diversity in radars-models and detection performance [J]. IEEE Transactions on Signal Processing, 2006, 54: 823-838.

[41] Haimovich A, Blum R S, Cimini L J. MIMO radar with widely separated antennas[J]. IEEE Signal Processing Magazine, 2008, 25(1): 116-129.

[42] Zhao Shanshan, Zhang Linrang, Zhou Yu, et al. Study of multistatic radar against false targets jamming using spatial scattering properties [C]//The 14th IEEE International Conference on Computer and Information Technology. Xi′an: [s. n.], 2014.

[43] Haykin S. Cognitive radar: A way of the future[J]. IEEE Signal Processing Magazine, 2006, 23(1): 30-40.

[44] Joseph R G. Cognitive radar: The knowledge-aided fully adaptive approach[M]. Artech Norwood, MA House: 2010.

[45] 王峰，雷志勇，黄桂根，等. 雷达智能抗干扰体系研究[J]. 现代雷达，2014，36(1)：80-82.
Wang feng, Lei Zhiyong, Huang Guigen, et al. Intelligent anti-jamming technique in radar [J]. Modern Radar, 2014, 36(1): 80-82.

[46] Phillip F. Is there a role for artificial intelligence in future electronic support measures? [J]. Knowledge-Based Intelligent Information and Engineering Systems, 2006: 523-530.

[47] Butt F A, Naqvi I H, Najam A I. Radar ECCM against deception jamming: a novel approach using bistatic and mono-static radars[C]//Proc 15th Int Multitopic Conf. Islamabad: [s. n], 2012: 137-141.

作者简介：张林让(1966-)，男，教授，博士生导师，研究方向：阵列信号处理，雷达系统仿真与建模，网络化雷达协同抗干扰，E-mail: lrzhang@xidian.edu.cn；赵珊珊(1989-)，女，博士研究生，研究方向：网络化雷达协同抗欺骗式干扰；周宇(1978-)，男，副教授，研究方向：雷达波形优化设计，雷达目标和干扰环境感知；刘楠(1981-)，男，副教授，研究方向：分布式及灵巧干扰对抗；张娟(1979-)，女，副教授，研究方向：压制式及分布式干扰抑制，网络化雷达资源优化配置。