空中交通控制系统网络状态估计器安全性分析

刘建良[1]，杨建[1]，刘为夷[2]，李舟[1]

(1. 中南大学 信息科学与工程学院，湖南 长沙，410083；
2. Qualcomm Inc, Santa Clara USA, 95051)

摘要：线性状态估计器已被广泛应用于空中交通控制(ATC)系统监测和飞行器控制中。本文分析其在 GPS 欺骗、虚假数据注入和计算机病毒等网络攻击情况下的安全性。由于网络攻击很少发生，准确地对网络攻击进行建模几乎不可行。因此，分析所有可能的攻击情况，并在最坏的情况下分析状态估计器的安全性。最后进行仿真，结果显示：对于一类广泛应用的线性 α-β 估计器，提出的优化工具可识别所有可能的网络攻击中的隐蔽攻击，证明该方法的有效性。同时，方法也具有一般性，可适用于其他一些控制系统的安全性分析。

关键词：卡尔曼滤波器； 网络安全； 凸优化； 空中交通管制
中图分类号：TP393 **文献标志码**：A **文章编号**：1672−7207(2013)08−3216−07

Security analysis of state estimator of networked control systems in air traffic control

LIU Jianliang[1], YANG Jian[1], LIU Weiyi[2], LI Zhou[1]

(1. School of Information Science and Engineering, Central South University, Changsha 410083, China;
2. Qualcomm Inc, Santa Clara 95051, USA)

Abstract: The security problem of the linear state estimator was focused on, which is used for air traffic control (ATC) monitoring and aircraft tracking. Since network attacks happen rarely, it is almost impossible to accurately model them. Therefore, all possible attack cases were analyzed, and the security problem of the estimator in the worst case was studied. Simulations show that the optimization tool proposed in this work is able to diagnose most dangerous stealthy attack in all possible network attacks. Especially for a class of linear state estimator, the alpha-beta filter, the result can be widely applied. Also, the proposed novel method is general enough to be extended to the security analysis of other control systems.

Key words: Kalman filter; network security; convex optimization; air traffic control

现代控制工程的发展，促进了空中交通控制(ATC)系统的自动化和智能化。在下一代的航空运输系统中，每架飞机都会广播自己的位置、速度和飞行意图给系统中其他飞行器，其他飞行器可根据这些信息来做出相应的控制决策[1]。然而，这种基于网络的沟通和协调很容易受到来自网络的攻击。若数据被篡改，错误的数据通过其他飞行器的状态估计器后可能会造成巨大的估计误差，因为它们的决策基于错误的数据[2]。严重情况下，这将会导致危险事故。在计算机科学领域，网络系统安全性方面的研究已经有几十年的历史，但是它们不能用于诊断宏观控制系统的行为。为克服这个缺点，根据控制系统动力学模型，提出基于模型的方法，从全系统的角度来检测和诊断系统的网络攻击以分析系统安全性[3−5]。网络攻击通常具

收稿日期：2012−12−25；修回日期：2013−04−02
基金项目：中南大学高层次人才科研启动基金资助项目(7601110214)
通信作者：杨建(1978−)，男，湖北武汉人，博士，副教授，从事电力电子和运动控制研究；电话：18974880556；E-mail：jian.yang@csu.edu.cn

有智能性、隐蔽性和不确定性，近年来很多有关网络安全控制系统的研究基于博弈论和/或概率方法[6−8]。在博弈论方法中，网络攻击者(黑客)和保护者(监视软件)进行竞争和/或合作[9]。博弈论方法已广泛应用于网络协议[8, 10]和无线网络入侵检测系统中的风险评估等方面[11]。例如，通过分析 1 个系统的纳什平衡点，可评估该控制系统的稳态特性[12]。另外，概率方法可捕捉到网络攻击的不确定性[12]。因此，该方法已被应用到各种随机模型中来分析网络攻击对控制系统的影响，包括传输的数据包丢失[13]、传感器的乱码观测[14]和虚假数据注入估计等[15]。概率方法主要用来诊断针对电网状态估计器的攻击[16−17]。由于关于网络攻击控制系统的估计器研究较少，建模困难。网络中，网络攻击很少发生，使得研究者难以用一个数学模型来描述网络攻击行为。因此，本文作者不直接对网络攻击建模, 而是研究估计器对于所有可能网络攻击的响应，即：对于一个给定的状态估计器，是否存在一种隐蔽的网络攻击方式使系统紊乱而不会被控制系统中的保护机制所检测到？对于一个控制系统而言，若不被检测到，则该控制系统是不安全的，需要进一步的措施来加强保护。本文作者假定动力学系统及其传感器为带高斯噪声的线性模型，状态估计器是稳态的卡尔曼滤波器(KF)，假设检验算法被用来检测该系统是否受到网络攻击。该算法检查 KF 产生的残差的检验统计特性，这种结构具有广泛的工程应用，并可扩展到许多非线性和/或非高斯分布的情况中[18−19]。为测试状态估计器对智能网络攻击的反应，设计一个“最佳”的攻击策略，该策略能够篡改来自传感观测器的数据，促使状态估计器偏离正确的估计值而不被假设检验算法所检测到。计算“最佳”攻击策略是一个受约束的随机优化问题：通过注入一系列的虚假数据，来最大限度增加 KF 的估计错误，与此同时残差的变化不会触发假设检验算法中的警报界限；所以，KF 针对“最优”的进攻策略的响应是在状态估计器最坏的情况下对网络攻击的表现。根据最坏的情况下的表现所提供的信息，可进一步设计系统的保护措施。

1　问题描述

状态估计器是一种在飞机跟踪、导航和空中交通管制中有着广泛应用的线性估计算法。网络攻击可向观测向量中注入虚假数据，从而使状态估计值偏离真实状况。在交通管理系统中，这种偏差可能会向空中交通控制系统以及飞机提供错误的飞行信息。导致它们可能发出或者执行错误的空中交通控制(ATC)指令。为保护系统不受观测器错误数据的干扰，许多状态估计器均采取一种保护机制[18−19]。此机制通过检查残差向量中的统计特性来检测出是否有故障。然而，恶意的网络攻击可伪造观测器数据从而不被检测到。在这种危险的隐蔽攻击下，这一保护机制可能失效。

假设系统的动态特性可由下列的离散线性系统模型描述：

$$\boldsymbol{x}(k+1)=\boldsymbol{A}\boldsymbol{x}(k)+\boldsymbol{B}\boldsymbol{w}(k) \tag{1}$$

其中：$\boldsymbol{A}$ 和 $\boldsymbol{B}$ 为系统矩阵并且$(\boldsymbol{A}, \boldsymbol{B})$是可控的；$\boldsymbol{x}\in\mathbf{R}^n$ 为状态向量；$\boldsymbol{w}(k)\in\mathbf{R}^p$ 是含恒定协方差矩阵 $\boldsymbol{Q}$ 的高斯白噪声。这样的线性系统在工程中有广泛的应用。例如，它可描述交通管理系统中单架飞机的动力学特性和空中交通流量变化[20−21]。

$\boldsymbol{y}_a(k)\in\mathbf{R}^m$ 为观测器在时刻 k 受到网络攻击时的观测向量，观测模型如下式所示：

$$\boldsymbol{y}_a(k)=\boldsymbol{C}\boldsymbol{x}(k)+\boldsymbol{a}(k)+\boldsymbol{v}(k) \tag{2}$$

其中：$\boldsymbol{a}(k)\in\mathbf{R}^m$ 表示网络攻击者注入的虚假数据矢量；$\boldsymbol{v}(k)\in\mathbf{R}^m$ 是一个恒定的协方差矩阵 $\boldsymbol{R}$ 的高斯白噪声，$(\boldsymbol{A}, \boldsymbol{C})$可观测。这类观测模型可描述很多种网络攻击，如 GPS 欺骗和虚假数据注入等。

针对式(1)和(2)所给出的线性系统模型，控制器可使用线性估计器来估计系统的状态。线性估计器可由卡尔曼滤波器构成。设 $\hat{\boldsymbol{x}}(k)$ 是稳态卡尔曼滤波器(KF)给出的系统状态 $\boldsymbol{x}(k)$的估计值，稳定状态下 KF 的动力学方程如下：

$$\hat{\boldsymbol{x}}(k+1)=\boldsymbol{A}\hat{\boldsymbol{x}}(k)+\boldsymbol{K}(\boldsymbol{y}_a(k+1)-\boldsymbol{C}\boldsymbol{A}\hat{\boldsymbol{x}}(k)) \tag{3}$$

其中：$\boldsymbol{K}=P_\infty\boldsymbol{C}^{\mathrm{T}}(\boldsymbol{C}P_\infty\boldsymbol{C}^{\mathrm{T}}+R)^{-1}$ 为稳态卡尔曼增益；P_∞ 是以下代数 Riccati 方程的解。

$$P_\infty=\boldsymbol{A}P_\infty\boldsymbol{A}^{\mathrm{T}}+\boldsymbol{B}\boldsymbol{Q}\boldsymbol{B}^{\mathrm{T}}-\boldsymbol{A}P_\infty\boldsymbol{C}^{\mathrm{T}}(\boldsymbol{C}P_\infty\boldsymbol{C}^{\mathrm{T}}+R)^{-1}\boldsymbol{C}P_\infty\boldsymbol{A}^{\mathrm{T}}$$

定义估计误差 $\boldsymbol{e}(k)=\boldsymbol{x}(k)-\hat{\boldsymbol{x}}(k)$。将式(1)减去式(3)，可得

$$\boldsymbol{e}(k+1)=(\boldsymbol{A}-\boldsymbol{K}\boldsymbol{C}\boldsymbol{A})\boldsymbol{e}(k)+(\boldsymbol{B}-\boldsymbol{K}\boldsymbol{C}\boldsymbol{B})\boldsymbol{w}(k)-\boldsymbol{K}\boldsymbol{a}(k+1)-\boldsymbol{K}\boldsymbol{v}(k+1) \tag{4}$$

式(4)为估计偏差的动力学方程。假设在系统进入稳定状态之后发生攻击，即 $E[\boldsymbol{e}(0)]=0$ 并且 $E[\boldsymbol{e}(0)\boldsymbol{e}^{\mathrm{T}}(0)]=\mathrm{var}\{\boldsymbol{e}(0)\}=(\boldsymbol{I}-\boldsymbol{K}\boldsymbol{C})P_\infty$。攻击的目的是用攻击序列 $\boldsymbol{a}(k)$最大化估计偏差$\|\boldsymbol{e}(k)\|$，从而使得 KF 无法正常工作。

定义稳态 KF 的残差矢量为：

$$\boldsymbol{r}(k+1)=\boldsymbol{y}_a(k+1)-\boldsymbol{C}\boldsymbol{A}\hat{\boldsymbol{x}}(k)=$$

$$\boldsymbol{CAe}(k)+\boldsymbol{CBw}(k)+\boldsymbol{a}(k+1)+v(k+1) \tag{5}$$

若系统没有受到任何攻击，即 $\boldsymbol{a}(k)\equiv 0$，剩余的残差 $\boldsymbol{r}(k)$是一个有恒定的协方差矩阵 $P_{\mathrm{r}}=\boldsymbol{C}P_{\infty}\boldsymbol{C}^{\mathrm{T}}+R$ 的零均值高斯随机变量。若系统受到攻击，$r(k)$的统计特性会改变。随着攻击矢量 $\boldsymbol{a}(k)$攻击变化，它的平均值和/或协方差将改变。这种变化可通过假设检验算法检测，比如似然比和累加和测试。可通过测试以下 2 个互斥的统计假设来检测是否存在网络攻击[21−22]：

$$H_0: r(k)\sim N(0,P_{\mathrm{r}})\text{ 和 }\ H_1: r(k)\not\sim N(0,P_{\mathrm{r}})$$

其中：$N(\bullet)$是高斯随机变量的概率分布函数(PDF)。假设通过检查残差矢量的加权值 $\boldsymbol{r}^{\mathrm{T}}(k)P_{\mathrm{r}}^{-1}\boldsymbol{r}(k)$ 进行检验。既然 H_0 为真时 $\boldsymbol{r}^{\mathrm{T}}(k)P_{\mathrm{r}}^{-1}\boldsymbol{r}(k)$ 有一个 χ^2 分布；那么若 $\boldsymbol{r}^{\mathrm{T}}(k)P_{\mathrm{r}}^{-1}\boldsymbol{r}(k)$ 位于 χ^2 分布的末尾，则 H_0 为假。这可以通过比较 $\boldsymbol{r}^{\mathrm{T}}(k)P_{\mathrm{r}}^{-1}\boldsymbol{r}(k)$ 和一设定的阈值来实现，若状态估计权值 $\boldsymbol{r}^{\mathrm{T}}(k)P_{\mathrm{r}}^{-1}\boldsymbol{r}(k)$ 超过设定阈值，H_1 被接受，即算法检测到系统中存在可能由网络攻击带来的故障。因此，一个隐蔽攻击只要不将残差矢量的权值增加过多，就能避免被检测出来。在所有的隐蔽攻击策略中，考虑能最大化估计偏差 $\|\boldsymbol{e}(k)\|^2=E[\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{e}(k)]$，且不被检测到的网络攻击序列 $\boldsymbol{a}(k)$，k=1，2，…，T。此过程可被描述成如下最随机优化控制问题：

问题 1 在固定的时间范围 T_a 内, 从所有可能的攻击序列 $\boldsymbol{a}_{T_a}=[a(1),\cdots,a(T_a)]$ 中寻求一个攻击序列 $\boldsymbol{a}_{T_a}^{*}$ 来解决如下的有约束优化问题。

最大化：$\sum_{k=1}^{T_a}E[\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{e}(k)]$

且满足：

(1) $E[\boldsymbol{r}^{\mathrm{T}}(k)P_{\mathrm{r}}^{-1}(k)]\le\gamma$，$\forall k\in\{1,\cdots,T_a-1\}$

(2) 误差的动力学方程，见式(4)。

其中 $\gamma>0$ 是一个固定的阈值。

由于网络攻击的意图是最大限度扩大估计偏差，成功的网络攻击能向系统中注入错误的信息，使得 ATC 控制器失去对飞机实际位置的控制。当找到“最优”的网络攻击 $\boldsymbol{a}_{T_a}^{*}$ 后，对于一给定的估计器，其响应能在最坏的情况下得以评估。

2 有约束随机最优化问题的求解

2.1 随机优化问题转化为确定性最优控制问题

定义 1：$\boldsymbol{A}_K=\boldsymbol{A}-\boldsymbol{KCA}$ 和 $\boldsymbol{B}_K=\boldsymbol{B}-\boldsymbol{KCB}$，于是，式(4)可写成：

$$\boldsymbol{e}(k+1)=\boldsymbol{A}_K\boldsymbol{e}(k)+\boldsymbol{B}_K\boldsymbol{w}(k)-\boldsymbol{Ka}(k+1)-\boldsymbol{Kv}(k+1) \tag{6}$$

定义 2：$\bar{\boldsymbol{e}}(k)=E[\boldsymbol{e}(k)]$ 和 $P_e(k):=E[\boldsymbol{e}(k)\boldsymbol{e}^{\mathrm{T}}(k)]$；根据式(6)可得：

$$\bar{\boldsymbol{e}}(k+1)=\boldsymbol{A}_K\bar{\boldsymbol{e}}(k)-\boldsymbol{Ka}(k+1) \tag{7}$$

$$P_e(k+1)=\boldsymbol{A}_KP_e(k)\boldsymbol{A}_K^{\mathrm{T}}+\boldsymbol{B}_K\boldsymbol{Q}\boldsymbol{B}_K^{\mathrm{T}}+\boldsymbol{KRK}^{\mathrm{T}} \tag{8}$$

由于 KF 已经达到稳态，对任意 k 均有 $P_e(k)\equiv(\boldsymbol{I}-\boldsymbol{KC})P_{\infty}$。由上述方程可得到下式：

$$E[\boldsymbol{e}(k+1)\boldsymbol{e}^{\mathrm{T}}(K+1)]=$$

$$\mathrm{cov}\{\boldsymbol{e}(k+1),\boldsymbol{e}(k+1)\}+E[\boldsymbol{e}(k+1)]\cdot$$

$$E[\boldsymbol{e}^{\mathrm{T}}(k+1)]=(\boldsymbol{I}-\boldsymbol{KC})P_{\infty}+\boldsymbol{A}_K\bar{\boldsymbol{e}}(k)\bar{\boldsymbol{e}}^{T}(k)\boldsymbol{A}_K^{T}-$$

$$\boldsymbol{A}_K\bar{\boldsymbol{e}}(k)\boldsymbol{a}^{\mathrm{T}}(\boldsymbol{K}+1)\boldsymbol{K}^{\mathrm{T}}+\boldsymbol{Ka}(k+1)\bar{\boldsymbol{e}}^{\mathrm{T}}(k)\boldsymbol{A}_K^{T}+$$

$$\boldsymbol{Ka}(k+1)\boldsymbol{a}^{\mathrm{T}}(\boldsymbol{K}+1)\mathrm{K}^{\mathrm{T}}$$

上式可简化为：

$$E[\boldsymbol{e}(k+1)\boldsymbol{e}^{\mathrm{T}}(k+1)]=\phi(\bar{\boldsymbol{e}}(k),\boldsymbol{a}(k+1)) \tag{9}$$

其中 $\phi:\mathbf{R}^n\times\mathbf{R}^m\to S^{+}$ (S^{+}表示所有正定矩阵的集合)是一个矩阵函数。该函数定义如下：

$$\phi(\bar{\boldsymbol{e}}(k),\boldsymbol{a}(k+1))=(\boldsymbol{I}-\boldsymbol{KC})P_{\infty}+\boldsymbol{A}_K\bar{\boldsymbol{e}}^{\mathrm{T}}(k)\boldsymbol{A}_K^{\mathrm{T}}-$$

$$\boldsymbol{A}_K\bar{\boldsymbol{e}}(k)\boldsymbol{a}^{\mathrm{T}}(k+1)\boldsymbol{K}^{\mathrm{T}}-\boldsymbol{K}_a(k+1)\bar{\boldsymbol{e}}^{\mathrm{T}}(k)\boldsymbol{A}_K^{\mathrm{T}}+$$

$$\boldsymbol{Ka}(k+1)\boldsymbol{a}^{\mathrm{T}}(k+1)\boldsymbol{K}^{\mathrm{T}} \tag{10}$$

注意 S^{+}为 n 阶正定矩阵的集合，另一方面，根据式(5)可知：

$$E[\boldsymbol{r}^{\mathrm{T}}(k+1)P_{\mathrm{r}}^{-1}\boldsymbol{r}(k+1)]=E[\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{A}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}P_{\mathrm{r}}^{-1}\boldsymbol{CAe}(k)]+$$

$$E[\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{A}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}P_{\mathrm{r}}^{-1}\boldsymbol{a}(k+1)+\boldsymbol{a}^{\mathrm{T}}(k+1)P_{\mathrm{r}}^{-1}\boldsymbol{CA}E[\boldsymbol{e}(k)]]+$$

$$E[\boldsymbol{w}^{\mathrm{T}}(k)\boldsymbol{B}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}P_{\mathrm{r}}^{-1}\boldsymbol{CBw}(k)+\boldsymbol{a}^{\mathrm{T}}(k+1)P_{\mathrm{r}}^{-1}\boldsymbol{a}(k+1)+$$

$$E[\boldsymbol{v}^{\mathrm{T}}(k)P_{\mathrm{r}}^{-1}v(k)]]=\mathrm{tr}\{\sqrt{P_{\mathrm{r}}^{-1}}\boldsymbol{CA}\phi(\bar{\boldsymbol{e}}(k-1),$$

$$\boldsymbol{a}(k))\boldsymbol{A}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\sqrt{P_r^{-1}}+2\bar{\boldsymbol{e}}^{\mathrm{T}}(k)\boldsymbol{A}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}P_{\mathrm{r}}^{-1}\boldsymbol{a}(k+1)\}+$$

$$\mathrm{tr}\{\sqrt{P_{\mathrm{r}}^{-1}}\boldsymbol{CBQB}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\sqrt{P_{\mathrm{r}}^{-1}}\}+$$

$$\boldsymbol{a}^{\mathrm{T}}(k+1)P_{\mathrm{r}}^{-1}\boldsymbol{a}(k+1)+\mathrm{tr}\{\sqrt{P_{\mathrm{r}}^{-1}}R\sqrt{P_{\mathrm{r}}^{-1}}\}$$

上述方程可简化为：

$$E[\boldsymbol{r}^{\mathrm{T}}(k+1)P_{\mathrm{r}}^{-1}\boldsymbol{r}(k+1)]=$$

$$\psi(\bar{\boldsymbol{e}}(k-1),\bar{\boldsymbol{e}}(k),\boldsymbol{a}(k),\boldsymbol{a}(k+1)) \tag{11}$$

其中 $\psi:\mathbf{R}^n\times\mathbf{R}^n\times\mathbf{R}^m\times\mathbf{R}^m\to\mathbf{R}^{+}$ 是一个矩阵函数。该

函数定义如下：

$$\psi(\bar{\boldsymbol{e}}(k-1),\bar{\boldsymbol{e}}(k),\boldsymbol{a}(k),\boldsymbol{a}(k+1))=$$
$$\mathrm{tr}\{\sqrt{P_{\mathrm{r}}^{-1}}\boldsymbol{CA}\phi\left(\bar{\boldsymbol{e}}k-1,\boldsymbol{a}(k)\right)\boldsymbol{A}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\sqrt{P_{\mathrm{r}}^{-1}}\}+$$
$$2\bar{\boldsymbol{e}}^{\mathrm{T}}(k)\boldsymbol{A}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}P_{\mathrm{r}}^{-1}\boldsymbol{a}k+1+\mathrm{tr}\{\sqrt{P_{\mathrm{r}}^{-1}}\boldsymbol{CBQB}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\sqrt{P_{\mathrm{r}}^{-1}}\}+$$
$$\boldsymbol{a}^{\mathrm{T}}k+1P_{\mathrm{r}}^{-1}\boldsymbol{a}k+1+\mathrm{tr}\{\sqrt{P_{\mathrm{r}}^{-1}}R\sqrt{P_{\mathrm{r}}^{-1}}\}\qquad(12)$$

因此，**问题 1** 可转化成如下确定性最优化问题。

问题 2　在固定的时间范围 T_a，从所有可能的攻击序列中选取一个攻击序列 $\boldsymbol{a}_{T_a}^{*}$ 进行分析，如 $\boldsymbol{a}_{T_a}=[a(1),\cdots,a(T_a)]$，解决下述约束优化问题。

最小化：$-\sum_{k=1}^{T_a}\mathrm{tr}\{\phi(\bar{\boldsymbol{e}}(k-1),\boldsymbol{a}(k))\}$

且满足：

(1)　$\psi(\bar{\boldsymbol{e}}(k-1),\bar{\boldsymbol{e}}(k),\boldsymbol{a}(k),\boldsymbol{a}(k+1))\le\gamma$　，　$\forall k\in\{1,\cdots,T_a-1\}$

(2) 误差的动力学方程，见式(7)。

2.2　问题 2 最优解的 KKT 条件

定义优化变量，$\boldsymbol{X}=[\bar{\boldsymbol{e}}^{\mathrm{T}}(1)\ \boldsymbol{a}^{\mathrm{T}}(1)\ \bar{\boldsymbol{e}}^{\mathrm{T}}(2)\ \boldsymbol{a}^{\mathrm{T}}(2)\ \cdots\ \bar{\boldsymbol{e}}^{\mathrm{T}}(T_a)\ \boldsymbol{a}^{\mathrm{T}}(T_a)]^{\mathrm{T}}$，**问题 2** 可被重新描述如下：

问题 3　寻找一个最优向量 $\boldsymbol{X}^{*}$来解决含有一个不等式和约束条件的最优化问题。

最小化：$\Phi(X)$

且满足：$\Psi(X)\le 0$；FX=0

其中：

$$\Phi(X)=-\sum_{k=1}^{T_a}\mathrm{tr}\{\phi(\bar{\boldsymbol{e}}(k-1),\boldsymbol{a}(k))\}\qquad(13)$$

$$\Psi(X)=\begin{bmatrix}\psi(0,0,0,\boldsymbol{a}(1))-\gamma\\ \psi(0,\bar{\boldsymbol{e}}(1),\boldsymbol{a}(1),\boldsymbol{a}(2))-\gamma\\ \psi(\bar{\boldsymbol{e}}(1),\bar{\boldsymbol{e}}(2),\boldsymbol{a}(2),\boldsymbol{a}(3))-\gamma\\ \vdots\\ \psi(\bar{\boldsymbol{e}}(T_a-2),\bar{\boldsymbol{e}}(T_a-1),\boldsymbol{a}(T_a-1),\boldsymbol{a}(T_a))-\gamma\end{bmatrix}\qquad(14)$$

$$F=\begin{bmatrix}I & K & 0 & 0 & 0 & \cdots & 0\\ -A_K & 0 & I & K & 0 & \cdots & 0\\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots\\ 0 & \cdots & 0 & -A_K & 0 & I & K\end{bmatrix}\qquad(15)$$

引入 2 个拉格朗日乘数 $\lambda\in\mathbf{R}^{T_a-1}$ 和 $\mu\in\mathbf{R}^{T_a}$，其中 $\lambda\ge 0$。于是最优化问题 3 的拉格朗日函数表示如下：

$$L(X,\lambda,u)=\Phi(X)+\lambda^{\mathrm{T}}\Psi(X)+\mu^{\mathrm{T}}\boldsymbol{F}X\qquad(16)$$

定义 $(X^{*},\lambda^{*},\mu^{*})$ 为问题 3 对偶问题的解。KKT[23] 条件特征的对偶问题的解如下式所示：

$$\begin{cases}\left\langle\lambda^{*},\Psi(X^{*})\right\rangle=0\\ \nabla\Phi(X^{*})+\sum_{i=1}^{T_a}\lambda_i^{*}\nabla\Psi_i(X^{*})+\boldsymbol{F}^{\mathrm{T}}\mu^{*}=0\end{cases}\qquad(17)$$

其中：下标 i 表示向量的第 i 个元素。

3　仿真

针对一种应用广泛的线性状态估计器即 α-β 滤波器，采用数值的方法对约束优化问题(**问题 3**)求解。仿真结果表明：**问题 3** 的最优解不唯一，也就是说，对于一给定的估计器，成功的网络攻击策略解并不唯一。

3.1　α-β 滤波器

α-β 滤波器是一类广泛应用于空中交通管制系统跟踪和导航的线性状态估计器[20]。用 1 个例子来说明这种滤波器的设计。假设一个这样的场景：地面空中交通控制器接收从飞机发出的 ADS-B 信号，并且使用这个信号来估计飞机的高度，由于包含 GPS 测量的高度信息中含有嘈杂的干扰信号，所接收的高度测量信息必须经过过滤处理后，才能得到飞机的实际位置的准海拔高度。α-β 滤波器中使用的飞机高度动力学模型如下式所示：

$$\begin{bmatrix}h(k+1)\\ \dot{h}(k+1)\end{bmatrix}=\begin{bmatrix}1 & T_S\\ 0 & 1\end{bmatrix}\begin{bmatrix}h(k)\\ \dot{h}(k)\end{bmatrix}+\begin{bmatrix}\frac{T_s^2}{2}\\ T_s\end{bmatrix}\boldsymbol{w}(k)\qquad(18)$$

令 $\boldsymbol{x}=[h\ \ \dot{h}]^{\mathrm{T}}$，将式(1)参数化，上述方程中的 T_s=5s 为 α-β 滤波器的采样时间，并且 $\boldsymbol{w}(k)$是带有零均值和单位协方差矩阵的独立、恒等分布的高斯随机变量。观测模型如下：

$$\boldsymbol{y}(k)=\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}h(k)\\ \dot{h}(k)\end{bmatrix}+\boldsymbol{a}(k)+\boldsymbol{v}(k)\qquad(19)$$

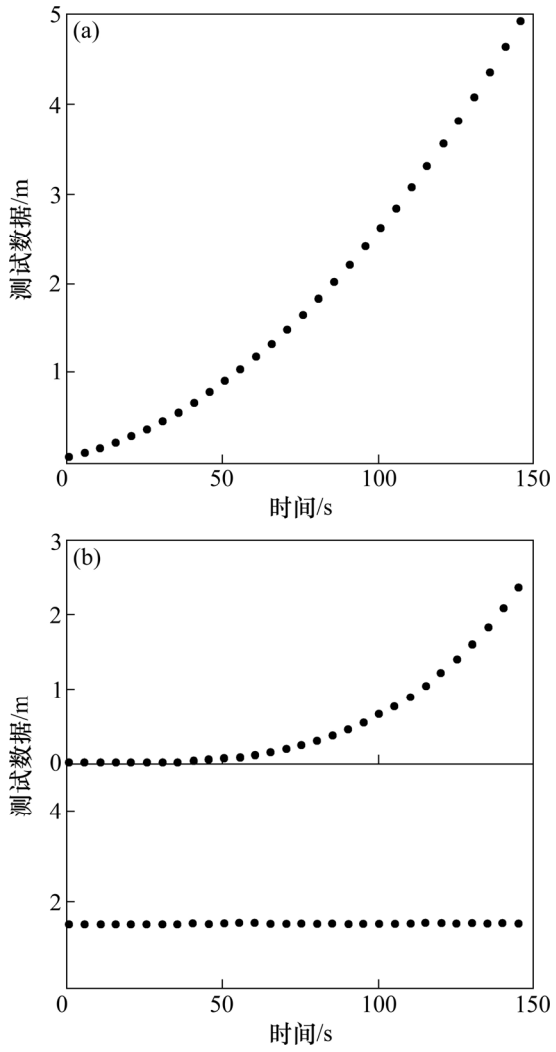
这是式(2)基于 $\boldsymbol{v}(k)$ 的一个参数化方程，该 $\boldsymbol{v}(k)$ 是恒等分布，带有一个平均值为 0 且协方差矩阵为 $\boldsymbol{R}$=300ft^2 的高斯随机变量。于是 α-β 滤波器可根据上述过程和观测模型并结合式(3)来设计。

3.2　仿真结果

在模拟仿真中，首先设置攻击序列的长度 T_a=30，即攻击序列由 30 步组成。其次设置网络攻击检测算法的阈值 γ=1.5, Matlab 中的 fmincon 函数可用来获取优化问题(**问题 3**)的数值解。由于目标函数 $\Phi(\bullet)$ 是一个凹函数，约束优化问题是一个凸优化问题并且它的解不唯一。因此，不同的初始条件，软件给出不同的数值解，这表明存在 1 个以上使估计器失效的网络攻击策略。

对于上述提到的 α-β 滤波器，数值仿真表明：对于该优化问题存在 2 个解。一个最佳的进攻策略是在不被检测发现的前提下逐步增加估计的海拔高度，从而使估计高度高于真实高度。另一个最优策略方式是采用类似的方式逐步减少估计海拔高度。图 1 和图 2 所示分别为针对最佳攻击序列 1 和 2 的优化问题的数值解。这些图分别显示了最优攻击序列 $\boldsymbol{a}(k)$、估计偏差 $E[\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{e}(k)]$ 以及检测算法 $\boldsymbol{r}^{\mathrm{T}}(k)P_{\mathrm{r}}^{-1}\boldsymbol{r}(k)$ 的统计特征。对于攻击者而言，攻击序列是采用最优的方式将错误的数据注入观测器中使得 α-β 滤波器失效。攻击序列的估计误差随时间呈指数增长，但其检验统计特性总是固定在阈值 γ=1.5 处，即最佳解在不等式约束条件 $\Psi(X)\leq 0$ 的边界上。

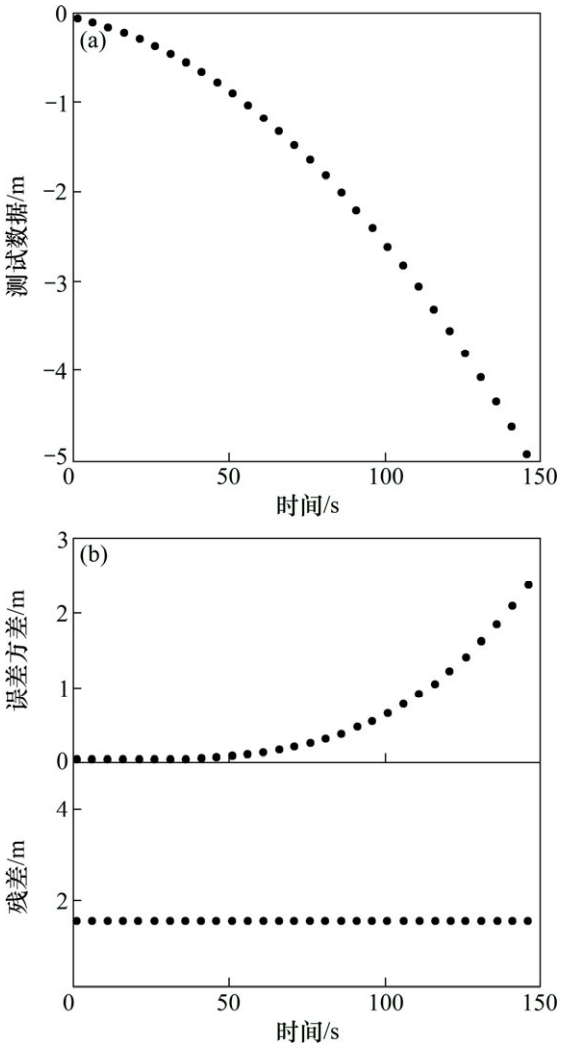
通过采用 1 000 步长的蒙特卡罗模拟仿真，比较标称系统和受到攻击的系统中的估计偏差的二次矩经验值 $E[\boldsymbol{e}^{\mathrm{T}}(k)\boldsymbol{e}(k)]$。仿真结果如图 3(a)所示。图 3(b)所示为在预设阈值 γ=1.5 处的检验统计经验值。仿真结果显示优化的网络攻击可引起大的估计误差而无法被检测到，所以 α-β 滤波器很容易受到网络攻击。此外，为证明数值解法的复杂度，针对不同的攻击序列长度，本文提出的算法可被用于解算最优攻击序列。仿真所得到的计算时间如表 1 所示。实验证明：即使解算比较长的攻击序列，本文所提出的算法时间复杂度也不高。



(a) 攻击序列；(b) 检验统计

图 1 最佳攻击序列 1

Fig. 1 Optimal attack sequence 1



(a) 攻击序列；(b) 检验统计

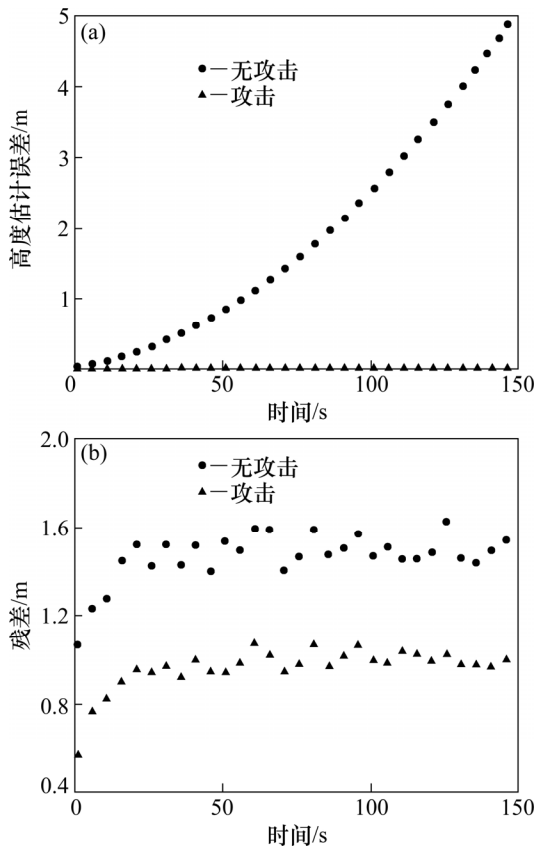
图 2 最佳攻击序列 2

Fig. 2 Optimal attack sequence 2

表 1 随攻击序列长度而变化的数值算法的计算时间

Table 1 Computational time of numberical algorithm in terms of attack sequence length

攻击序列长度 T_{a}	计算时间/s
30	0.13
60	0.93
90	2.38



(a) 高度估计误差；(b) 检验计量

图 3　蒙特卡罗模拟仿真攻击性能(1 000 步长)

Fig. 3　Attack performance with monte carlo running (1 000 steps)

4　结论

本文研究一类广泛应用于空中交通管制(ATC)系统中线性状态估计器的网络安全问题。网络攻击可通过注入虚假数据、干扰观测数据致使状态估计器给出错误估计。而在需要保障安全的 ATC 中，这是非常危险的。随机优化的目的是发现最严重的网络攻击，它可最大限度地注入错误而不被发现。KKT 条件可被推导用来解决此类最优化问题。由于最优化问题是不凸的，其解决方案可能不唯一。文中采用 2 种数值解演示 2 种典型攻击估计器的方法，显示当前使用 α-β 滤波器的 ATC 系统不能使系统免受网络攻击，从而验证本文提出的方法识别网络攻击的有效性。

参考文献：

[1]　房建成，申功勋，高洪霞. 民用导航型 C/A 码 GPS 接收机动态定位的强跟踪卡尔曼滤波研究[J]. 电子测量与仪器学报，1998, 12(2): 1−6.
FANG Jiancheng, SHEN Gongxun, GAO Hongxia. The research of strong tracking kalman filtering in kinematic positioning of civil C/A code GPS receiver for moving vehicles[J]. Journal of Electronic Measurement and Instrument, 1998, 12(2): 1−6.

[2]　房建成，申功勋，万德钧. GPS 动态定位中卡尔曼滤波模型的建立及其强跟踪算法研究[J]. 控制与决策，1997，12(6): 683−689.
FANG Jiancheng, SHEN Gongxun, WAN Dejun. A modified strong tracking kalman filter and its application in GPS Kinematic positioning for moving vehicles[J]. Control and Decision,1997, 12(6): 683−689.

[3]　郑小霞，钱锋. 动态系统故障诊断技术的研究与发展[J]. 化工自动化及仪表, 2005, 32(4): 1−7.
ZHENG Xiaoxia, QIAN Feng. Research and development of fault diagnosis methods for dynamic system[J]. Control and Instruments In Chemical Industry, 2005, 32(4): 1−7.

[4]　Ding S X. Model-based fault diagnosis techniques: Design schemes, algorithms and tools[M]. Washington: Springer, 2008: 77−124.

[5]　Nicol D, Saunders W, Trivedi K. Model-based evaluation: From dependability to security[J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 48−65.

[6]　Alpcan T, Basar T. Network security: A decision and game theoretic approach[M]. London: Cambridge University Press, 2010: 72−143.

[7]　迈尔森. 博弈论: 矛盾冲突分析[M]. 北京: 中国经济出版社, 2001.
Myerson. The game theory: Conflict analysis[M]. Beijing: The Press of China Economy, 2001: 1−104.

[8]　Lin C, Wang Y, Wang Y. A stochastic game nets based approach for network security analysis[C]//Proceedings of the 29th International Conference on Application and Theory of Petri Nets and other Models of Concurrency. Xi'an, China: Springer, 2008: 21−33.

[9]　Roy S, Ellis C, Hiva S, et al. A survey of game theory as applied to network security[C]//Boyd D. System Sciences (HICSS), 2010 43rd Hawaii International Conference on IEEE. Hawaii: Wiley Press, 2010: 1−10.

[10]　Alpcan T, Basar T. A game theoretic approach to decision and analysis in network intrusion detection[C]//Lye K. Decision and Control, 2003. Proceedings of 42nd IEEE Conference on IEEE. New York: Wiley Press, 2003: 2595−2600.

[11]　Lye K, Wing J. Game strategies in network security[J]. International Journal of Information Security, 2005, 4(1/2): 71−86.

[12]　Carin L, Cybenko G, Hughes J. Quantitative evaluation of risk for investment efficient strategies in cybersecurity: The queries methodology[J]. Computer, 2008, 41(8): 20−26.

[13] Sinopoli B, Schenato L, Franceschetti M, et al. Kalman filtering with intermittent observations[J]. IEEE Transactions on Automatic Control, 2004, 49(9): 1453−1464.

[14] Amin S, Schwartz G, Sastry S. Security of interdependent and identical networked control systems[J]. Automatica, 2012, 12(2): 12−19.

[15] Kosut O, Jia L, Thomas R J, et al. On malicious data attacks on power system state estimation[C]//Sinopoli B. Universities Power Engineering Conference (UPEC), 2010 45th International IEEE, Californnia: Springer, 2010: 1−6.

[16] Teixeira A, Amin S, Sandberg H, et al. Cyber security analysis of state estimators in electric power systems[C]//Thomas R J. Decision and Control (CDC), 2010,49th IEEE Conference on IEEE, New York: Springer, 2010: 5991−5998.

[17] Baumeister T. Literature review on smart grid cyber security[R]. University of Hawaii, 2010: 25−29.

[18] 周东华, 叶银忠. 现代故障诊断与容错控制[M]. 北京: 清华大学出版社, 2000: 54−98.
ZHOU Donghua, YE Yinzhong. Modern fault diagnosis and fault-tolerant control[M]. Beijing: Tsinghua University Press, 2000: 54−98.

[19] 张萍, 王桂增, 周东华. 动态系统的故障诊断方法[J]. 控制理论与应用, 2000, 17(2): 153−158.
ZHANG Ping, WANG Guizeng, ZHOU Donghua. Dynamic system fault diagnosis methods[J]. Control Theory and Application, 2000, 17(2): 153−158.

[20] Bar-Shalom Y, Li X R, Kirubarajan T. Estimation with applications to tracking and navigation: Theory algorithms and software[M]. New York: Wiley-Interscience, 2004: 1−153.

[21] Willsky A S. A survey of design methods for failure detection in dynamic systems[J]. Automatica, 1976, 12(6): 601−611.

[22] 杨位钦, 顾岚. 时间序列分析与动态数据建模[M]. 北京: 北京理工大学出版社, 1988: 73−189.
YANG Weiqin, GU Lan. Time series analysis and dynamic data modeling[M]. Beijing: Beijing University of Science and Technology Press, 1988: 73−189.

[23] 薛毅. 最优化理论[M]. 北京: 北京工业大学出版社, 2001: 44−219.
XUE Yi. Optimization theory[M]. Beijing: Beijing Industrial University Press, 2011: 44−219.

(编辑 邓履翔)