DOI:10.11918/201812119

基于检测器性能实时评估的欺骗检测融合算法

范广腾,李献斌,王 建,庹洲慧

(军事科学院 国防科技创新研究院,北京 100080)

摘 要: 随着GPS欺骗生成技术的发展,欺骗信号可以在某一些属性上与真实信号保持一致,如到达角、多普勒频移等,此时单独使用某一种欺骗干扰检测方法,将无法有效地对欺骗信号进行检测,而如果采用直接将多种欺骗检测器结果相或的方法,则检测性能将会随着某一种检测器性能下降而下降.针对不同欺骗干扰场景下,检测器检测性能实时变化且先验信息缺失的情况,本文提出性能实时评估的欺骗检测融合算法.该方法通过建立性能误差评价准则,对融合后的检测性能与单个检测器性能进行实时比较,如果发现某一个检测器性能误差超过门限,则在融合过程中剔除该检测器,从而可以保证当一种检测器失效不会影响融合后的整体性能,该方法可以适用于任意数量,任意种类的欺骗检测方法融合,本文针对相位差和载波多普勒方差两种具体的检测方法,给出了工程实现方法.最后通过仿真结果表明,性能实时评估的欺骗检测融合算法与单独检测算法以及传统融合算法相比,具有更高的检测性能和更广的适应能力.

关键词: 卫星导航;欺骗干扰;检测融合;相位差检测;多普勒方差检测

中图分类号: TN967.1 **文献标志码:** A **文章编号:** 0367-6234(2020)05-0165-06

An anti-spoofing method based on evaluating the performance of detectors in real time

FAN Guangteng, LI Xianbin, WANG Jian, TUO Zhouhui

(National Innovation Institute of Defense Technology, Academy of Military Sciences, Beijing 100080, China)

Abstract: With the development of the GPS spoofing signal generating technology, the spoofing signal can be similar to the authentic signal in such attributes as arrival angle and Doppler frequency, making it difficult to detect the spoofing signal by only employing one spoofing interference detection method. While if directly combining several methods, the detection performance will be decreased when one detector is degraded. Thus, considering that under different deception jamming scenarios, the detection performance of detectors has real-time changes and the priori information is missing, a detection fusion method is proposed in this paper to detect spoofing signals by evaluating real-time performance of detectors. By establishing the evaluation criteria for performance error, the real-time performance comparison between the proposed method and the single detector method was conducted. With this method, the degraded detector will be rejected if the performance falls down below the threshold, which can ensure that when a detector fails, it will not affect the overall performance of the fusion. This method can be applied to the fusion of any number and any kind of deception detection methods. Based on the detection methods of phase difference and carrier Doppler variance, an engineering implementation method is presented in this paper. Finally, simulation results showed that the spoofing detection fusion algorithm for real-time performance evaluation had better deception performance and wider adaptability than one detector and traditional detection fusion algorithms.

Keywords: satellite navigation; spoofing interference; detection fusion; phase difference detection; Doppler variance detection

随着卫星导航应用逐渐深入到社会生活以及军事应用的方方面面,导航接收机收到虚假信号得出错误的定时定位结果将导致重大灾难.尤其在导航战背景下,敌方有针对性施放的欺骗干扰信号可以改变无人机、导弹等载体的运动轨迹,使其到达欺骗干扰方指定的位置[1].如何有效检测欺骗干扰,从而保护己方导航接收机不受欺骗干扰影响,是当前GNSS领域的研究热点[2].

正常工作的导航接收机是自洽的,当欺骗干扰信号存在时会打破原有的参数特征.现有文献都是针对欺骗信号与真实信号在某一参数和特定属性上的区别进行设计.这些属性包括信号到达角[4]、伪距[5-6]、信号载噪比[7]、信号功率[8-9]、导航电文等[10-11].虽然这些方法对于某一类欺骗信号具有很

收稿日期: 2018-12-20
基金项目: 国家自然科学基金(61801503)
作者简介: 范广腾(1988—),男,博士,助理研究员
通信作者: 李献斌,lixianbincn@163.com

强的检测能力,但是无法适应未来导航战中欺骗模式的快速更新变化. 因此融合多种欺骗干扰检测手段是未来高可靠抗欺骗干扰导航接收机的必然选择. 由于或融合规则实现简单且可靠性高,所以在工程中得到了广泛应用,但是某种检测器性能下降时,将直接导致融合后的欺骗检测性能大幅下降. 融合检测方法在雷达领域研究较多且较为成熟,尤其是分布式检测理论的研究,所以这里参考了雷达领域信号检测相关研究成果,并结合导航领域实际应用场景,尤其是检测器性能实时变化且检测器先验信息未知的场景给出了一种性能实时评估的欺骗检测融合算法. 该方法实时评估每一种欺骗检测器的性能,一旦发现某种检测器性能下降,则在融合过程中将该检测器剔除. 在不同干扰场景下,采用该算法融合后的性能始终与参与融合中性能最优的检测器性能相当,检测适应能力大幅提高. 理论上,该方法可以适用于任意数量,任意种类的欺骗检测方法融合,但为方便说明原理,本文选取了两种常用的欺骗检测方法,即相位差检测的欺骗信号检测算法和多普勒方差检测的欺骗信号检测算法.

1 欺骗信号检测算法

1.1 相位差检测的欺骗信号检测算法

在接收机天线阵基线以及姿态条件已知的情况下(对固定安装的天线阵进行预先精密测定),通过卫星星历获取所跟踪卫星的精确位置,即可计算得到真实卫星信号到达天线阵的入射俯仰角以及方位角;通过精密时延标定,可以获取两副天线到达接收机信号处理端的时延差;再结合对接收机载波测量误差的估计,即可得到天线阵对真实卫星信号的测量相位差估计值. 将接收机对接收到的实际信号相位差测量结果与真实卫星信号的测量相位差估计值相比较,如果误差超出一定的范围即可判定为欺骗干扰信号.

不失一般性,假定接收机天线阵处于水平面上并且以两天线间连线所在方向为方位角零度位置,那么信号入射关系见图 1. 图中,A、B 为两个天线阵元所处位置,b 为天线基线长度,S 为入射信号,α 为入射信号俯仰角,β 为入射信号方位角. 根据三余弦定理,信号到达接收天线平面入射角 θ 为

$$\cos\theta = \cos\alpha\cos\beta. \tag{1}$$

可进一步改写为

$$d\varphi = |b|\cos\alpha\cos\beta + C + \gamma$$

式中:$d\varphi$ 为入射信号到两个阵元的相位差,C 为天线间的时延差,γ 为载波相位测量误差之和.

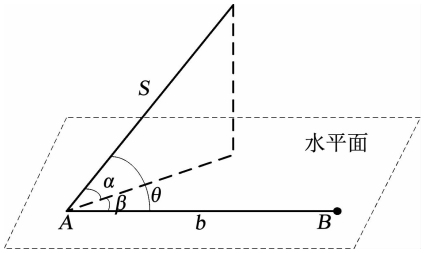

图 1 信号入射角与天线阵位置关系

Fig. 1 Relation between the incident angle of signal and the position of antenna array

即同一路信号在两副天线上表现出的相位差与天线基线长度、信号入射俯仰角以及信号入射方位角相关. 由文献[12]分析可知,天线阵载波相位差的误差源主要是天线间的时延差. 因此,对单路信号相位差检测建立检验统计量 ρ,其在真实卫星信号(假设 H0)以及欺骗干扰信号(假设 H1)条件下的概率分布为

$$\begin{cases} H0:\rho = d\varphi_{\mathrm{au}} - \hat{d\varphi} \sim N(0,\sigma), \\ H1:\rho = d\varphi_{\mathrm{sp}} - \hat{d\varphi} \sim N(d\varphi_{\mathrm{sp}} - \hat{d\varphi},\sigma). \end{cases}$$

式中:$d\varphi_{\mathrm{au}}$ 为真实信号相位测量值,$d\varphi_{\mathrm{sp}}$ 为欺骗信号相位测量值,$\hat{d\varphi}$ 为根据卫星位置和天线阵位置估算的相位值,σ 为相位差测量噪声的均方差,由此可以根据 N-P 准则,确定在一定虚警概率 P_{fa} 下的欺骗信号检测门限 ρ_{Th}

$$P_{\mathrm{fa}} = 1 - \int_{-\rho_{\mathrm{Th}}}^{\rho_{\mathrm{Th}}} p_{N(0,\sigma)}(x)\,\mathrm{d}x.$$

式中:$p_{N(0,B)}$ 为真实信号下的相位差概率密度分布函数,欺骗信号的检测概率 P_{D} 为

$$P_{\mathrm{D}} = 1 - \int_{\rho_{\mathrm{Th}}}^{\infty} p_{N(d\varphi_{\mathrm{sp}} - \hat{d\varphi},\sigma)}(x)\,\mathrm{d}x. \tag{2}$$

式中:$p_{N(d\varphi_{\mathrm{sp}} - \hat{d\varphi},B)}$ 为欺骗信号下的相位差概率密度分布函数,结合式(2)可知,单路信号相位差检测法对欺骗干扰信号的检测性能与欺骗信号入射角密切相关

$$d\varphi_{\mathrm{sp}} - \hat{d\varphi} \approx 2|b| \cdot \left|\sin\left[\frac{\theta_{\mathrm{sp}} + \theta_{\mathrm{au}}}{2}\right]\sin\left[\frac{\theta_{\mathrm{sp}} - \theta_{\mathrm{au}}}{2}\right]\right|. \tag{3}$$

式中下标 sp 与 au 分别为欺骗干扰信号和真实卫星信号. 由上式可以看出,当欺骗干扰信号与真实卫星信号的相对于接收机天线阵的入射角相同或者对称时,式(3)恒为 0,此时单路信号相位差检测无法正确鉴别欺骗信号与真实卫星信号. 同时,当欺骗信号与真实信号入射角一定的条件下,天线阵的基线长度越大,H1 条件下检验统计量的均值越大,因此天线阵基线长度越大,H0 和 H1 条件下的概率密度分布函数间隔越大,欺骗干扰检测性能越好.

1.2　载波多普勒方差检测的欺骗信号检测算法

第二种方法利用了接收机接收真实卫星信号的多普勒特性. 接收信号的多普勒是由于卫星与接收机相对运动所致，如(4)式

$$f_r = f_c\left(1 - \frac{v_r}{c}\right). \tag{4}$$

式中：f_c 为发射的载波频率，f_r 为接收机接收到的载波频率，v_r 为接收机与卫星的相对运动速度，c 为光速. 由于 GNSS 信号载波频率高，卫星速度快，因此可以产生 ±5 kHz 范围内的多普勒频偏. 如果 GNSS 接收机的晶振同样有 ±5 kHz 的频偏，则相对频偏可以达到 ±10 kHz. 对于静止终端来说，由卫星运动引起的多普勒频偏变化率最大不超过 40 Hz 每分钟，因此可以认为其多普勒频偏是线性的[13]. 对多普勒偏移测量值在一定范围加窗长度下求平均，加窗长度越长其线性度越好. 再对接收真实卫星信号的多普勒求方差，其方差在很小的范围内波动，计算方差采用矩形窗如下式

$$w(n) = \begin{cases} 1, & n \leqslant K; \\ 0, & n > K. \end{cases}$$

式中：K 为加窗长度，K 大于 100 时，其方差的波动小于 20 Hz^2，即使 K 缩小为 10 时，其方差的波动也小于 40 Hz^2. 存在欺骗信号下第 i 颗卫星的基带信号 $S_i(t)$ 为

$$S_i(t) = A_i d_i(t-\tau_i)c_i(t-\tau_i)e^{j2\pi t f_{d,i}} + A_{is} d_{si}(t-\tau_{si})c_i(t-\tau_{si})e^{j2\pi t f_{ds,i}} + \eta(t).$$

式中：A_i 为真实信号幅度，d_i 为真实信号电文，τ_i 为真实信号时延，c_i 第 i 颗卫星扩频码，$f_{d,i}$ 为真实信号多普勒，A_{is} 为欺骗信号幅度，d_{si} 为欺骗信号电文，τ_{si} 为真实信号时延，$f_{ds,i}$ 为欺骗信号多普勒，$\eta(t)$ 为噪声. 当多普勒方差超过门限则认为受到欺骗攻击.

根据文献[13]可知，接收真实信号的多普勒方差分布满足对数正态分布，因此，对载波多普勒方差检测建立检验统计量 ρ，其在真实卫星信号(假设 H0)以及欺骗干扰信号(假设 H1)条件下的概率分布为

$$\begin{cases} H0: \rho \sim \dfrac{1}{\rho\sigma\sqrt{2\pi}} e^{-(\log\rho-\mu_{au})^2/2\sigma^2}, \\ H1: \rho \sim \dfrac{1}{\rho\sigma\sqrt{2\pi}} e^{-(\log\rho-\mu_{sp})^2/2\sigma^2}. \end{cases} \tag{5}$$

由(5)式可知，当欺骗信号与真实信号多普勒差异越大，该方法的检测性能越优.

2　融合算法

欺骗信号检测算法章节中介绍的两个检测方法，分别利用了真实信号与欺骗信号在到达角和载波多普勒上的差异. 传统的融合方法只对每个检测器的检测结果进行融合，即只要其中一种方法检测结果为欺骗信号，则最终系统的检测结果即为欺骗信号，其检测框图见图 2，即为传统的分布式硬决策 N-P 检测融合系统，其中 u_1 为载波相位差检测结果，u_2 为多普勒方差检测结果，u_0 为融合后的检测结果.

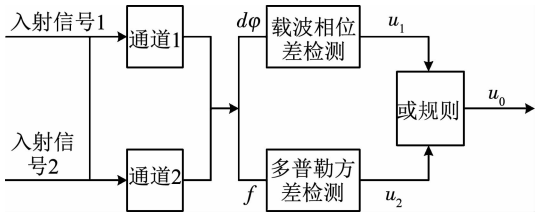

图 2　传统的检测融合方法

Fig. 2　Traditional detection fusion method

假定融合后的虚警概率为 P_f，若平均分配至每个检测器，则每个检测器虚警概率为 $1-\sqrt{1-P_f}$，总的检测概率 P_d 为

$$P_d = f_1(1-\sqrt{1-P_f}) + f_2(1-\sqrt{1-P_f}) - f_1(1-\sqrt{1-P_f})f_2(1-\sqrt{1-P_f}). \tag{6}$$

由(6)式可知，融合后的检测性能与上述两种检测方法其性能和欺骗信号的特性有关，当欺骗信号在到达角或载波多普勒方差上与真实信号比较接近时，其中一个方法的检测性能将大幅度地下降，直接采用传统的融合方法将会导致系统整体的检测性能下降，见图 3.

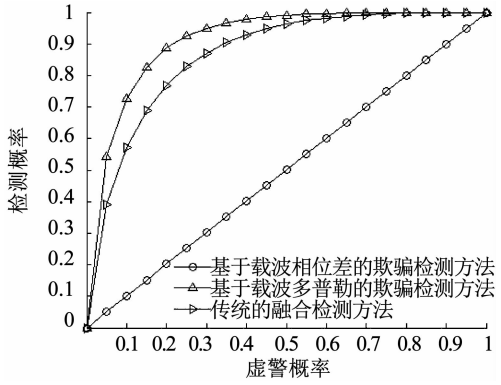

图 3　单独检测器和传统融合后检测器的性能曲线

Fig. 3　Performance curves of detector after fusion of individual and traditional detectors

图 3 中真实信号入射角为 45°，欺骗信号入射角为 46°，真实信号载波多普勒方差为 14.86 Hz^2，欺骗信号载波多普勒方差为 20.52 Hz^2. 由图 3 可知，当真实信号入射角和欺骗信号入射角非常接近时，载波相位差的欺骗检测方法基本无效. 如果此时采用传统的融合方法，系统最终的检测性能反而低于单独使用载波多普勒方差的欺骗检测方法.

基于上述原因,本文设计了性能实时评估的融合检测算法. 其基本思想为:融合算法实时对每个检测器的性能进行估计,当发现其中一个检测器性能明显较差时,系统将剔除该检测器,单独使用另一种检测器进行欺骗干扰检测. 当两种检测器性能接近时,系统将同时使用两个检测器进行欺骗干扰检测.

性能实时评估的融合检测算法是利用各检测器判决结果和传统的融合中心全局判决结果之差的最近 M 个累积平均值来判定该检测器是否可用. 具体方法如下:如果该平均值小于门限值 λ(λ 为一个 0 ~ 1之间的常数),则认为该检测器可用,否则认为不可用,将其剔除.

该误差平均值的计算如下式

$$E_i^k = \frac{1}{M}\sum_{j=K-M+1}^{K} | u_0^j - u_{i1}^j | . \tag{7}$$

性能实时评估的融合检测算法的实现框图见图 4.

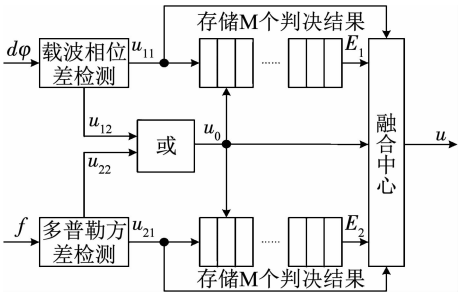

图 4 性能实时评估的检测融合方法

Fig. 4 Detection fusion method for real-time performance evaluation

其中图中采用 2 个深度为 M 的 FIFO 来存储 M 个判决结果. 下面结合图 4 具体说明该算法的实现步骤:

步骤一:设定整个系统的虚警概率为 P_f,在或规则下将 P_f 均分到两个检测器中,即两个检测器的虚警概率为 $1 - \sqrt{1 - P_f}$.

步骤二:两个检测器分别根据虚警概率 P_f 和 $1 - \sqrt{1 - P_f}$设置双门限 Th_{11}、Th_{12} 和 Th_{21}、Th_{22} 其中 Th_{11} 和 Th_{12} 是载波相位差检测器在虚警概率为 P_f 和 $1 - \sqrt{1 - P_f}$ 下的门限,Th_{21}、Th_{22} 是载波多普勒方差检测器在虚警概率为 P_f 和 $1 - \sqrt{1 - P_f}$ 下的门限.

步骤三:两个检测器把根据 Th_{11}、Th_{21} 的检测结果 u_{11} 和 u_{21} 送入存储器,同时将根据门限 Th_{12}、Th_{22} 的检测结果 u_{21} 和 u_{22} 相或的结果 u_0 送入存储器.

步骤四:根据(7)式计算每个检测器的误差平均值,将其分别与 λ 比较,判定该检测器的检测性能.

步骤五:如果两个检测器的检测性能都满足要求则采用 u_0 作为检测结果输出,否则采用 u_{11} 或者 u_{21} 作为检测结果输出.

3 性能分析

为了全面的分析该算法的性能,下面给出三种不同的应用场景:

场景一:真实信号的入射角为 45°,欺骗信号的入射角为 65°,真实信号多普勒方差均值为 14.86 Hz^2,欺骗信号多普勒方差均值为 18.93 Hz^2.

场景二:真实信号的入射角为 45°,欺骗信号的入射角为 65°,真实信号多普勒方差均值为 14.86 Hz^2,欺骗信号多普勒方差均值为 15.33 Hz^2.

场景三:真实信号的入射角为 45°,欺骗信号的入射角为 46°,真实信号多普勒方差均值为 14.86 Hz^2,欺骗信号多普勒方差均值为 18.93 Hz^2.

仿真参数设置见表 1.

表 1 仿真参数设置

Tab. 1 Setting of simulation parameters

仿真参数	仿真数值
蒙特卡罗仿真点数	100 000
双天线基线长度	1 m
天线间时延差	100 ns
载波相位方差	0.5
多普勒方差	0.0 371
判决切换门限值	0.1
积累点数	100

仿真过程中,不同虚警概率下载波相位差检测器和多普勒方差检测器的双门限见图 5、6.

下面给出 3 种不同场景下各个方法的 ROC 曲线. 其中检测器 1 为载波相位差检测方法,检测器 2 为多普勒方差检测方法.

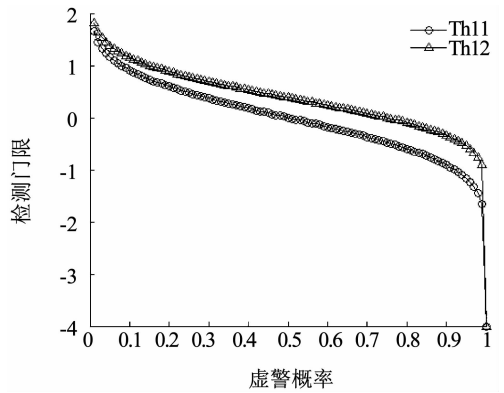

图 5 载波相位差检测器的双门限

Fig. 5 Double threshold of carrier phase difference detector

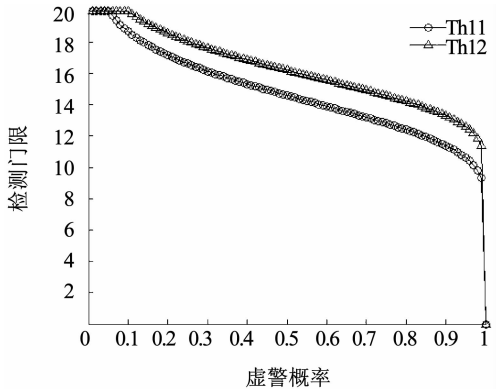

图 6　多普勒方差检测器的双门限

Fig. 6　Double threshold of Doppler variance detector

根据图 7 ~9 将不同场景下各种检测方法的性能汇总见表 2. 由表 2 可看出，在不同场景下，基于检测器性能实时评估的融合检测方法表现出良好的适应能力，在未知传感器先验信息以及传感器性能实时变化时均能保持系统整体的融合检测性能，验证了该算法性能具有很强的鲁棒性.

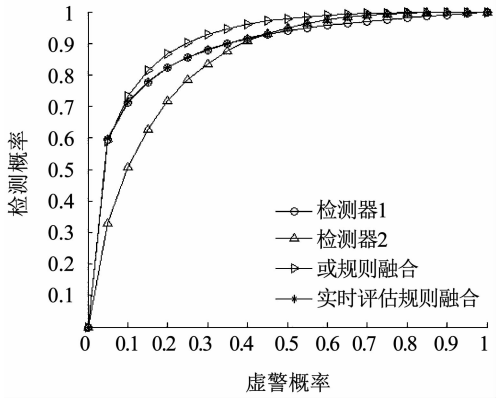

图 7　场景 1 下不同检测方法的性能比较

Fig. 7　Performance comparison of different detection methods in Scenario 1

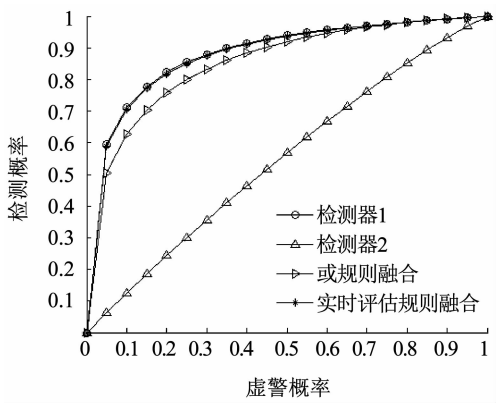

图 8　场景 2 下不同检测方法的性能比较

Fig. 8　Performance comparison of different detection methods in Scenario 2

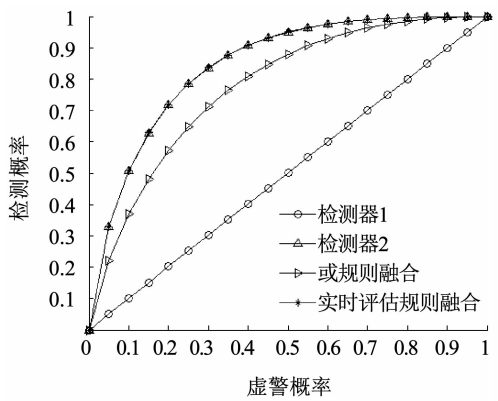

图 9　场景 3 下不同检测方法的性能比较

Fig. 9　Performance comparison of different detection methods in Scenario 3

表 2　不同场景下不同检测方法的性能比较

Tab. 2　Performance comparison of different detection methods in different scenarios

场景	载波相位差检测性能	多普勒方差检测性能	传统融合检测性能	性能实时评估的融合检测性能
1	中	中	高	高
2	高	低	中	高
3	低	高	中	高

为更好地展现实时评估规则如何对两种检测器的性能进行评估，在场景 3 中，将虚警概率设为 0. 9，分别得到载波相位观测值、多普勒方差观测值见图 10、11，由图可以看出场景 3 下载波相位观测值检测概率低，而利用多普勒方差观测值检测概率高，两个检测器输出的误差平均值 E_1 和 E_2 见图 12，可以看出检测器 1 输出的误差平均值 E_1 明显高于检测器 2 输出的误差平均值 E_2，故在融合算法中将检测器 1 的判决结果剔除，有效地保证了融合后的检测器性能.

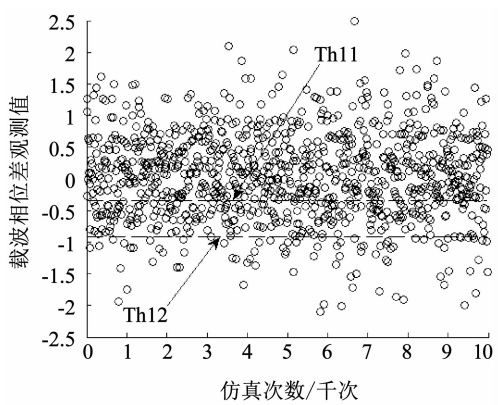

图 10　场景 3 下载波相位观测值

Fig. 10　Carrier phase observations in Scenario 3

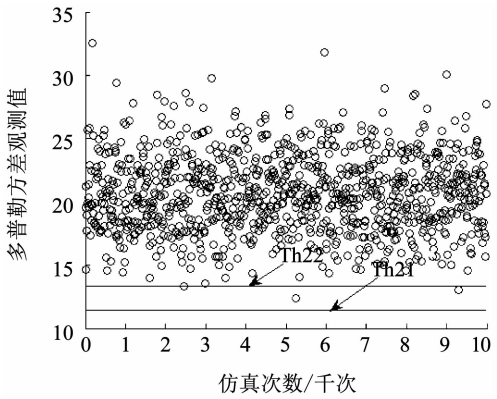

图 11 场景 3 下多普勒方差观测值

Fig. 11 Doppler variance observations in Scenario 3

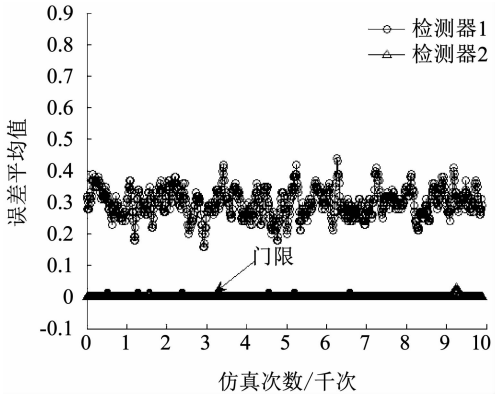

图 12 场景 3 下两个检测器的误差均值

Fig. 12 Error means of two detectors in Scenario 3

4 结 论

本文针对检测器性能实时变化且先验信息未知的欺骗干扰检测场景,提出了一种性能实时评估的欺骗检测融合算法. 通过实时评估各检测器性能,将检测性能低的检测器从融合算法中剔除,既保证了融合后的适应性,又避免因为某一个检测器性能偏低导致融合后整体性能下降. 最后本文通过仿真比较了性能实时评估的欺骗检测融合算法与单独使用到相位差检测或者载波多普勒方差检测以及传统融合算法的性能. 仿真结果表明,性能实时评估的欺骗检测融合算法与单独两种方法以及传统融合算法相比具有更高的检测性能和更广的适应能力.

参考文献

[1]张瑞华, 贾琼琼, 吴仁彪. 利用矢量跟踪环路的欺骗干扰检测与抑制方法[J]. 信号处理, 2018, 34(6): 688
ZHANG Ruihua, JIA Qiongqiong, WU Renbiao. Spoofing detection and suppression method by utilizing vector tracking loop[J]. Journal of Signal Processing, 2018, 34(6): 688. DOI:10.16798/j.issn.1003-0530.2018.06.007

[2]黄龙, 吕志成, 王飞雪. 针对卫星导航接收机的欺骗干扰研究[J]. 宇航学报, 2012, 33(7): 884
HUANG Long, LYU Zhicheng, WANG Feixue. Spoofing pattern research on GNSS receivers[J]. Journal of Astronautics, 2012, 33(7): 884. DOI:10.3873/j.issn.1000-1328.2012.07.005

[3]范广腾, 黄仰博, 伍微, 等. 惯导辅助的三元天线阵欺骗干扰检测算法[J]. 国防科技大学学报, 2017, 39(2): 91
FAN Guangteng, HUANG Yangbo, WU Wei, et al. Detection of spoofing threats by inertial assisted three elements antenna[J]. Journal of National University of Defense Technology, 2017, 39(2): 91. DOI:10.11887/j.cn.201702013

[4]DANESHMAND S, JAFARNIA-JAHROMI A, BROUMANDON A, et al. A low-complexity GPS anti-spoofing method using a multi-antenna array[C]//Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation. Nashville, Thennessee, USA:[s.n.], 2012: 1233

[5]LEDVINA B M, BENCZE W J, et al. An in-line anti-spoofing device for legacy civil GPS receivers[C]//Proceedings of the Institute of Navigation International Technical Meeting. San Diego, Calif, USA:[s.n.], 2010: 698

[6]史鹏亮, 靳文鑫, 吴舜晓. 实施转发 GNSS 欺骗干扰的选星方法研究[J]. 北京理工大学学报, 2019, 39(5): 524
SHI Pengliang, JIN Wenxin, WU Shunxiao. Research on satellite selection algorithm of GNSS repeater deception jamming[J]. Transaction of Beijing Institute of Technology, 2019, 39(5): 524. DOI:10.15918/j.tbit1001-0645.2019.05.015

[7]JAFARNIA-JAHROMI A, BROUMANDAN A, NIELSEN J, et al. GPS vulnerability to spoofing threats and a review of antispoofing techniques[J]. International Journal of Navigation & Observation, 2012, 2012(9): 1. DOI:10.1155/2012/127072

[8]PSIAKI M L, HUMPHREYS T E. GNSS spoofing and detection[J]. Proceedings of the IEEE, 2016, 104(6): 1258. DOI:10.1109/JPROC.2016.2526658

[9]胡彦逢, 边少锋, 曹可劲, 等. GNSS 接收机欺骗干扰功率控制策略[J]. 中国惯性技术学报, 2015, 23(2): 207
HU Yanfeng, BIAN Shaofeng, CAO Kejin, et al. Spoofing power control strategy for GNSS receiver[J]. Journal of Chinese Inertial Technology, 2015, 23(2):207. DOI:10.13695/j.cnki.12-1222/o3.2015.02.013

[10]HUMPHREYS T E, LEDVINA BM, PSIAKI ML, et al. Assessing the spoofing threat: Development of a portable GPS civilian spoofer[C]//Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation. Savannah, Ga, USA:[s.n.], 2008: 2341

[11]CHENG Xijun, XU Jiangning, CAO Kejin, et al. An authenticity verification scheme based on hidden messages for current civilian GPS signals[C]//Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology. Piscataway: IEEE, 2009: 345

[12]黄龙. GNSS 接收机欺骗与抗欺骗关键技术研究[D]. 长沙: 国防科技大学, 2013
HUANG Long. Study on techniques of receiver spoofing and anti-spoofing for global navigation satellite system[D]. Changsha: National University of Defense Technology, 2013

[13]JOVANOVIC A, BOTTERON C, FARINE PIERRE-ANDRÉ. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers[C]//Proceedings of Position, Location & Navigation Symposium—PLANS. Piscataway: IEEE, 2014: 1258. DOI:10.1109/PLANS.2014.6851501

(编辑 苗秀芝)