卫星导航系统中的最优欺骗攻击与对策

Laura Crosara、Francesco Ardizzon、Stefano Tomasin、Nicola Laurenti 信息工程系，意大利帕多瓦大学 邮箱：{crosaralau、ardizzonfr、tomasin、nil}@dei.unipd.it

arXiv:2302.01841v1 [eess.SP] 3 Feb 2023

摘要——近年来，针对全球导航卫星系统（全球导航卫星系统）的信号欺骗攻击威胁日益加剧，推动了反欺骗技术的研究。然而，现有防御方法仅针对特定攻击而设计。本文提出了一个全球导航卫星系统欺骗攻击框架的通用模型，并据此推导出最优攻击与防御策略。我们考虑这样一种情形：合法接收方（Bob）需要判断接收信号是来自多个合法空间飞行器（Alice），还是来自攻击设备（Eve）。首先，我们针对来自 Alice 的高斯传输，通过最小化欺骗检测检验可达错误概率区域的一个外界，推导出最优攻击策略。随后，我们将欺骗及其检测建模为对抗博弈，并证明高斯传输及其对应的最优攻击构成纳什均衡。最后，我们考虑 Alice 采用实用调制方案的情形，并推导出广义似然比检验。数值结果验证了解析推导，并表明可达错误区域的界能够代表实际性能。

索引词——**欺骗、全球导航卫星系统（GNSS）、信号认证、物理层安全。**

I. 引言

越来越多的基于位置的服务依赖全球导航卫星系统（GNSS）进行定位和授时，但全球导航卫星系统的广泛应用也增加了对其发动攻击的动机 [1]。具体而言，欺骗攻击是指传输伪造的类全球导航卫星系统信号，意图使接收机计算出错误的位置 [1]–[3]。最简单的欺骗技术之一是信号转发欺骗，即欺骗器将接收到的信号重新传输给受害者，使后者根据欺骗器所在位置接收到的信号计算测距估计。更高级的此类攻击会有选择地伪造延迟版本的测距信号，从而使欺骗器能够诱使受害者得到任意的位置估计。当处理受密码学保护的测距信号时，可利用安全码估计与重放攻击（SCER） [4], [5] 估计消息签名，然后根据估计结果实时重构信号。另一种称为距离缩短攻击的重放攻击 [6], ，则通过降低伪距估计来改变接收机的位置，并试图在接收符号持续时间结束前将其解码。

过去十年间，全球导航卫星系统领域一直在研究数据层和测距码层的反欺骗技术。保障距离估计意味着对信号源进行认证并保护接收信号的完整性，这需要在物理层采取措施。因此，本文聚焦于物理层认证，该方法利用通信媒介，而不依赖更高层的加密。

扩频码加密（SCE）是限制对全球导航卫星系统信号访问最可靠的方案，因为它使攻击者无法预测扩频码，从而限制其实施成功信号生成攻击的能力[7]。此外，采用SCE时，SCER攻击难以从含噪的接收信号中估计出每个扩频码片，因为码片周期通常比消息符号周期短几个数量级 [8]。SCE方案包括GPS的P(Y)码和Galileo的商业认证服务（CAS）。CAS目前仍在开发中，但预计将于2024年建成：具体而言，近期提出的一项名为辅助CAS（ACAS）的方案 [9], [10], 提供了一种SCE方法，可从伽利略开放服务导航电文认证（OS-NMA）中不可预测的签名导出加密密钥 [11], [12]。

文献 [13],提出了针对民用信号的SCE方法改进方案，概述了一种利用信号水印的扩频码认证（SCA）技术。文献 [14], 也介绍了类似的SCA技术，该技术使用短序列的扩频安全码（SSSC）来修改扩频码。这种设计方法在文献 [15], 中得到进一步发展，并应用于文献 [16], [17],提出的方案。该方案名为码片消息鲁棒认证（CHIMERA），旨在对民用GPS信号的导航数据和扩频码进行联合认证。另一种联合认证导航数据与扩频码片的方案——基于扩频码和导航数据的认证提案（SNAP），见文献 [18]；文献 [7]也提出了类似方法。文献 [19]–[21]还介绍了其他面向开放GNSS信号的SCA技术，它们采用不同的方法生成和布置水印码片。然而，现有文献中的抗欺骗机制都是针对特定问题设计的，没有采用任何最优性准则，其性能评估针对的是某些特定攻击，而这些攻击未必能代表设计机制所面临的最坏情况。

首次提出了一个统一的通用模型，用于 SCA 技术的设计、描述、评估和比较。

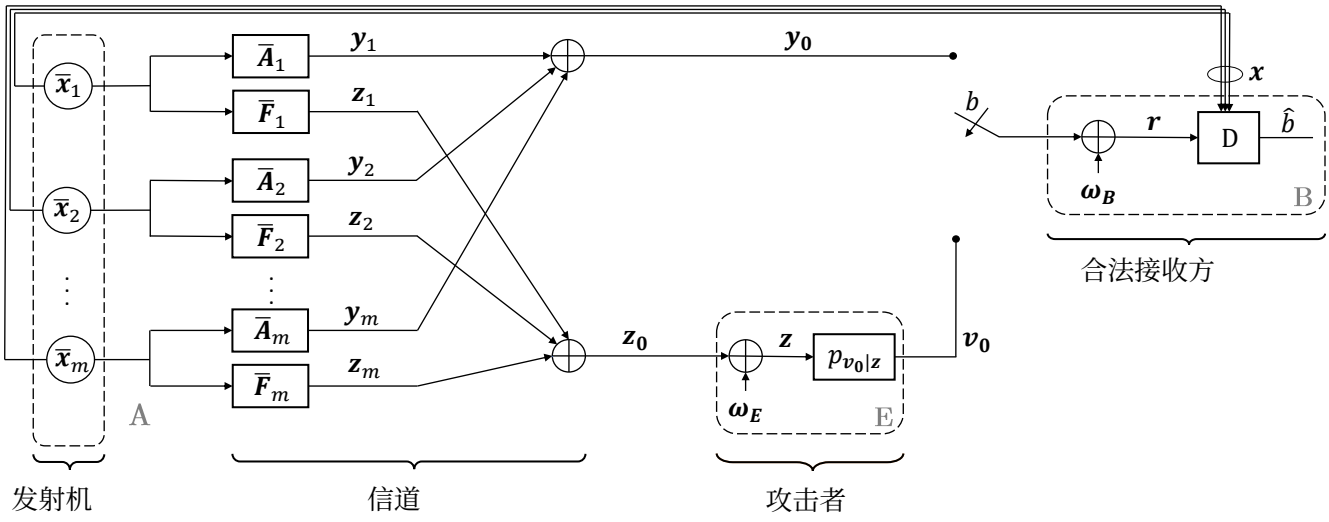


图1. 反欺骗认证模型。

在 [22]，中，在安全性与水印中随机比特的数量之间实现了最佳折衷。然而，安全性仅通过在已知公开码的条件下猜中水印码的概率来评估，因此忽略了信道传输、噪声以及可能发生的 SCER攻击所带来的影响。另一方面，[23] 提出了一种基于物理层保密的信号认证方法：导航信号与一个同步且正交的认证信号一同传输，该认证信号经过保密编码，并受到人工噪声（AN）的干扰。其总体安全性结论基于这样一点：欺骗器在不知道 AN 的情况下无法解码认证信号；之后会公开 AN 以供验证。

然而，据我们所知，目前仍缺乏一个完全通用的框架，用于推导一大类解决方案、优化其参数，并评估其针对多种攻击的安全性；本研究旨在填补这一空白。

本文的贡献如下。首先，我们提出一个通用模型，用于刻画全球导航卫星系统（GNSS）中的欺骗攻击，并考虑多个空间飞行器（SV）、受害接收机和攻击者的存在。我们描述了最优攻击策略：在对卫星信号施加预期偏移的同时，使正常条件与攻击条件下的接收信号分布之间的 Kullback-Leibler（K-L）散度最小。事实上，K-L 散度为检测误差权衡（DET）曲线提供了一个外界，该曲线由 虚警 概率和漏检 概率决定；而检测误差权衡又是评估受害接收机检测攻击能力的恰当度量。因此，所提出的优化过程无需依赖特定的检测流程，即可得出最优攻击策略，并可预先评估其有效性。

对于一类一般的攻击策略，我们推导出 K-L 散度的闭式表达式，以及一个下界该下界仅取决于全球导航卫星系统场景和信道物理参数，而与受害者采用的具体检测策略无关。随后，我们将欺骗及其检测建模为对抗博弈，并证明由高斯传输和最优攻击组成的策略集合构成该博弈的纳什均衡。此外，我们讨论了均衡点处得到的 K-L 散度。最后，我们考虑 Alice 采用实用调制方案的情形，并推导出广义似然比检验。最后，我们针对攻防方案给出仿真结果，其中考虑了似然比检验（LRT）和广义似然比检验（GLRT）两种攻击检测机制，以验证解析推导，并表明由 K-L 散度给出的可实现错误区域界能够反映实际性能。

本文其余部分安排如下。第二节详细介绍通用 GNSS 欺骗模型及其性能指标。第三节推导最优攻击策略，并给出分析结果。第四节讨论发射机和接收机两端的防御策略。随后，采用两种传输调制方式——高斯信号传输和有限基数信号传输——给出第五节的数值结果。最后，第六节总结全文。

记号：向量和矩阵分别用小写和大写粗体字母表示。符号 $\mathbf{A}^{\mathrm{H}}$表示矩阵 A 的共轭转置，而 $\mathbf{A}^{\dagger}$ 表示 A 的摩尔－彭若斯伪逆。符号 $\mathbf{I}_n$ 表示大小为 $n \times n$ 的单位矩阵，$|\mathbf{A}|$ 和$\|\mathbf{A}\|_F$ 分别表示 A 的行列式和弗罗贝尼乌斯范数。给定两个随机变量 x 和 y，p_x表示 x 的概率密度函数（pdf），$p^{x|y}$表示给定 y 时 x 的条件概率密度函数，p^{xy} 表示 x 和 y 的联合概率密度函数。若 $\mathbf{a} \in \mathbb{C}^n$ 和 $\mathbf{b} \in \mathbb{C}^m$ 是随机向量，则 $\mathbf{K}_{ab} = \mathbb{E}[\mathbf{a}\mathbf{b}^{\mathrm{H}}]$ 表示它们的 $n \times m$ 协方差

矩阵。最后，log 表示自然对数。

II. 系统模型

我们考虑由m 颗卫星组成的星座（Alice，图1中的模块 A）向接收机（Bob，图1中的模块 B）发送信号。Bob 通过估计从m 颗卫星接收到的信号之间的相对时延，并获知卫星的位置，利用测距技术 [24]估计自身位置。第三方设备（Eve，图1中的模块 E）既接收卫星发送的信号，也将这些信号转发给 Bob。Bob 的目标是验证接收信号，即确定信号来自卫星星座还是 Eve。反过来，Eve 的目标是发送一种能让 Bob 误认为是真实信号的信号，但该信号中各卫星信号之间的时延不同，从而诱导出不同的位置估计。可靠的异步侧通信信道（不能用于位置估计）使 Alice 能够向 Bob 传输经过认证的数据，以验证 GNSS信号；而 Eve 无法访问该信道来实施攻击。实现该信道的一种可行方法是采用延迟认证技术 [25]。本文研究 Alice 如何发送其信号（通过主信道和侧信道），以及 Bob 如何执行认证过程的验证步骤。此外，我们还研究 Eve 可能采用的攻击策略。

A. 传输过程

第 i 个 SV（i $\in \{1,2,\ldots, m\}$）广播一个无线电信号，其离散时间复基带等效向量表示为 $\bar{\mathrm{x}}_i \in \mathbb{C}^n$，其中 $\bar{\mathrm{x}}_i$ 与 $\bar{\mathrm{x}}_j$ 相互独立（若 i $\neq$ j）。我们将所有 SV 传输的信号连接起来，定义传输字 x：x $= [\bar{\mathrm{x}}1, \bar{\mathrm{x}}_2,\ldots, \bar{\mathrm{x}}_m] \in \mathbb{C}^{mn}$；码字 x 还通过侧信道传送给 Bob。需要注意的是，向接收机提供的侧信息也可以是传输字 x 的压缩无损版本。每个信号 $\bar{\mathrm{x}}_i$均与两个时延相关，即 $\tau_{\mathrm{B},i}$ 和 $\tau_{\mathrm{E},i}$，分别表示从第 i 个 SV 到 Bob 和 Eve 的 $\bar{\mathrm{x}}_i$ 的传播时间。不失一般性，我们假设 $\min_i\{\tau_{\mathrm{B},i}\} = \min_i\{\tau_{\mathrm{E},i}\} = 0$，因此向量 $\boldsymbol{\tau}_\mathrm{B} = [\tau_{\mathrm{B},1}, \tau_{\mathrm{B},2},\ldots, \tau_{\mathrm{B},m}]$ 和 $\boldsymbol{\tau}_\mathrm{E} = [\tau_{\mathrm{E},1}, \tau_{\mathrm{E},2},\ldots, \tau_{\mathrm{E},m}]$分别收集来自 m 颗卫星的信号之间的相对时延。此外，我们定义 $\delta_\mathrm{B} = \max_i\{\tau_{\mathrm{B},i}\}$ 和$\delta_\mathrm{E} = \max_i\{\tau_{\mathrm{E},i}\}$。

信号 $\bar{\mathrm{x}}_i$，i $\in \{1,2,\ldots, m\}$，通过两个线性信道 $\mathrm{y}_i = \mathrm{A}_i\,\bar{\mathrm{x}}_i$ 和 $\mathrm{z}_i = \mathrm{F}_i\,\bar{\mathrm{x}}_i$传输，分别向 Bob 和 Eve 提供所接收的有用信号。矩阵 A_i 和 F_i由信号之间的相对时延、衰落环境、大气参数波动、信号失真以及信道增益决定。此外，A_i 和 F_i 还包含适当的填充，以确保每个信道输出向量具有相同的大小。我们将矩阵 $\bar{\mathrm{A}}_i$ $\bar{\mathrm{F}}_i$ $= 1$ $= [\bar{\mathrm{F}}_1, \bar{\mathrm{F}}_2, \bar{\mathrm{F}}_m] \in \mathrm{A}$ 和 F $\mathbb{C}^{+\delta_\mathrm{B}\times}$ $+\delta_\mathrm{E}\times$（i，...，m）的串联分别记为 A A，A ...，A (n) (mn) 和 F $= [\bar{\mathrm{F}}1、\mathrm{F}_2,\ldots,\mathrm{F}_m] \in \mathbb{C}$(n) (mn)。

在正常条件下，Bob 接收到来自m 颗卫星的信号求和，

$$\boldsymbol{y}_0 = \sum_{i=1}^{m} \boldsymbol{y}_i = \boldsymbol{A}\boldsymbol{x}\,. \tag{1}$$

Eve 也同样如此，她获得

$$\boldsymbol{z}_0 = \sum_{i=1}^{m} \boldsymbol{z}_i = \boldsymbol{F}\boldsymbol{x}\,. \tag{2}$$

此外，$\boldsymbol{y}_0$ 和$\boldsymbol{z}_0$ 受到加性高斯白噪声（AWGN）的干扰，该噪声由两个分量相互独立、圆对称的复高斯随机向量表示，其分布分别为 $\boldsymbol{\omega}_\mathrm{B} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{K}_\mathrm{B})$ 和 $\boldsymbol{\omega}_\mathrm{E} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{K}_\mathrm{E})$，其中$\boldsymbol{K}_\mathrm{B} = 2\sigma_\mathrm{B}^2\boldsymbol{I}^{n+\delta_\mathrm{B}}$、$\boldsymbol{K}_\mathrm{E} = 2\sigma_\mathrm{E}^2\boldsymbol{I}^{n+\delta_\mathrm{E}}$以及 σ_B^2、 σ_E^2 分别是 Bob 和 Eve 接收机处复噪声各分量（实部或虚部）的方差。因此，在正常条件下 Bob 和 Eve 接收到的信号分别为

$$\boldsymbol{y} = \boldsymbol{y}_0 + \boldsymbol{\omega}_\mathrm{B}\,, \quad \boldsymbol{z} = \boldsymbol{z}_0 + \boldsymbol{\omega}_\mathrm{E}\,. \tag{3}$$

B. 攻击策略

Eve 的目标是伪造传播时间，从而引入伪造的相对时延 $\boldsymbol{\tau}_\mathrm{f} = [\tau_{\mathrm{f},1}, \tau_{\mathrm{f},2},\ldots, \tau_{\mathrm{f},m}]$，使其对应的位置可能不同于接收机的实际位置。我们假设：(i) Eve 不知道$\boldsymbol{x}$，只知道$\boldsymbol{z}$，而$\boldsymbol{z}$是$\boldsymbol{x}$的含噪声且尺寸较小的版本；(ii) Eve 知道$\boldsymbol{x}$、$\boldsymbol{y}$和$\boldsymbol{z}$的联合分布；(iii) Eve 知道链路 A $\rightarrow$B、A $\rightarrow$ E 和 E $\rightarrow$ B 的信道矩阵，以及相应的噪声统计特性。需要指出的是，攻击者无法分别处理每个卫星信号：事实上，这种处理需要知道每个码字 $\bar{\boldsymbol{x}}_i$、$i = 1$、...、m。

我们假设 Eve 可以在遭受攻击时直接设计 Bob 接收到的向量 $\boldsymbol{v}_0$，接收机噪声除外。因此，遭受攻击时 Bob 接收到的信号为

$$\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{\omega}_\mathrm{B}\,. \tag{4}$$

其中 $\boldsymbol{v}$、$\boldsymbol{v}_0 \in \mathbb{C}^{n+\delta_\mathrm{f}}$，且 $\delta_\mathrm{f} = \max \boldsymbol{\tau}_f$。

Eve 的欺骗策略可以利用其观测值 $\boldsymbol{z}$ 所携带的信息。为保持一般性，我们认为 Eve 采用由条件概率密度函数 $p_{\boldsymbol{v}_0|\boldsymbol{z}}$表征的概率策略。此外，我们假设 Eve 知道 Bob 处噪声的统计特性，因此攻击策略可以用概率密度函数 $p_{\boldsymbol{v}|\boldsymbol{z}}$ 来描述。由于观测值 $\boldsymbol{z}$ 包含了 Eve 可用于欺骗 Bob 的所有信息，我们可以得出结论：给定 $\boldsymbol{z}$后，伪造策略 $\boldsymbol{v}$ 与传输字 $\boldsymbol{x}$条件独立。

设 Bob 接收到的信号为

$$\boldsymbol{r} = \begin{cases} \boldsymbol{y} & \text{if Bob is locked on the legitimate signal } (b = 0) \\ \boldsymbol{v} & \text{if Bob is locked on the spoofing signal } (b = 1)\,, \end{cases} \tag{5}$$

其中，式 (5) 中的二元变量 b 表示合法/攻击状态。我们假设 Eve 能够完全抵消 Bob 处的信号 $\boldsymbol{y}_0$ ，从而考虑最坏情况：Bob 接收并锁定欺骗信号 $\boldsymbol{v}$ [26]。因此，Eve 旨在阻止 Bob 区分 $\boldsymbol{v}$ 与在 $\boldsymbol{\tau}_\mathrm{B} = \boldsymbol{\tau}_\mathrm{f}$ 条件下获得的合法信号 $\boldsymbol{y}$ 。

C. 认证过程

合法接收方 Bob 的目标是判断其接收到的信号 $\boldsymbol{r}$ 是对应于真实信号 $\boldsymbol{y}$，还是对应于 Eve 伪造的信号 $\boldsymbol{v}$ 。在作出这一判断时，Bob 可以利用 Alice 通过侧信道披露的 $\boldsymbol{x}$。我们指出，通过侧信道传输的消息可以是 $\boldsymbol{x}$ 的无损压缩版本。为检测欺骗攻击，Bob 执行认证测试：给定 $\boldsymbol{x}$ 和观测值 $\boldsymbol{r}$，Bob 在以下两个假设之间作出选择：

$$\mathcal{H}_0 : \boldsymbol{r} = \boldsymbol{y}\text{, the message is from Alice,} \tag{6}$$

$$\mathcal{H}_1 : \boldsymbol{r} = \boldsymbol{v}\text{, the message was forged.} \tag{7}$$

$\hat{}$ 在图1中，当$\hat{b} = b$时，即可成功验证。认证过程总结于模块D中，该模块以接收信号$\boldsymbol{r}$ 为输入，并输出布尔值$\hat{}b$。

值得注意的是，图1中的模型将文献中的已有模型作为特例纳入其中。在 [15]–[17], 提出的方案中，仅考虑了一颗卫星；令$m = 1$，即可将其纳入我们的模型。在这些方案中，扩频码的一小部分与一个秘密的密码学生成序列叠加；接收机获知密钥后，即可重现该序列。同时，导航消息数据通过对大部分或全部数据进行数字签名来保护。因此，码字$\boldsymbol{x}$ 是将经签名的导航数据与经签名的扩频码叠加后，再进行二进制相移键控（BPSK）调制所得的信号。随后，密钥相对于$\boldsymbol{x}$延迟广播，作为侧信息，使接收机能够重构$\boldsymbol{x}$。类似的方法也可用于描述 Galileo OS-NMA [11], [12],，并可结合 CAS [10]或 ACAS 功能 [9]。通过将 $\boldsymbol{x}$ 限定为二进制水印序列，并假设攻击者对此一无所知，从而去除其观测$\boldsymbol{z}$，即可将 [22] 中的模型纳入这一框架。在 [23], 的认证方案中，$\boldsymbol{x}$ 是传输的认证消息与人工噪声分量的叠加。随后，认证消息和人工噪声通过认证信道传输给合法接收方。

本章节中介绍的所有参数汇总于表I中。

D. 性能指标

认证系统的性能通过以下指标进行评估：*a)* 第一类（虚警）错误概率p_{FA}，即 Bob 将来自 Alice 的消息误判为 Eve 伪造并丢弃的概率；*b)* 第二类（漏检）错误概率 p_{MD}，即 Bob 将来自 Eve 的消息误认为合法消息并接受的概率。在给定$p_{\boldsymbol{x}}$和$p^{\boldsymbol{v}|\boldsymbol{z}}$[27]的条件下，似然比检验是使虚警概率最小化的最优检测方法。然而，通常很难通过解析方法推导这些概率密度函数。因此，可达错误概率区域的理论界有助于评估实用方案的有效性。

表I 系统参数、$i \in 1、2、...、m$

符号	定义
m	卫星数量
n	离散时间信号 $\boldsymbol{x}_i$的长度
$\boldsymbol{x}_i$	第 i 颗卫星传输的离散时间信号
$\boldsymbol{x}$	传输字
$\tau_{\mathrm{B},i}$	$\boldsymbol{x}_i$ 从第 i 颗卫星到 B 的传播时间
$\tau_{\mathrm{E},i}$	$\boldsymbol{x}_i$ 从第 i 颗卫星到 E 的传播时间
$\tau_{\mathrm{f},i}$	与 $\boldsymbol{x}_i$相关的虚假传播时间
$\boldsymbol{\tau}_{\mathrm{B}}$	从 A 到 B 的传播时间向量
$\boldsymbol{\tau}_{\mathrm{E}}$	从 A 到 E 的传播时间向量
$\boldsymbol{\tau}_{\mathrm{f}}$	E 引入的虚假传播时间向量
δ_{B}	从 A 到 B 传播的信号的最大传播时间
δ_{E}	从 A 到 E 传播的信号的最大传播时间
δ_{f}	从 E 到 B 传播的信号的最大传播时间
$\boldsymbol{A}$	A→ B 信道矩阵
$\boldsymbol{F}$	A→ E 信道矩阵
$\boldsymbol{\omega}_{\mathrm{B}}$	信道 A→ B 和 E→ B 中的加性高斯白噪声
$\boldsymbol{\omega}_{\mathrm{E}}$	信道 A→ E 中的加性高斯白噪声
σ^2_{B}	A→ B 分量信道的噪声方差
σ^2_{E}	A→ E 分量信道的噪声方差
$\boldsymbol{K}_{\mathrm{B}}$	$\boldsymbol{\omega}_{\mathrm{B}}$的协方差矩阵
$\boldsymbol{K}_{\mathrm{E}}$	$\boldsymbol{\omega}_{\mathrm{E}}$的协方差矩阵
$\boldsymbol{y}$	经过加性高斯白噪声信道 A→ B 的接收信号
$\boldsymbol{z}$	经过加性高斯白噪声信道 A→ E 的接收信号
$\boldsymbol{v}_0$	由 E 生成的信号
$\boldsymbol{v}$	经过加性高斯白噪声信道 E→ B 的接收信号
$\boldsymbol{r}$	B 接收的信号
$\hat{b}$	接收方 B 作出的决策
b	的正确值 $\hat{b}$

对于给定的攻击策略，可达错误区域的一个初始界由 K-L 散度给出。可达错误区域是在 $(p_{\mathrm{FA}},p_{\mathrm{MD}})$ 平面中所有可达点构成的集合。事实上，根据[28]和 [29] ，我们有

$$\mathbb{D}(p_{\hat{b}|\mathcal{H}_1} \| p_{\hat{b}|\mathcal{H}_0}) \leq \mathbb{D}(p_{\boldsymbol{rx}|\mathcal{H}_1} \| p_{\boldsymbol{rx}|\mathcal{H}_0}) = \mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}}). \tag{8}$$

在式 (8) 中，我们考虑了联合概率密度函数 $p_{\boldsymbol{rx}}$ ，因为我们假设在验证时，合法接收方已知$\boldsymbol{x}$，且决策 $\hat{}b$ 是基于这两个输入作出的。因此，定义函数

$$h(p_{\mathrm{MD}}, p_{\mathrm{FA}}) \triangleq p_{\mathrm{MD}} \log \frac{p_{\mathrm{MD}}}{1-p_{\mathrm{FA}}} + (1-p_{\mathrm{MD}}) \log \frac{1-p_{\mathrm{MD}}}{p_{\mathrm{FA}}}, \tag{9}$$

其中 p_{FA}、$p_{\mathrm{MD}} \in [0,1]$，并注意到 $p^{\hat{b}|\mathcal{H}_0}(1) = p_{\mathrm{FA}}$、$p^{\hat{b}|\mathcal{H}_0}(0) = 1 - p_{\mathrm{FA}}$、$p^{\hat{b}|\mathcal{H}_1}(1) = 1 - p_{\mathrm{MD}}$，以及 $p^{\hat{b}|\mathcal{H}_1}(0) = p_{\mathrm{MD}}$，式 (8) 可改写为

$$h(p_{\mathrm{MD}}, p_{\mathrm{FA}}) \leq \mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}}). \tag{10}$$

这限制了可实现的$(p_{\mathrm{FA}},p_{\mathrm{MD}})$ 取值范围，该范围取决于 $\mathbb{D}(p_{\boldsymbol{xv}} \| p^{\boldsymbol{xy}})$，且适用于任意决策机制选择。 [1]

一方面，攻击者 Eve 的目标是通过采用攻击策略 $p^{\boldsymbol{v}|\boldsymbol{z}}$，尽可能缩小 $\mathbb{D}(p_{\boldsymbol{xv}} \| p^{\boldsymbol{xy}})$ 的值，从而缩小可实现区域。另一方面，Alice 旨在通过适当选择传输字的分布来扩大可实现区域

[1]当 Bob 知道 Eve 的攻击策略而 Eve 不知道 Bob 的防御策略时，式 (10) 中的界是紧的；不过，在我们关注的情况下，该界同样成立：Bob 不知道 Eve 会采取什么行动，而 Eve 知道 Bob 会采取什么行动。

$\boldsymbol{x}$ ，以增大 $\mathbb{D}(p_{\boldsymbol{xv}}\|p^{\boldsymbol{xy}})$。因此，防御策略由概率密度函数 $p_{\boldsymbol{x}}$定义。

度量 $\mathbb{D}\left(p_{\boldsymbol{xv}}\|p^{\boldsymbol{xy}}\right)$ 可以用攻击和防御策略表示为

$$\begin{aligned}\mathbb{D}(p_{\boldsymbol{xv}}\|p_{\boldsymbol{xy}}) &= \iint p_{\boldsymbol{x}}(a)p_{\boldsymbol{v}|\boldsymbol{x}}(b|a)\log\frac{p_{\boldsymbol{v}|\boldsymbol{x}}(b|a)}{p_{\boldsymbol{y}|\boldsymbol{x}}(b|a)}\mathrm{d}a\,\mathrm{d}b\\ &= \iint p_{\boldsymbol{x}}(a)\int p_{\boldsymbol{v}|\boldsymbol{z}}(b|c)p_{\boldsymbol{z}|\boldsymbol{x}}(c|a)\,\mathrm{d}c\\ &\quad\cdot\log\frac{\int p_{\boldsymbol{v}|\boldsymbol{z}}(b|c)p_{\boldsymbol{z}|\boldsymbol{x}}(c|a)\mathrm{d}c}{p_{\boldsymbol{y}|\boldsymbol{x}}(b|a)}\,\mathrm{d}a\,\mathrm{d}b\,. \quad (11)\end{aligned}$$

为突出攻击和防御策略的作用，我们定义

$$f(p_{\boldsymbol{x}},p_{\boldsymbol{v}|\boldsymbol{z}})\triangleq\mathbb{D}(p_{\boldsymbol{xv}}\|p_{\boldsymbol{xy}})\,, \quad (12)$$

在信道 $p^{\boldsymbol{y}|\boldsymbol{x}}$ 和 $p^{\boldsymbol{z}|\boldsymbol{x}}$固定的情况下。因此，从防御方的角度来看，本文要解决的问题可定义为以下极大极小问题:

$$\max_{p_{\boldsymbol{x}}}\min_{p_{\boldsymbol{v}|\boldsymbol{z}}} f(p_{\boldsymbol{x}},p_{\boldsymbol{v}|\boldsymbol{z}}). \quad (13)$$

攻击策略与防御策略的一个重要区别在于，Eve 准确知道 $\boldsymbol{\tau}_{\mathrm{E}}$ 和受害者位置，而 Alice 的防御策略则必须针对所有可能的接收机和信道实现保持稳健且对称，这些实现由矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{F}$描述。

在第三节中，我们将首先根据第二节中提出的模型，假设 $\boldsymbol{x}$ 服从高斯分布，并讨论式（13）中的内层最小化。然后，在讨论可实现的 K-L 散度值之后，最后将在第四节研究式（13）中的最大化问题。

III. 攻击策略

现在我们聚焦于攻击策略优化，即根据式（13），旨在推导条件概率密度函数 $p^{\boldsymbol{v}|\boldsymbol{z}}$ ，使得

$$p^{\star}_{\boldsymbol{v}|\boldsymbol{z}}=\arg\min_{p_{\boldsymbol{v}|\boldsymbol{z}}} f(p_{\boldsymbol{x}},p_{\boldsymbol{v}|\boldsymbol{z}})\,. \quad (14)$$

我们假设$\boldsymbol{x}$ 是一个零均值高斯随机向量，因此$p_{\boldsymbol{x}}\sim\mathcal{N}(\boldsymbol{0},\boldsymbol{K}_{\boldsymbol{x}})$，并将在第IV-A节证明这一选择的最优性。在此假设下，如 [30], 所证明的，存在一种最优攻击$p^{\star}{}_{\boldsymbol{v}|\boldsymbol{z}}$ ，使式（12）中的散度最小。

定理 1. 给定零均值联合高斯随机向量$\boldsymbol{x}$、$\boldsymbol{y}$和$\boldsymbol{z}$，在信道 $p^{\boldsymbol{y}|\boldsymbol{x}}$ 和 $p^{\boldsymbol{z}|\boldsymbol{x}}$固定，且随机向量$\boldsymbol{v}$ 与$\boldsymbol{x}$ 在给定$\boldsymbol{z}$的条件下相互独立的约束下，使式（*12*）中的散度最小的最优攻击 $p^{\star}{}_{\boldsymbol{v}|\boldsymbol{z}}$ 属于以下类别

$$\mathcal{C}=\left\{p_{\boldsymbol{v}|\boldsymbol{z}}\sim\mathcal{N}(\boldsymbol{G}\boldsymbol{z},\,\boldsymbol{C}\boldsymbol{C}^{\mathrm{H}}+\boldsymbol{K}_{\mathrm{B}})\right\}, \quad (15)$$

因此可以将其写成$\boldsymbol{z}$的线性变换，加上相互独立的加性白色复高斯噪声，即

$$\boldsymbol{v}=\boldsymbol{G}\boldsymbol{z}+\boldsymbol{C}\boldsymbol{\omega}_{\mathrm{c}}+\boldsymbol{\omega}_{\mathrm{B}}, \quad (16)$$

其中$\boldsymbol{G}\in\mathbb{C}^{(n+\delta_{\mathrm{f}})\times(n+\delta_{\mathrm{E}})}$，$\boldsymbol{C}\in\mathbb{C}^{(n+\delta_{\mathrm{f}})\times(n+\delta_{\mathrm{f}})}$。

证明。 见 [30,定理 2]。 □

具体而言，通过对$\boldsymbol{G}$ 和$\boldsymbol{C}$进行优化，计算出满足式（14）的概率密度函数$p^{\star}{}_{\boldsymbol{v}|\boldsymbol{z}}$ ，因此式（14）变为

$$(\boldsymbol{G}^{\star},\boldsymbol{C}^{\star})=\arg\min_{\boldsymbol{G},\boldsymbol{C}} f(p_{\boldsymbol{x}},p_{\boldsymbol{v}|\boldsymbol{z}})\,. \quad (17)$$

目前定义的信号的方差矩阵和协方差矩阵为

$$\begin{aligned}\boldsymbol{K}_{\boldsymbol{xy}}&=\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{A}^{\mathrm{H}}\,, &(18a)\\ \boldsymbol{K}_{\boldsymbol{y}}&=\boldsymbol{A}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{A}^{\mathrm{H}}+\boldsymbol{K}_{\mathrm{B}}\,, &(18b)\\ \boldsymbol{K}_{\boldsymbol{xz}}&=\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}\,, &(18c)\\ \boldsymbol{K}_{\boldsymbol{z}}&=\boldsymbol{F}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}+\boldsymbol{K}_{\mathrm{E}}\,, &(18d)\\ \boldsymbol{K}_{\boldsymbol{xv}}&=\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}}\,, &(18e)\\ \boldsymbol{K}_{\boldsymbol{v}}&=\boldsymbol{G}\boldsymbol{F}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}\boldsymbol{G}^{\mathrm{H}}+\boldsymbol{G}\boldsymbol{K}_{\mathrm{E}}\boldsymbol{G}^{\mathrm{H}}+\boldsymbol{C}\boldsymbol{C}^{\mathrm{H}}+\boldsymbol{K}_{\mathrm{B}}\,, &(18f)\end{aligned}$$

考虑式（18）并按照 [30], 的推导，最优矩阵为

$$\boldsymbol{G}^{\star}=\boldsymbol{A}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}}(\boldsymbol{F}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{F}^{\mathrm{H}})^{\dagger}\,, \quad (19)$$

以及$\boldsymbol{C}^{\star}\in\mathbb{C}^{(n+\delta_{\mathrm{f}})\times(n+\delta_{\mathrm{f}})}$ 是信号$\boldsymbol{v}_0$ 在给定$\boldsymbol{z}$条件下的协方差矩阵$\boldsymbol{K}_{\boldsymbol{v}_0|\boldsymbol{z}}$ 的平方根。如 [30], $\boldsymbol{C}^{\star}$所述，其可通过闭式表达式或迭代过程获得。

$\mathcal{C}$中的 *A.* 攻击的 *K-L* 散度

在本章节中，当$p_{\boldsymbol{x}}$ 为具有协方差矩阵$\boldsymbol{K}_{\boldsymbol{x}}$的通用概率密度函数（pdf）时，我们将推导$f(p_{\boldsymbol{x}},\ p^{\boldsymbol{v}|\boldsymbol{z}})$ 的解析表达式。在假设$p_{\boldsymbol{v}|\boldsymbol{z}}\in\mathcal{C}$的条件下，定义$\boldsymbol{B}\triangleq\boldsymbol{G}\boldsymbol{F}$和 $\boldsymbol{\eta}\triangleq\boldsymbol{G}\boldsymbol{\omega}_{\mathrm{E}}+\boldsymbol{C}\boldsymbol{\omega}_{\mathrm{c}}+\boldsymbol{\omega}_{\mathrm{B}}$, $\boldsymbol{v}$ 可写为（见式（16））

$$\boldsymbol{v}=\boldsymbol{B}\boldsymbol{x}+\boldsymbol{\eta}\,, \quad (20)$$

with

$$\boldsymbol{\eta}\sim\mathcal{N}(\boldsymbol{0},\boldsymbol{K}_{\boldsymbol{\eta}})\,,\ \boldsymbol{K}_{\boldsymbol{\eta}}=\boldsymbol{G}\boldsymbol{K}_{\mathrm{E}}\boldsymbol{G}^{\mathrm{H}}+\boldsymbol{C}\boldsymbol{C}^{\mathrm{H}}+\boldsymbol{K}_{\mathrm{B}}\,. \quad (21)$$

根据式（20）中给出的$\boldsymbol{v}$ 定义，一般分布$p_{\boldsymbol{x}}$ 和$p_{\boldsymbol{v}|\boldsymbol{z}}\in\mathcal{C}$ 的度量$f(p_{\boldsymbol{x}},\ p^{\boldsymbol{v}|\boldsymbol{z}})$ 可计算为

$$\begin{aligned}f(p_{\boldsymbol{x}},p_{\boldsymbol{v}|\boldsymbol{z}}) &= \mathbb{E}\left[\log\frac{p_{\boldsymbol{xv}}(\boldsymbol{x},\boldsymbol{v})}{p_{\boldsymbol{xy}}(\boldsymbol{x},\boldsymbol{v})}\right]=\mathbb{E}\left[\log\frac{p_{\boldsymbol{v}|\boldsymbol{x}}(\boldsymbol{v}|\boldsymbol{x})}{p_{\boldsymbol{y}|\boldsymbol{x}}(\boldsymbol{v}|\boldsymbol{x})}\right]\\ &=\mathbb{E}\left[\log\frac{p_{\boldsymbol{\eta}}(\boldsymbol{v}-\boldsymbol{B}\boldsymbol{x})}{p_{\boldsymbol{\omega}_{\mathrm{B}}}(\boldsymbol{v}-\boldsymbol{A}\boldsymbol{x})}\right]=\mathbb{E}\left[\log\frac{p_{\boldsymbol{\eta}}(\boldsymbol{\eta})}{p_{\boldsymbol{\omega}_{\mathrm{B}}}(\boldsymbol{\eta}-(\boldsymbol{A}-\boldsymbol{B})\boldsymbol{x})}\right]\\ &=\mathbb{E}\left[\log\frac{p_{\boldsymbol{\eta}}(\boldsymbol{\eta})}{p_{\boldsymbol{\omega}_{\mathrm{B}}}(\boldsymbol{\eta})}\right]+\mathbb{E}\left[\log\frac{p_{\boldsymbol{\omega}_{\mathrm{B}}}(\boldsymbol{\eta})}{p_{\boldsymbol{\omega}_{\mathrm{B}}}(\boldsymbol{\eta}-(\boldsymbol{A}-\boldsymbol{B})\boldsymbol{x})}\right]\\ &=\mathbb{D}(p_{\boldsymbol{\eta}}\|p_{\boldsymbol{\omega}_{\mathrm{B}}})+\mathbb{E}\left[((\boldsymbol{A}-\boldsymbol{B})x)^{\mathrm{H}}{\boldsymbol{K}_{\mathrm{B}}}^{-1}(\boldsymbol{A}-\boldsymbol{B})x\right]\\ &=\frac{1}{2}\log\frac{|\boldsymbol{K}_{\mathrm{B}}|}{|\boldsymbol{K}_{\boldsymbol{\eta}}|}+\frac{1}{2}\operatorname{tr}(\boldsymbol{K}_{\boldsymbol{\eta}}{\boldsymbol{K}_{\mathrm{B}}}^{-1})-\frac{(n+\delta_{\mathrm{f}})}{2}\\ &\quad+\frac{1}{2}\left[\operatorname{tr}\left((\boldsymbol{B}-\boldsymbol{A})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{B}-\boldsymbol{A})^{\mathrm{H}}{\boldsymbol{K}_{\mathrm{B}}}^{-1}\right)\right]\\ &=\frac{1}{2}\left[\sum_{i=1}^{n+\delta_{\mathrm{f}}}\left(\frac{\lambda_i}{\sigma_{\mathrm{B}}^2}-\log\left(\frac{\lambda_i}{\sigma_{\mathrm{B}}^2}\right)\right)-(n+\delta_{\mathrm{f}})\right]\\ &\quad+\frac{1}{2\sigma_{\mathrm{B}}^2}\operatorname{tr}\left((\boldsymbol{B}-\boldsymbol{A})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{B}-\boldsymbol{A})^{\mathrm{H}}\right), \quad (22)\end{aligned}$$

其中，λ_i、$i \in \{1,2,\ldots\ldots, n+\delta_f\}$是$\boldsymbol{K}_{\boldsymbol{\eta}}$的特征值。我们注意到，只要攻击概率密度函数$p_{v|z}$ 取自 $\mathcal{C}$，式（22）就对任意分布p_x成立。

为方便起见，我们分别分析式（22）中的两项

$$t_1 = \frac{1}{2}\left[\sum_{i=1}^{n+\delta_f}\left(\frac{\lambda_i}{\sigma_B^2} - \log\left(\frac{\lambda_i}{\sigma_B^2}\right)\right) - (n+\delta_f)\right], \quad (23)$$

$$t_2 = \frac{1}{2\sigma_B^2}\,\mathrm{tr}\left((\boldsymbol{B}-\boldsymbol{A})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{B}-\boldsymbol{A})^{\mathrm{H}}\right). \quad (24)$$

由于$c - 1 \geq \log c, \quad \forall c \in \mathbb{R}^+$，因此可以断定，$t_1$ 中的每一项求和结果均为非负。此外，当且仅当 $\lambda_i/\sigma_B^2 = 1, \quad \forall i \in \{1,2,\ldots\ldots, n+\delta_f\}$时，$t_1 = 0$ 成立；也就是说，当且仅当攻击者成功构造出$\boldsymbol{K}_{\boldsymbol{\eta}} = \boldsymbol{K}_B$时，$t_1 = 0$ 成立。另一方面，式（22）中的t_2 与攻击者噪声 $\boldsymbol{\omega}_E$无关，因为它不依赖于$\boldsymbol{K}_{\boldsymbol{\eta}}$，而是取决于协方差矩阵$\boldsymbol{K}_{\boldsymbol{x}}$、标称情况下的合法接收机噪声功率 σ_B^2以及差值$\boldsymbol{A}-\boldsymbol{B}$，其中$\boldsymbol{A}$ 和$\boldsymbol{B}$分别为真实信道矩阵和伪造信道矩阵。因此，以下不等式成立

$$f(p_x, p_{v|z}) \geq t_2\,, \ \forall p_{v|z} \in \mathcal{C}\,. \quad (25)$$

B. 最优攻击下的*K-L*散度

由式（22）和（25）可知，对于具有协方差矩阵$\boldsymbol{K}_{\boldsymbol{x}}$的一般$p_x$ ，一旦$\boldsymbol{A}$、$\boldsymbol{K}_{\boldsymbol{x}}$和 σ_B^2 的取值确定，K-L 散度的下界可表示为$\boldsymbol{B}$ 的函数：

$$\mathbb{D}_{min}(\boldsymbol{B}) \triangleq \frac{1}{2\sigma_B^2}\,\mathrm{tr}\left((\boldsymbol{B}-\boldsymbol{A})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{B}-\boldsymbol{A})^{\mathrm{H}}\right). \quad (26)$$

特别是，当攻击者成功构造出$\boldsymbol{K}_{\boldsymbol{\eta}} = \boldsymbol{K}_B$时，则$t_1 = 0$，并且

$$f(p_x, p^{\star}_{v|z}) = \mathbb{D}_{min}(\boldsymbol{B}^{\star})\,. \quad (27)$$

值得注意的是，对于固定的$\boldsymbol{K}_{\boldsymbol{x}}$，无论$p_x$的形状如何，$p^{\star}_{v|z}$ 在所有可能的攻击策略$p_{v|z} \in \mathcal{C}$中实现最小的 K-L 散度，因此

$$f(p_x, p_{v|z}) \geq f(p_x, p^{\star}_{v|z}), \ \forall\, p_{v|z} \in \mathcal{C}. \quad (28)$$

特别是，当$\boldsymbol{K}_{\boldsymbol{x}} = M_x\boldsymbol{I}_{mn}$ （如第IV-A节进一步讨论的那样），$\mathbb{D}_{min}(\boldsymbol{B})$ 可以写为

$$\mathbb{D}_{min}(\boldsymbol{B}) = \frac{M_x}{2\sigma_B^2}\,\|\boldsymbol{A}-\boldsymbol{B}\|_F^2 = \frac{mn}{2}\,k\,\Lambda_{AB}\,, \quad (29)$$

其中

$$k = \frac{\|\boldsymbol{A}-\boldsymbol{B}\|_F^2}{\|\boldsymbol{A}\|_F^2} \quad (30)$$

表示$\boldsymbol{A}$ 与$\boldsymbol{B}$之间的分集指数，并且

$$\Lambda_{AB} = \frac{M_x}{\sigma_B^2}\,\frac{\|\boldsymbol{A}\|_F^2}{mn}\,, \quad (31)$$

表示 Bob 处的平均接收信号信噪比（SNR）。值得注意的是，攻击者总是可以选择$\boldsymbol{G}$使得$k \leq 1$ （只需简单地设置$\boldsymbol{G} = 0$，我们便有$k = 1$）。此外，在（31）中，该项

$$\frac{\|\boldsymbol{A}\|_F^2}{mn} = \frac{1}{m}\sum_{i=1}^{m}\frac{1}{n}\|\boldsymbol{A}\|_F^2 \quad (32)$$

表示合法信道的m 个冲激响应的平均能量。因此，(29) 根据m 个发射信号的总长度（mn）、信道矩阵之间的差异度量（k）以及合法信道$\boldsymbol{A}$ 的信噪比来描述 $\mathbb{D}_{min}(\boldsymbol{B})$，其中$\boldsymbol{B}$ 是伪造信道矩阵，$A \to B$ （Λ_{AB}）。

C. 极限情形

现在讨论一些极限情形，在这些情形中，所考虑的欺骗攻击与合法信号完全不可区分，因此无法检测：

S1: $\boldsymbol{A} = \boldsymbol{F}$，即 Eve 发起信号转发欺骗攻击，将自身的位置诱导到 Bob 所在的位置；**S2:** $m = 1$，此时 Eve 和 Bob 都只接收到来自一颗卫星的信号，因此缺乏足够的多样性；**S3:** 信道 A $\to$B 相对于信道 A $\to$E 是随机退化的。

在以下分析中，我们假设攻击者 Eve 使用最优攻击策略$p^{\star}_{v|z}$。

在情形 **S1** 中，其中 $\boldsymbol{A} = \boldsymbol{F}$，我们有 $\delta_E = \delta_B = \delta_f = \delta$。根据 (19)，Eve 得到 $\boldsymbol{G}^{\star} = \boldsymbol{I}_{n+\delta}$，因此 $\boldsymbol{B}^{\star} = \boldsymbol{G}^{\star}\boldsymbol{F} = \boldsymbol{F}$，且 $\boldsymbol{B}^{\star} = \boldsymbol{F} = \boldsymbol{A}$，这意味着 $\mathbb{D}_{min}(\boldsymbol{B}^{\star}) = 0$。因此，在该模型中无法检测到信号转发欺骗攻击。

在情形**S2** 中，我们假设$m = 1$。这意味着 $\delta_E = \delta_B = \delta_f = 0$，因此$\boldsymbol{A}$ 和$\boldsymbol{F}$ 均可左逆。因此，当$\boldsymbol{G}^{\star}$ 按式（19）计算时，Eve 将得到$\boldsymbol{B}^{\star} = \boldsymbol{G}^{\star}\boldsymbol{F} = \boldsymbol{A}$，这意味着 $\mathbb{D}_{min}(\boldsymbol{B}^{\star}) = 0$。因此，为了得到 $\mathbb{D}_{min}(\boldsymbol{B}^{\star}) > 0$，Bob 必须合并来自$m > 1$ 颗卫星的信号。不过，这也是全球导航卫星系统接收机计算位置、速度和时间（PVT）解的必要条件。

在情形 S3 中，信道 A $\to$ B（由条件概率密度函数 $p_{y|x}$ 表示）可以分解为 $p_{z|x}$ 与适当选取的 $p_{y|z'}$ 的级联。因此，在这种情况下，Eve 可以选择 $p_{v|z} = p_{y|z'}$，以获得 $p_{y|x} = p_{v|x}$。此外，我们有 $\mathrm{y} = \mathrm{G}'\mathrm{z}' + \mathrm{C}'\boldsymbol{\omega}_c$，而 Eve 选择 $\mathrm{G}^{\star} = \mathrm{G}'$ 和 $\mathrm{C}^{\star} = \mathrm{C}'$，使得 $\mathrm{B}^{\star} = \mathrm{A}$ 且 $\mathbb{D}_{min}(\mathrm{B}^{\star}) = 0$。因此，在这种情况下，这种攻击不会被检测到。

当$m > 1$、$\boldsymbol{A} \neq \boldsymbol{F}$ 和 $\sigma_E^2 > 0$时，会出现更一般、也更现实的欺骗场景。此外，场景**S3** 中的假设非常悲观。因此，在现实场景中，若进一步假设 $\ker(A) \nsubseteq \ker(F)$，则总能保证 $\mathbb{D}_{min}(\boldsymbol{B}) > 0$。

IV. 防御策略设计

传输策略和攻击检测策略共同决定防御策略。因此，在本章节中，我们将探讨 Alice 如何设计传输信号，以及 Bob 如何执行认证过程中的验证步骤。

A. 高斯传输

最优传输策略 $p^{\star}x$由式（13）的极大极小解给出。我们首先确定受约束协方差矩阵下的最优分布，并引入以下定理。

定理 2. 给定协方差矩阵 $\boldsymbol{K}x$，定义 $p^{\star}x \sim \mathcal{N}(0, \boldsymbol{K}x)$。若传输分布 p_x 从所有均值为零且协方差为 $\boldsymbol{K}x$ 的分布中选取，则策略对 $(p^{\star}x, p^{\star}v|z)$ 构成函数 $f(p_x, p^{v|z})$的鞍点。

证明。对于任意攻击策略 $\mathrm{p}_{v|z} \in \mathcal{C}$，我们可以根据式 (22) 计算一般分布 $\mathrm{p}x$ 对应的 $\mathrm{f}(\mathrm{p}x, \mathrm{p}^{v|z})$。注意，当 $\mathrm{p}_{v|z} \in \mathcal{C}$ 时，K-L 散度仅通过协方差矩阵 K x $v|z \in \mathcal{C}$ 依赖于 $\mathrm{p}x$。因此，如果 p，一旦矩阵 A、B 和 Kx 确定，对于 Alice 选择的每个概率分布 $\mathrm{p}x$，$\mathrm{f}(\mathrm{p}x, \mathrm{p}^{v|z})$ 都是常数。因此，我们得出结论：策略集合 $(\mathrm{p}^{\star}\mathrm{x}, \mathrm{p}^{\star}\mathrm{v|z})$ 构成 $\mathrm{f}(\mathrm{p}x, \mathrm{p}^{v|z})$ 的鞍点，因为如果另一方的策略保持不变，攻击者和防御者都无法通过单方面改变策略获利。特别是

$$f(p_x, p^{\star}_{v|z}) = f(p^{\star}_x, p^{\star}_{v|z}),\ \forall\, p_x, \tag{33}$$

$$f(p^{\star}_x, p_{v|z}) > f(p^{\star}_x, p^{\star}_{v|z}),\ \forall\, p_{v|z}, \tag{34}$$

其中，式 (33) 是由式 (22) 推出的，此时协方差矩阵 $\boldsymbol{K}x$ 固定；而式 (34) 则在传输分布为 $p^{\star}x$ 时，依据定理 1 得出 $p^{\star}v|z$ 的最优性。□

式 (13) 中的极大极小问题可视为一个有两位参与者的零和博弈，其中 p_x 和 $p^{v|z}$ 是混合策略，而 $f(p_x, p^{v|z})$ 和 $-f(p_x, p^{v|z})$ 分别是防御者和攻击者的平均收益[2]。在这种情况下，策略集 $(p^{\star}x, p^{\star}v|z)$ 构成该博弈的一个纳什均衡。需要指出的是，纳什均衡可能不止一个；然而，根据零和博弈的性质，它们的平均收益 [31]都相同。

根据定理 2，我们得出，求解式 (13) 的最优防御策略 $p^{\star}x$ 必须是零均值高斯分布。此外，Alice 可以选择 $p^{\star}x$ 的协方差矩阵$\boldsymbol{K}x$，使 $f(p^{\star}x, p^{\star}v|z)$ 最大化，同时满足发射功率Mx的约束：$\mathrm{tr}(\boldsymbol{K}x) \leq mn\, Mx$。鉴于问题的对称性，以及发射机不了解信道，因而也不了解矩阵$\boldsymbol{A}$ 和$\boldsymbol{F}$，选择 $\boldsymbol{K}x$ 为$\boldsymbol{K}_{\boldsymbol{x}} = Mx\boldsymbol{I}mn$是合理的。

根据二元假设检验理论，我们知道，如果合法信号和欺骗信号的统计特性都已知（即受害者知晓欺骗器采用的特定攻击策略），那么对于给定的p_{MD} 约束，使p_{FA}最小的检验就是似然比检验（LRT），也称为奈曼-皮尔逊准则 [27], [28]。在假设攻击策略属于类 $\mathcal{C}$ 的条件下，检测问题可简化为检验

$$L' = (\boldsymbol{r} - \boldsymbol{A}\boldsymbol{x})^{\mathrm{H}}\boldsymbol{K}_{\mathrm{B}}{}^{-1}(\boldsymbol{r} - \boldsymbol{A}\boldsymbol{x}) - (\boldsymbol{r} - \boldsymbol{B}\boldsymbol{x})^{\mathrm{H}}\boldsymbol{K}_{\boldsymbol{\eta}}{}^{-1}(\boldsymbol{r} - \boldsymbol{B}\boldsymbol{x}) \underset{H_0}{\overset{H_1}{\gtrless}} \theta\,. \tag{35}$$

当 Eve 和 Alice 都采用第三节和第IV-A节推导出的纳什均衡策略时，Bob 将使用似然比检验，因为他知道攻击策略的分布。

B. 实用调制方案下的传输策略

在第IV-A节中，我们推导出，求解式 (13) 的最优防御策略必须是零均值高斯分布。然而，在实践中这并不可行，因此我们分析$\boldsymbol{x}$ 取有限集合中的符号（例如 QAM 星座）的情形。

在式 (22) 中我们表明，当 $p_{v|z} \in \mathcal{C}$时，$f(p_x, p^{v|z})$ 仅通过协方差矩阵$\boldsymbol{K}x$依赖于p_x。这意味着

$$f(p_x, p_{v|z}) = f(p^{\star}_x, p_{v|z}),\ \forall\, p_{v|z} \in \mathcal{C}, \tag{36}$$

其中p_x 是信号$\boldsymbol{x}$的一般分布，其协方差矩阵与$p^{\star}x \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{K}x)$的协方差矩阵相同$\boldsymbol{K}x$。因此，当攻击属于类别 $\mathcal{C}$ 时，我们可以得出结论：无论采用高斯调制还是有限基数调制，其散度性能都相同。此外，根据式 (33) 和 (34)，我们有

$$f(p_x, p^{\star}_{v|z}) = f(p^{\star}_x, p^{\star}_{v|z}) \leq f(p^{\star}_x, p_{v|z}),\ \forall\, p_{v|z}\,. \tag{37}$$

另一方面，$p^{\star}v|z$ 仅当传输信号$\boldsymbol{x}$ 是长度为mn的高斯码字时，才是最优攻击策略。这意味着，对于非高斯p_x，可能存在一种攻击策略$p^{o}{}_{v|z} \not\in \mathcal{C}$，能够实现

$$f(p_x, p^{o}_{v|z}) \leq f(p_x, p^{\star}_{v|z})\,. \tag{38}$$

因此，根据式（36）–（38）可推导出以下关系

$$f(p_x, p^{o}_{v|z}) \leq f(p_x, p^{\star}_{v|z}) = f(p^{\star}_x, p^{\star}_{v|z}) \leq f(p^{\star}_x, p^{o}_{v|z})\,. \tag{39}$$

当信号$\boldsymbol{x}$ 的符号取自有限集合时，传输策略不同于$p^{\star}x$，且最优攻击策略分布$p^{o}{}_{v|z}$ 未知。因此，接收机只知道真实信号的统计特性，无法对 E 选择的攻击策略作出假设，也不了解信道 A $\rightarrow$ E 和 E $\rightarrow$ B。在这种情况下，LRT检测方法不再适用，一种可行的解决方案是使用 GLRT [27], [32], ，即检测问题可表示为

$$G' = (\boldsymbol{r} - \boldsymbol{A}\boldsymbol{x})^{\mathrm{H}}\boldsymbol{K}_{\mathrm{B}}{}^{-1}(\boldsymbol{r} - \boldsymbol{A}\boldsymbol{x}) \underset{H_0}{\overset{H_1}{\gtrless}} \theta\,. \tag{40}$$

[2]玩家的收益是在混合策略玩家所采用的策略以及噪声分布下取平均得到的，$f(p_x, p^{v|z}) = \mathbb{E}\left[\log \frac{p_{xv}(x,v)}{p_{xy}(x,v)}\right]$。

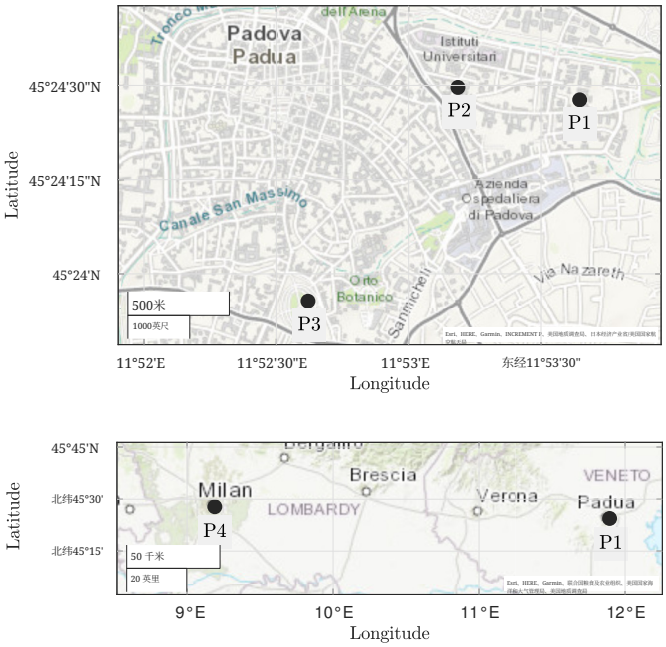


图2. 所考察位置的地图。其中三个位于意大利帕多瓦：DEI（P1）、保洛蒂街（P2）和普拉托德拉瓦莱广场（P3）。一个位于意大利米兰：主教座堂广场（P4）。

表II 所考察位置及其坐标

	经纬高坐标	地标
P1	45.4077° N, 11.8941° E, 12 米	DEI，帕多瓦，意大利
P2	45.4079° N, 11.8860° E, 12 米	保洛蒂街，帕多瓦，意大利
P3	45.3980° N，11.8766° E，12 米	普拉托德拉瓦莱，帕多瓦，意大利
P4	45.4641° N，9.1903° E，120 米	主教座堂广场，米兰，意大利

V. 数值结果

本章节将说明在以下场景下，采用高斯信令或有限基数信令时，LRT 和 GLRT 的性能：

- 信道矩阵 $\boldsymbol{A}$ 和$\boldsymbol{F}$ 仅考虑时延，即从第i颗卫星到 Eve 和 Bob 的每个信号 $\bar{\boldsymbol{x}}_i$的传播时间，因此我们忽略其他可能的信道现象；
- 攻击策略$p^{\star}_{\boldsymbol{x}|\boldsymbol{z}}$如第三节所述。此外，在典型的全球导航卫星系统欺骗场景中，接收机处的欺骗信号$\boldsymbol{v_0}$ 功率通常大于合法信号的功率；因此，攻击信号的信噪比将显著高于真实信号。假设 Bob 前端的自动增益控制（自动增益控制）能够将接收信号缩放至近乎恒定的幅度，那么在攻击情况下，接收机噪声方差也会相应降低，从而为欺骗器塑造$\boldsymbol{K}\eta = \boldsymbol{K}_{\mathrm{B}}$留出一定余量。与（31）类似，我们将接收到的欺骗器信噪比定义为

$$\Lambda_{\mathrm{AE}} = \frac{M_x}{\sigma_{\mathrm{E}}^2}\frac{\|\boldsymbol{F}\|_F^2}{mn}, \tag{41}$$

在所分析的场景中，我们将考虑与我们部门位置相关的时延向量 $\boldsymbol{\tau}_{\mathrm{f}}$

表 III Eve 与目标位置之间的距离

Eve 位置	目标位置	距离
P1	P2	607 米
P1	P3	1.7 千米
P1	P4	211 千米

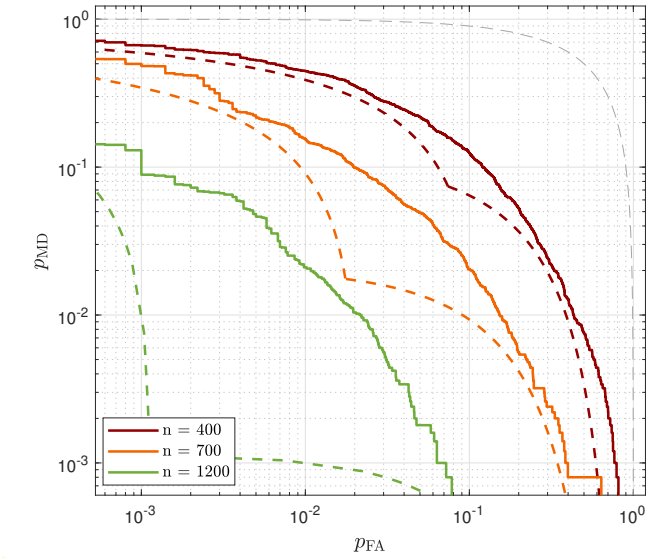


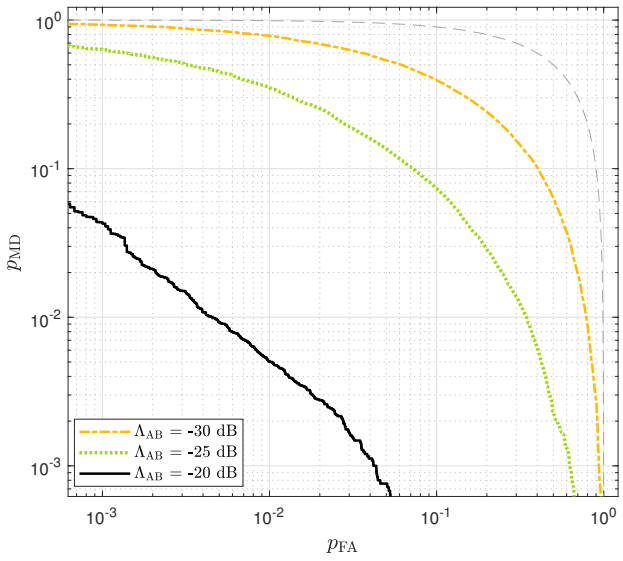
图 3. 当n取不同值、p_x 服从高斯分布、$M_x = 1$、$m = 5$，$\boldsymbol{\tau}_{\mathrm{f}}$ 与 P1 相关、$\boldsymbol{\tau}_{\mathrm{E}}$ 与 P2 相关、$\Lambda_{\mathrm{AB}} = -25$ dB 且 $\Lambda_{\mathrm{AE}} = -10$ dB 时，似然比检验检测方法（实线）和 K- L散度界（虚线）的 DET曲线。灰色虚线表示平凡极限情形，即通过抛掷一枚有偏硬币来作出决策。

(DEI) (P1)，位于意大利帕多瓦，以及与三个不同位置相关的时延向量 $\boldsymbol{\tau}_{\mathrm{E}}$，其中两个位于意大利帕多瓦，分别是保洛蒂街的一处住宅 (P2) 和普拉托德拉瓦莱广场 (P3)；另一个是位于意大利米兰的主教座堂广场 (P4)。图 2 展示了这四个位置。时延测量数据采集于 2022 年 12 月 14 日上午 12:00。表 II 列出了各个所考虑位置的坐标，表 III 则汇总了目标位置与 Eve 所在位置之间的距离。

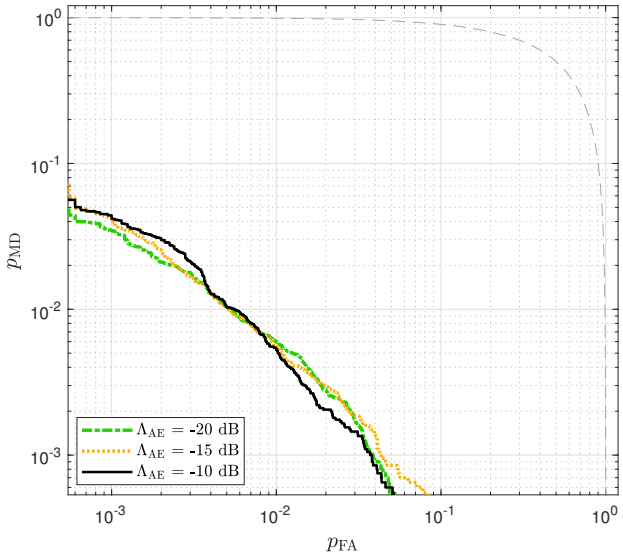
A. 高斯信号传输

在本章节中，评估发射信号$\boldsymbol{x}$ 为长度n的高斯码字时的性能，并采用似然比检验检测方法。

图 3 展示了不同 n 值下，似然比检验检测方法（实线）的 DET曲线以及根据 K-L 散度推导出的性能界（虚线）。考虑来自 $m = 5$ 颗卫星的信号，$M_x = 1$,$\Lambda_{\mathrm{AB}} = -25$ dB，$\Lambda_{\mathrm{AE}} = -10$ dB，其中 $\boldsymbol{\tau}_{\mathrm{E}}$ 和 $\boldsymbol{\tau}_{\mathrm{f}}$ 分别收集与 P1 和 P2 相关的时延。该界呈现出与式 (29) 相同的趋势，因此能够代表实际性能。对于 $n = 400$，该界很紧；而随着 n 增大，该界与实际性能之间的差距也随之增大。实际上，随着 n 减小，DET曲线迅速趋近于灰色虚线，该虚线表示



(a)



(b)

图4. 当p_x 服从高斯分布、$M_x = 1$、$m = 5$、$n = 500$，且 $\boldsymbol{\tau}_{\mathrm{f}}$ 与P1相关、$\boldsymbol{\tau}_{\mathrm{E}}$ 与P2相关时，不同(a) Λ_{AB} 和(b) Λ_{AE}取值下的LRT检测方法DET曲线。在(a)中，$\Lambda_{\mathrm{AE}} = -10$ dB；在(b)中，$\Lambda_{\mathrm{AB}} = -20$ dB。

平凡极限情形，此时不观察信号，而是通过抛掷有偏硬币来作出决策。因此，如图 3 所示，对于给定的 p_{FA} 值，可通过增大 n 的值来降低所得到的 p_{MD}。当 $n = 1200$ 时，与 $n = 400$ 的情形相比，p_{MD} 的值约降低一个数量级。此外，我们注意到，K-L 散度给出的界具有对称性，这一点已在附录 A 中证明。

图4显示了在以下条件下，LRT检测方法针对不同的 (a) Λ_{AB} 和 (b) Λ_{AE} 值的DET曲线：考虑来自$m = 5$ 颗卫星、$M_x = 1$的信号；(a) $\Lambda_{\mathrm{AE}} = -10$ dB，(b) $\Lambda_{\mathrm{AB}} = -20$ dB；当 $\boldsymbol{\tau}_{\mathrm{E}}$ 和 $\boldsymbol{\tau}_{\mathrm{f}}$ 收集

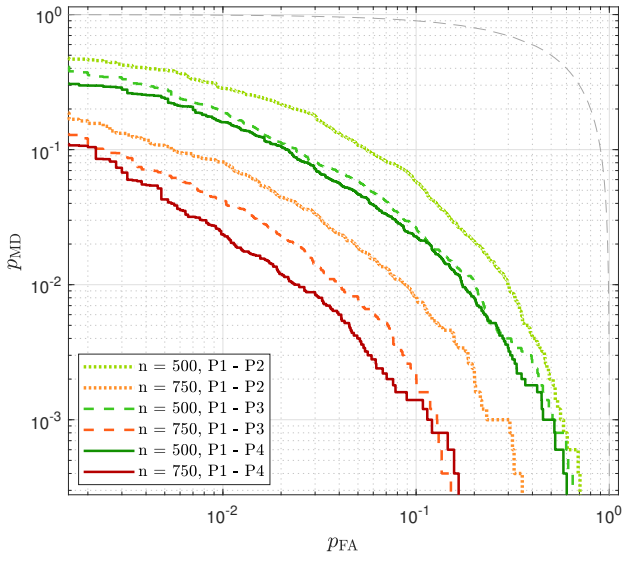


图5. 当p_x 服从高斯分布、$M_x = 1$、$m = 5$、$\Lambda_{\mathrm{AB}} = -25$ $\Lambda_{\mathrm{AE}} = -10$ dB时，不同 n 取值和位置对下的LRT检测方法DET曲线。

分别与P1和P2相关的时延。可以看出，曲线遵循式(29)所示的变化规律；实际上，随着 Λ_{AB} 减小，曲线会上升，而对于不同的 Λ_{AE} 值，曲线保持不变。因此，只要满足 $\Lambda_{\mathrm{AE}} > \Lambda_{\mathrm{AB}}$，LRT验证机制的性能就与攻击者的信噪比无关。

图5展示了图2所示的不同n 取值和位置对下的LRT检测方法DET曲线，其中$M_x = 1$、$m = 5$、$\Lambda_{\mathrm{AB}} = -25$ dB，且 $\Lambda_{\mathrm{AE}} = -10$ dB。在每种测试场景中，时延向量 $\boldsymbol{\tau}_{\mathrm{f}}$ 与P1相关，而向量 $\boldsymbol{\tau}_{\mathrm{E}}$ 与三个不同位置相关，即（从距P1最近到最远）：P2、P3和P4。可以看出，当与 $\boldsymbol{\tau}_{\mathrm{E}}$ 和 $\boldsymbol{\tau}_{\mathrm{f}}$ 相关的位置之间的距离减小时，曲线会远离完全可区分性（左下角）。因此，随着攻击的目标位置远离攻击者的实际位置，攻击性能会下降。最后，我们注意到，与图3的情况相同，随着n增大，防御性能会提升（即曲线向左下角移动）。

B. 实用调制方案

如第四节 IV-B 所述，当攻击策略属于 $\mathcal{C}$ 时，从高斯信号传输切换为有限基数信号传输不会影响验证机制的性能。本段将通过仿真结果展示这一现象。以下将考虑 BPSK 调制（即基数为$M = 2$）。

图 6 展示了在不同 n 值下，广义似然比检验检测方法的 DET 曲线。其中，p_x 服从高斯分布（实线），而 p_x 服从二元分布（虚线）；$M_x = 1$、$m = 9$、$\boldsymbol{\tau}_{\mathrm{f}}$ 和 $\boldsymbol{\tau}_{\mathrm{E}}$ 分别收集了与 P1 和 P4 相关的时延。这些结果是在

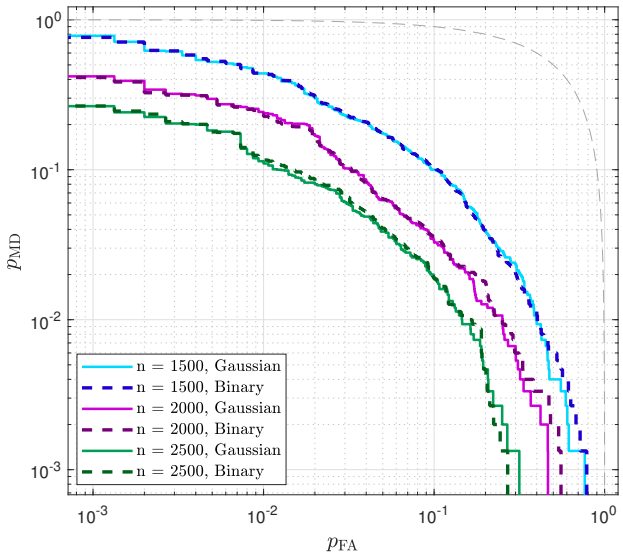


图 6. 当 n_x 取不同值时，p_x 服从高斯分布（实线）和二元分布（虚线）情况下，广义似然比检验检测方法的 DET 曲线；$M_x = 1$，$m = 9$，$\boldsymbol{\tau}_{\mathrm{f}}$ 与 P1 相关联，$\boldsymbol{\tau}_{\mathrm{E}}$ 与 P4 相关联，$\Lambda_{\mathrm{AB}} = -20$ dB，且 $\Lambda_{\mathrm{AE}} = -10$ dB。

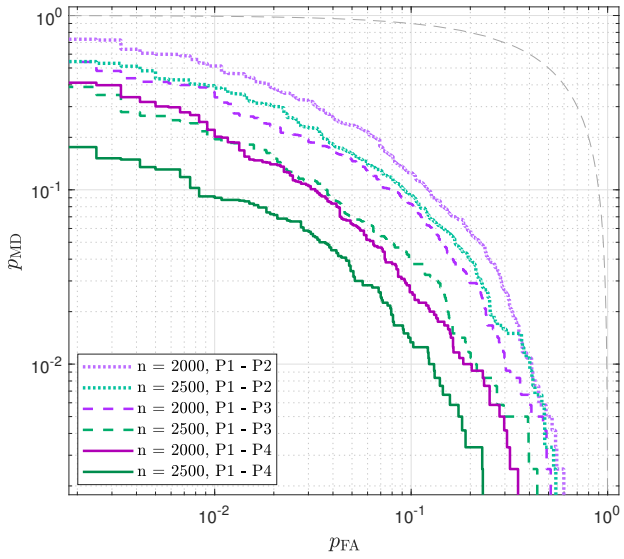


图 7. 当n 和位置对取不同值，p_x 服从高斯分布，$M_x = 1$、$m = 9$、$\Lambda_{\mathrm{AB}} = -20$ $\Lambda_{\mathrm{AE}} = -10$ dB 和 dB 时，广义似然比检验检测方法的DET曲线。

$\Lambda_{\mathrm{AB}} = -20$ dB 和 $\Lambda_{\mathrm{AE}} = -10$ dB 下获得的，因此我们处于低信噪比区间。可以看出，高斯信号传输与二元信号传输所得到的曲线非常接近，这证实了第四节 IV-B 的结果。此外，结果表明，即使事先不了解欺骗者策略，广义似然比检验也能有效检测欺骗。对于具有实际意义的 p_{FA} 和 p_{MD} 值，我们应考虑使用更长的信号，因此相较于似然比检验情形，应采用更大的 n 值。显然，在做出判决前观测更多样本，判决会更准确，但这需要缓冲并处理更多数据。此外，这会延长认证时间（TTA）。因此，观测时段必须在设备的计算资源、期望的 TTA 以及 DET 性能要求之间进行权衡。

图 7 展示了 n 取不同值及不同位置对时，广义似然比检验检测方法的 DET 曲线，其中p_x 服从高斯分布，$M_x = 1$，$m = 9$，$\Lambda_{\mathrm{AB}} = -20\,\mathrm{dB}$，且 $\Lambda_{\mathrm{AE}} = -10$ dB。在每种测试场景中，时延向量 $\boldsymbol{\tau}_{\mathrm{f}}$ 与 P1 相关联，而向量 $\boldsymbol{\tau}_{\mathrm{E}}$ 与 P2、P3 和 P4 相关联。与 LRT 情况一样，当与 $\boldsymbol{\tau}_{\mathrm{E}}$ 和 $\boldsymbol{\tau}_{\mathrm{f}}$ 相关联的位置之间的距离减小时，攻击性能会提升。因此，对于广义似然比检验，随着攻击的目标位置远离攻击者的实际位置，在虚警概率固定时，漏检概率也会降低。

VI. 结论

本文提出了一种通用模型，用于刻画全球导航卫星系统中的欺骗检测问题，假设欺骗器能够观测合法信号，并将具体的调制格式和密码机制抽象化。我们证明，仅依靠来自多个卫星的信号组合，以及攻击者位置与预期伪造位置之间的差异，就能实现有效检测。我们还研究了一类基于发射信号和接收信号统计特性的攻击策略，并证明该策略能够最小化 K-L 散度度量，因此是最优的。最优攻击策略是对攻击者位置处接收的信号进行适当的线性变换，并叠加经过恰当调整的独立加性高斯白噪声。我们推导出了 K-L 散度的一个下界，该下界仅取决于发射信号的总长度、合法信道的信噪比，以及伪造信道矩阵与合法信道矩阵之间的差异。此外，我们还讨论了不同调制方案下得到的结果；并证明，当采用最优攻击策略时，高斯信号传输与有限基数信号传输在 K-L 散度方面具有相同的性能。随后，我们求得攻防方案的一个纳什均衡，推导出针对上述攻击的最优防御策略；该策略又可由高斯分布描述。最后，我们通过数值仿真分析了检测方案在应对所提出攻击时的性能，并考虑了两种验证机制：似然比检验（LRT）和广义似然比检验（GLRT）。

附录 A K-L 散度的对称性

在本附录中，我们证明当攻击者采用第三节中提出的最优攻击策略 $p^{\star}{}_{v|z}$ 时，K-L 散度的对称性成立，并且 $\boldsymbol{K}^{\eta} = \boldsymbol{K}_{\mathrm{B}}$，即

$$\mathbb{D}(p_{xv^{\star}} \| p_{xy}) = \mathbb{D}(p_{xy} \| p_{xv^{\star}})\,. \tag{42}$$

对于任意 $p_{v|z} \in \mathcal{C}$, $\mathbb{D}(p_{xy}\|p_{xv})$，都可以按照与式 (22) 相同的步骤计算，因此我们得到

$$\begin{aligned}\mathbb{D}(p_{xy}\|p_{xv}) &= \frac{1}{2}\Bigg[\log\frac{|\boldsymbol{K}_{\eta}|}{|\boldsymbol{K}_{\mathrm{B}}|} + \mathrm{tr}(\boldsymbol{K}_{\mathrm{B}}\boldsymbol{K}_{\eta}{}^{-1}) \\ &\quad + \mathrm{tr}\left((\boldsymbol{A}-\boldsymbol{B})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{A}-\boldsymbol{B})^{\mathrm{H}}\boldsymbol{K}_{\mathrm{B}}{}^{-1}\right) - (n+\delta_{\mathrm{f}})\Bigg] \\ &= \frac{1}{2}\left[\sum_{i=1}^{n+\delta_{\mathrm{f}}}\left(\frac{\sigma_{\mathrm{B}}^2}{\lambda_i} - \log\left(\frac{\sigma_{\mathrm{B}}^2}{\lambda_i}\right)\right) - (n+\delta_{\mathrm{f}})\right] \\ &\quad + \frac{1}{2\sigma_{\mathrm{B}}^2}\mathrm{tr}\left((\boldsymbol{A}-\boldsymbol{B})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{A}-\boldsymbol{B})^{\mathrm{H}}\right)\end{aligned} \tag{43}$$

当攻击策略为$p^{\star}{}_{v|z}$且$\boldsymbol{K}^{\eta} = \boldsymbol{K}_{\mathrm{B}}$时，我们有 $\lambda_i = \sigma_{\mathrm{B}}^2, \forall i \in \{1, 2, \ldots, n+\delta_{\mathrm{f}}\}$。因此，我们得到

$$\begin{aligned}\mathbb{D}(p_{xy}\|p_{xv^{\star}}) &= \frac{1}{2\sigma_{\mathrm{B}}^2}\mathrm{tr}\left((\boldsymbol{A}-\boldsymbol{B}^{\star})\boldsymbol{K}_{\boldsymbol{x}}(\boldsymbol{A}-\boldsymbol{B}^{\star})^{\mathrm{H}}\right) \\ &= \mathbb{D}_{min}(\boldsymbol{B}^{\star}) = \mathbb{D}(p_{xv^{\star}}\|p_{xy}).\end{aligned} \tag{44}$$

参考文献

[1] Z. Wu、Y. Zhang、Y. Yang、C. Liang 和 R. Liu，“全球导航卫星系统欺骗与反欺骗技术：综述”，*IEEE Access*，第8卷，第165 444–165 496页，2020年9月。[2] D. Margaria、B. Motella、M. Anghileri、J. Floch、I. Fernandez-Hernandez 和 M. Paonni，“民用全球导航卫星系统基于信号结构的认证：近期解决方案与展望”，*IEEE Signal Processing Magazine*，第34卷，第5期，第27–37页，2017年。[3] M. L. Psiaki 和 T. E. Humphreys，“全球导航卫星系统欺骗与检测”，载于*Proceedings of the IEEE*，第104卷，第6期，2016年，第1258–1270页。[4] T. E. Humphreys，“基于密码学的全球导航卫星系统反欺骗检测策略”，*IEEE Transactions on Aerospace and Electronic Systems*，第49卷，第2期，第1073–1090页，2013年4月。[5] G. Caparra、N. Laurenti、R. Ioannides 和 C. Massimo，“改进安全码估计-重放攻击及其在全球导航卫星系统信号中的检测”，载于*ProceedingsofESAWorkshopon Satellite NavigationTechnologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*，2014年。[6] K. Zhang 和 P. Papadimitratos，“距离缩短攻击对受密码学保护的全球导航卫星系统信号的影响”，载于*Proceedingsof the International Technical Meeting of The Institute of Navigation*，2019年，第363–372页。[7] J. T. Curran 和 M. Paonni，“全球导航卫星系统安全防护：伽利略开放服务的端到端可行性分析”，载于*Proceedings of the 27thInternational Technical Meeting oftheSatellite Division of The Institute of Navigation (ION GNSS+ 2014)*，美国佛罗里达州坦帕，2014年，第2828–2842页。[8] G. Caparra 和 J. T. Curran，“全球导航卫星系统测距码加密的可实现等效安全性”，载于*Proceedings of IEEE/ION Position, Location and Navigation Symposium (PLANS)*，2018年，第956–966页。[9] R. Terris-Gallego、I. Fernandez-Hernandez、J. A. L´opez-Salcedo 和 G. Seco-Granados，“伽利略辅助商业认证服务实施指南”，载于*Proceedings of the International Conference on Localization and GNSS (ICL-GNSS)*，2022年，第01–07页。[10] I. Fernandez-Hernandez、S. Cancela、R. Terris-Gallego、G. Seco-Granados、J. A. L´opez-Salcedo、C. O'Driscoll、J. Winkel、A. d. Chiara、C. Sarto、V. Rijmen、D. Blonski 和 J. de Blas，“基于伽利略ACAS的半辅助式信号认证”，*arXiv*，2022年6月。[11] I. Fern´andez-Hern´andez、V. Rijmen、G. Seco-Granados、J. Simon、I. Rodr´ıguez 和 J. D. Calle，“面向伽利略开放服务的导航电文认证方案”，*NAVIGATION: Journal of the Instituteof Navigation*，第63卷，第1期，第85–102页，2016年3月。

[12] I. F. Hern´andez、T. Ashur、V. Rijmen、C. Sarto、S. Cancela 和 D. Calle，“迈向运行导航消息认证服务：OSNMA 协议附加功能的提案与论证”，载于*Proceedings of European Navigation Conference (ENC)*，2019年，第1–6页。[13] M. G. Kuhn，“导航信号的非对称安全机制”，*Information Hiding*，第239–252页，2005年。[14] L. Scott，“民用导航系统的反欺骗与认证信号架构”，载于*Proceedings of the Institute of Navigation GPS/GNSSConference*，2003年，第1543–1552页。[15] ——，“使用 GPS 位置签名证明位置：必要性及实现方法”，载于*Proceedingsofthe 26thInternationalTechnicalMeeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013)*，美国田纳西州纳什维尔，2013年，第2880–2892页。[16] A. G. T. I. 空军研究实验室航天器部门，芯片消息稳健认证（*CHIMERA*）增强版*L1C* 信号：空间段/用户段接口。接口规范 IS-AGT-100，2019年4月。

[17] J. M. Anderson, J. Hamlin, J. Caldwell, W. Bradley, P. Revelman, J. L. Scott, 以及 C. A. Yazdi，“面向 GPS 民用信号的码片消息鲁棒认证（CHIMERA）”，载于美国导航学会卫星分部第*30*届国际技术会议（*ION GNSS+ 2017*），2017，2388–2416，9月，页码 –。

[18] B. Motella, M. Paonni, 和 D. Margaria，“伽利略开放服务的一种认证概念”，载于*IEEE/ION* 定位、位置与导航研讨会（*PLANS*），2018年，页码 967–977。

[19] S. Wang, “基于二进制相位跳变的扩频码认证技术”，《卫星导航》，第2卷，第4期，2021年2月。

[20] O. Pozzobon, L. Canzian, M. Danieletto, 和 A. D. Chiara, “反欺骗 - 以及开放式全球导航卫星系统信号认证与信号认证序列，”见 *ESA*卫星导航技术研讨会和欧洲全球导航卫星系统信号与信号处理研讨会（*NAVITEC*）论文集，2010年，第1–6页。

[21] O. Pozzobon, G. Gamba, M. Canzian, 和 S. Fantinato，“超音速全球导航卫星系统认证码”，载于美国导航学会卫星分会第27届国际技术会议（*ION GNSS+ 2014*）论文集，佛罗里达州坦帕，美国，2014年，第2862–2869页。[22] N. Laurenti 和 A. Poltronieri，“全球导航卫星系统扩频码认证序列设计中安全性、可用性与资源之间的最佳折衷”，载于国际定位与全球导航卫星系统会议（*ICL-GNSS*）论文集，2020年，第1–6页。[23] F. Formaggio 和 S. Tomasin，“通过窃听信道编码和人工噪声认证卫星导航信号”，*EURASIP*《无线通信与网络杂志》，第98期，2019年4月。[24] E. D. Kaplan 和 C. J. Hegarty，《理解*GPS*：原理与应用——第二版》。Artech House，2005年。[25] I. Fern´andez-Hern´andez、T. Ashur 和 V. Rijmen，“延迟披露全球导航卫星系统认证协议中消息认证码和密钥长度的分析与建议”，《*IEEE*航空航天与电子系统汇刊》，第57卷，第3期，第1827–1839页，2021年。[26] T. E. Humphreys、B. M. Ledvina、M. L. Psiaki、B. W. O'Hanlon 和 P. M. Kintner Jr，“评估欺骗威胁”，《*GPS*世界》，第20卷，第1期，第28–38页，2009年。[27] S. M. Kay，《统计信号处理基础——第*2*卷：检测理论》。美国：Prentice-Hall, Inc.，1993年。[28] U. M. Maurer，“认证理论与假设检验”，《*IEEE*信息论汇刊》，第46卷，第4期，第1350–1356页，2000年7月。[29] C. Cachin，“隐写术的信息论模型”，第二届信息隐藏国际研讨会（*IH*）论文集，LNCS-1525卷，第306–318页，1998年。[30] A. Ferrante、N. Laurenti、C. Masiero、M. Pavon 和 S. Tomasin，“瑞利衰落信道上基于信道估计的物理层认证的错误区域”，《*IEEE*信息取证与安全汇刊》，第10卷，第5期，第941–952页，2015年5月。[31] J. 冯·诺依曼和 O. 摩根斯坦，《博弈论与经济行为》，第*2*次修订版。普林斯顿大学出版社，1947年。[32] O. Zeitouni、J. Ziv 和 N. Merhav，“广义似然比检验何时最优？”，《*IEEE*信息论汇刊》，第38卷，第5期，第1597–1602页，1992年9月。