GNSS信号交叉认证检查的局限性

Francesco Ardizzon *IEEE*会员、Laura Crosara*IEEE*学生会员、Stefano Tomasin *IEEE*高级会员和 Nicola Laurenti

arXiv:2304.02977v1 [cs.CR] 6 Apr 2023

摘要—**全球导航卫星系统（GNSS）正在实施安全机制，例如伽利略开放服务导航电文认证（OS-NMA）和GPS芯片消息鲁棒认证（CHIMERA）。这些机制均在单一频段内运行。然而，如今即使是商用GNSS接收机，通常也会同时利用多个星座和多个频段的信号计算位置、速度和时间（PVT）解，从而显著提高精度和可用性。因此，人们提出了交叉认证检查，其依据是通过混合使用认证信号和未认证信号获得的PVT。**

本文首先对交叉认证检查的模型进行形式化。接着，我们针对每种检查描述一种欺骗攻击，通过生成虚假信号，在不被察觉的情况下使受害者得到目标PVT。我们从分析上说明，攻击者操纵受害者解的自由度与所采用的安全检查，以及攻击者能够篡改的开放信号数量之间的关系。我们在一个实验数据集上测试了所考虑攻击策略的性能。最后，我们展示了基于PVT的GNSS交叉认证检查的局限性；这类检查同时使用认证信号和未认证信号。

索引词—**GNSS，PVT保障，物理层安全。**

I. 引言

全球导航卫星系统（GNSS）为各种民用和军事应用提供实时定位和授时。然而，由于接收功率较低，GNSS信号特别容易受到意外和蓄意干扰。此外，民用GNSS信号及其调制格式均向公众开放 [1], [2]：因此，攻击者可以通过生成虚假GNSS信号，危害依赖位置或授时的应用，使接收机计算出虚假位置或时间 [3], [4]。这些攻击称为欺骗攻击。此外，已有多项研究报告称，即使使用现成硬件也能成功实施攻击 [5], [6]。

因此，服务提供商提出了多种认证机制。在系统侧，通过在广播GNSS信号中加入攻击者无法预测和生成的特定特征来强化认证。具备认证功能的接收机随后可以解析这些特征，以区分真实信号和伪造信号。这些特征可以加入两个互补层面：数据层，即加入导航电文；以及测距层，即加入卫星与接收机之间的伪距。

信息工程系（DEI），帕多瓦大学，意大利。电子邮箱：{ardizzonfr, crosaralau, tomasin, nil}@dei.unipd.it

导航电文认证（NMA）技术旨在确保导航电文内容的真实性。开放服务导航电文认证（OS-NMA） [7] 是面向公众伽利略E1B信号的一种数据认证功能，其中，卫星传输的电文与认证数据交织在一起；这些认证数据通过一种称为时间高效、容忍丢失的认证（TESLA） [8]–[10]的广播认证协议生成。然而，基于NMA的协议容易受到安全码估计与重放攻击（SCER） [11], [12] 的影响，这类攻击会估计电文签名，从而实时伪造虚假信号。

测距层认证作用于信号扩频码，实际上认证了每个信号的传播时间，即信号到达接收机所需的时间。扩频码加密（SCE）技术是限制对GNSS信号访问的最可靠方案，因为它们使整个扩频码变得不可预测。伽利略的SCE方案由商业认证服务（CAS）提供，该服务将在E6频段提供扩频测距层认证，以补充OS-NMA。近期在 [13]和 [14],中介绍的辅助CAS（ACAS），则是一种基于OS-NMA接收并认证的导航数据的扩频码认证（SCA）方法。对于GPS，芯片消息鲁棒认证（CHIMERA）方案 [15], [16],旨在联合认证民用GPS信号的导航数据和扩频码，同时实现NMA和SCA。该方案以一小段保密加密序列替换扩频码的一小部分；接收机获知密钥后，即可重新生成该序列。导航电文数据则通过对大部分或全部数据进行数字签名来保护。事实上，正如 [17]中所述，测距层认证会降低SCER类攻击的有效性。因此，下文将采用SCA（或SCE）保护的信号称为认证信号，其他所有信号则称为开放信号。

ACAS和CHIMERA 都存在一些问题。首先，用于距离验证的数据仅在事后提供给接收机，因此无法验证当前的位置、速度和时间（PVT）。为解决这一问题，在 [18]，中，作者提出了一种仅使用ACAS来生成连续、稳健且安全的授时服务的策略：然而，该应用仅限于静态场景。有人提出了一种基于连续GPS信号运行并使用基于随机可达性的卡尔曼滤波器的验证方法，见 [19]。然而，该解决方案仅依赖 CHIMERA，未利用其他系统或不同频段传输的信号。

第二个问题是，仅使用认证信号来推导位置、速度和时间的接收机可能会降低解的精度和可用性。为了使位置、速度和时间解更加准确，GNSS接收机通常会利用所有可用频段上的信号。因此，近期的一种趋势是采用交叉认证机制：在接收机端，将认证信号与开放的非认证信号相结合，并对所得解进行一致性检查。

为提高位置、速度和时间解的可信度， [20]提出了一种逐步方法，其中接收机将经认证的信号用作完整位置、速度和时间解的信任锚。具体而言， [14]纳入了对同一频段但载波频率不同的信号进行检查，以验证伽利略加密E6C与E1B开放测量值之间的一致性。然而，当纳入来自不同系统的信号以及处于城市环境时，所提出方法的有效性会降低。

在 [21], 中，作者提出了一种交叉认证方案，旨在增强伽利略测距层保护，而不依赖CAS，同时利用CHIMERA和OS-NMA单系统认证概念。鉴于GPS和伽利略参考时间通过GPS至伽利略时间偏差（GGTO）相关联， [22], 他们提出了对测得的本地时钟偏差与从导航电文中获取的GGTO进行一致性检查。然而，我们将展示，即使仅篡改开放的伽利略信号，也可以攻击此类机制。

本文研究了 GNSS 中基于PVT的检查所采用交叉认证的安全性。具体而言，我们推导出针对交叉认证方案的欺骗攻击策略，并表明此类机制无法保证计算结果的真实性。更具体地说，本文的主要贡献如下。

1) 我们为位置、速度和时间交叉认证检查提出了一个新的通用框架。具体而言，我们确定了两类交叉检查：用于定位服务的基于时间的检查，以及用于授时的基于位置的检查。所讨论的先进机制均属于这两类。2) 我们提出了能够破解交叉认证检查的攻击策略，以及一种新颖的信号生成类生成时间欺骗攻击。3)我们从理论上研究了新型攻击的局限性，例如，将攻击者操纵受害者解的自由度与传输/传播场景的参数联系起来。4)我们同时考虑无噪声场景和现实的有噪声场景，对攻击性能进行了理论评估。5)我们使用由Septentrio PolarRx5 接收机采集的实验数据集对攻击进行了测试。

本文其余部分安排如下。第二节介绍系统模型。第三节给出基于位置、速度和时间的认证检查的一般模型。随后，第四节介绍所提出的攻击策略。第六节展示从实验数据集中获得的数值结果。最后，第七节给出结论。

II. 系统模型

我们考虑一台接收来自 $M > 1$ 个星座信号的多星座接收机。接收到的信号中有一部分经过认证，即受到 SCE（或 SCA）机制的保护。例如，这些信号可以是一组由伽利略系统在 E6C 频段通过 CAS 保护的信号，或一组由 CHIMERA 在 L1 C/A 频段保护的 GPS 信号。我们假设这些信号的认证评估不会发生故障；因此，攻击者无法生成新信号来替代经过认证的信号。

一般而言，受害者接收机从 N颗可见卫星获取信号：N_{A} 颗经过认证，其余$N_{\mathrm{O}} = N - N_{\mathrm{A}}$ 颗为开放式（即未认证）。为便于表示，将经过认证的卫星编号为 $j = 1, \ldots, N_{\mathrm{A}}$，未认证的卫星编号为 $j = N_{\mathrm{A}} + 1, \ldots, N$。经过常规的捕获和跟踪流程（例如参见 [23, 第 5]章）后，接收机获得伪距测量值向量 $\boldsymbol{r} = [r_1, \ldots, r_{\mathrm{N}}]^{\mathrm{T}}$。

在正常条件下，受害者接收机计算出的**位置、速度和时间解**是

$$p = [x,\, y,\, z,\, t_1,\, \ldots,\, t_M]^{\mathrm{T}}\,, \tag{1}$$

表示接收机在地心地固坐标系（ECEF）中的三维位置，以及时钟偏差，每个时间基准对应一个。求解式（1）的过程概述见附录A。实际上，我们可以考虑单一时间基准，例如某个全球导航卫星系统时间基准或协调世界时（UTC），并利用相应的系统间偏差（ISB） [24,Ch. 21], 关联其他时间基准，从而获得位置、速度和时间解。

$$p = [x,\, y,\, z,\, t]^{\mathrm{T}}\,, \tag{2}$$

如附录 B 所述。然而，部分所考虑的机制改用系统间偏差来评估解的真实性，因此，在这些情况下，我们将像式 (1) 中那样，分别估计各个时钟偏差。另一方面，当评估依据是接收机位置时，我们将位置、速度和时间解视为按式 (2) 计算。

A. 位置、速度和时间解

本节将简要介绍 GNSS 接收机通常如何计算位置、速度和时间解，该解将用于交叉认证检查。

在每个历元，位置、速度和时间解都通过迭代方法计算，分别从初始解 $\hat{}\boldsymbol{p} = [\hat{}x,\ \hat{}y,\ \hat{}z,\ \hat{}t_1,\ \ldots\ldots \hat{}t_M]^{\mathrm{T}}$ 或 $\hat{}\boldsymbol{p} = [\hat{}x,\ \hat{}y,\ \hat{}z,\ \hat{}t]^{\mathrm{T}}$ 开始，具体取决于我们分别要得到式 (1) 还是式 (2)。具体而言，$\hat{}\boldsymbol{p}$ 是前一历元计算得到的位置、速度和时间解，或是预定义的起始点（冷启动）。该方法遵循线性化过程，其中位置、速度和时间解通过几何矩阵 $\boldsymbol{G}$ 与距离相关（详情见附录 A 和 B）。因此，给定第 j 个信号 r_j 的距离测量值及其估计值 $\hat{}r_j$，距离残差为

$$\Delta r_j = r_j - \hat{r}_j\,. \tag{3}$$

接下来，注意到伪距位移 $\Delta\boldsymbol{r}$ 与位置位移 $\Delta\boldsymbol{p}$ 相关，表示为

$$\Delta\boldsymbol{r} = \boldsymbol{G}\Delta\boldsymbol{p} = \begin{bmatrix}\boldsymbol{G}_{\mathrm{A}} \\ \boldsymbol{G}_{\mathrm{O}}\end{bmatrix}\Delta\boldsymbol{p}\,, \tag{4}$$

其中，我们分别考虑了 $\boldsymbol{G}_{\mathrm{A}}$ 和 $\boldsymbol{G}_{\mathrm{O}}$中的已认证信号和开放信号，对几何矩阵进行了分解。由前述关系可知， $\Delta\boldsymbol{p}$ 可以由 $\Delta\boldsymbol{r}$ 计算得出，具体为

$$\Delta\boldsymbol{p} = (\boldsymbol{G}^{\mathrm{T}}\boldsymbol{G})^{-1}\boldsymbol{G}^{\mathrm{T}}\Delta\boldsymbol{r} \triangleq \boldsymbol{H}\Delta\boldsymbol{r}\,, \tag{5}$$

其中， $\boldsymbol{H}$ 是 $\boldsymbol{G}$的摩尔－彭若斯伪逆，通常也称为最小二乘解矩阵。我们注意到，矩阵 $\boldsymbol{H}$ 的各个分量仅取决于用户与参与最小二乘计算的 N 卫星之间的相对几何关系。最后，位置更新为$\hat{}\boldsymbol{p}' = \hat{}\boldsymbol{p} + \Delta\boldsymbol{p}$，其中$\hat{}\boldsymbol{p}'$是下一次迭代的起始点。

迭代过程持续进行，直到满足以下任一条件：i）达到最大迭代次数，或 ii）解的更新量小于用户定义的步长，即 $\|\Delta\boldsymbol{p}\| < \epsilon$。有关该过程以及各项推导的更多细节，请参见附录。

B. 攻击者模型

本节将详细介绍攻击者的能力和操作。我们假设消息数据（例如，大气改正和星历）是从公开可用的认证侧信道中获取的。此外，我们假设攻击者已知受害者接收机的实际位置。我们考虑两种类型的攻击：

生成攻击：这种攻击包括生成并传输伪造的 GNSS信号，这些信号对应的位置、速度和时间解可能与使用合法信号计算出的解不同。

中继攻击： 这种攻击包括对整个调制信号进行采样、记录和转发，同时保持代码和数据不变。这种攻击有时也称为转发欺骗。

我们指出，攻击者无法对受 SCA（或 SCE）保护的认证信号发动生成攻击，因为他不知道实际的扩频码。攻击者对认证信号唯一能采取的行动就是发动中继攻击。另一方面，攻击者可以生成、转发或选择性延迟开放信号，因为在这种情况下，扩频码和消息内容都是完全公开的。

我们假设遭受攻击的受害者获取并锁定了攻击者传输的伪造信号。例如，可以通过提高伪造信号的发射功率或抵消合法的开放信号来实现这一点。

攻击者旨在诱使受害者接收机将目标位置 $\boldsymbol{p}^{\star}$ 作为位置、速度和时间解，而非真实解$\boldsymbol{p}$。为此，攻击者篡改信号传播时间，使测距残差 $\Delta\boldsymbol{r}$ 产生改变量 $\Delta\boldsymbol{r}_{\mathrm{T}}$，从而在遭受攻击时，(4) 和 (5) 分别变为

$$\Delta\widetilde{\boldsymbol{r}} \triangleq \Delta\boldsymbol{r} + \Delta\boldsymbol{r}_{\mathrm{T}} = \boldsymbol{G}(\Delta\boldsymbol{p} + \Delta\boldsymbol{p}_{\mathrm{T}})\,, \tag{6}$$

$$\Delta\widetilde{\boldsymbol{p}} \triangleq \Delta\boldsymbol{p} + \Delta\boldsymbol{p}_{\mathrm{T}} = \boldsymbol{H}\Delta\widetilde{\boldsymbol{r}}\,. \tag{7}$$

这意味着测距篡改 $\Delta\boldsymbol{r}_{\mathrm{T}}$ 会导致位置、速度和时间解发生位移 $\Delta\boldsymbol{p}_{\mathrm{T}}$。因此，攻击者欺骗导致的位置、速度和时间更新将为

$$\widetilde{\boldsymbol{p}} = \hat{\boldsymbol{p}} + \Delta\widetilde{\boldsymbol{p}} = \hat{\boldsymbol{p}} + \Delta\boldsymbol{p} + \Delta\boldsymbol{p}_{\mathrm{T}}\,. \tag{8}$$

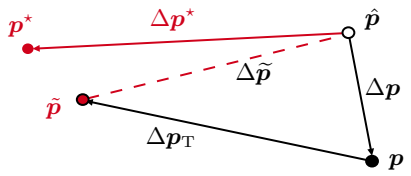


图1. 受攻击场景示例：$\hat{}\boldsymbol{p}$ 是迭代起点处的解， $\boldsymbol{p}$ 是合法解， $\boldsymbol{p}^{\star}$ 是攻击者目标解， $\tilde{\boldsymbol{p}}$ 是受害者通过混合使用开放信号和篡改信号计算出的解。

我们指出，只有当攻击者引入的伪距位移 $\Delta\boldsymbol{r}_{\mathrm{T}}$相对于 $\boldsymbol{r}$ 较小时，才可用线性变换来近似受攻击时计算位置、速度和时间的迭代最小二乘方法。在第六节中，我们将利用线性化过程测试攻击的有效性，并评估其性能随目标与实际位置之间距离的变化情况，即随待引入的伪距位移幅度的变化情况，从而检验线性近似的稳健性。

图1展示了攻击者篡改导致攻击者的位置、速度和时间发生的偏移：在合法条件下，接收机从$\hat{}\boldsymbol{p}$开始，会计算 $\Delta\boldsymbol{p}$ 以得到合法解 $\boldsymbol{p}$ （黑色）。而攻击者希望引导接收机得到目标 $\boldsymbol{p}^{\star}$ （红色），因此篡改信号，造成改变量 $\Delta\boldsymbol{p}_{\mathrm{T}}$。在这种情况下，受害者计算出的不是实际的位置、速度和时间，而是 $\tilde{\boldsymbol{p}}$，并使其尽可能接近目标$\boldsymbol{p}^{\star}$。请注意，图1既可以表示实际的三维位置，也可以表示整个位置、速度和时间向量，即考虑 $3 + M$空间中的点。

为清晰起见，我们将区分攻击者分别对认证信号和未认证信号引入的已认证和未认证伪距残差，$\Delta\boldsymbol{r}_{\mathrm{T,\,A}}$ 和 $\Delta\boldsymbol{r}_{\mathrm{T,\,O}}$。

$$\Delta\boldsymbol{r}_{\mathrm{T}} = \left[\Delta\boldsymbol{r}_{\mathrm{T,A}}\Delta\boldsymbol{r}_{\mathrm{T}}{}_{\mathrm{,O}}^{\mathrm{A}}\right]. \tag{9}$$

最后，将最小二乘矩阵划分为$\boldsymbol{H} = [\boldsymbol{H}_{\mathrm{A}}\,\boldsymbol{H}_{\mathrm{O}}]$，其中 $\boldsymbol{H}_{\mathrm{A}}$ 和 $\boldsymbol{H}_{\mathrm{O}}$ 分别表示与认证信号和开放信号相关的矩阵。特别地，由于攻击者只能对认证信号实施中继攻击，我们将攻击者对已认证伪距的篡改变模为$\Delta\boldsymbol{r}_{\mathrm{T,\,A}} = k\mathbf{1}$，其中$\mathbf{1}$是由全1填充的列向量。事实上，当实施生成攻击时，攻击者设置 $k = 0$，即实际上只有开放信号是伪造的。

III. 基于位置、速度和时间的交叉认证检查模型

接收机使用已认证伪距和未认证伪距计算位置、速度和时间解。随后，为评估其真实性，接收机会对位置、速度和时间解（或其中一部分）执行一项或多项一致性检查。我们使用决策理论来描述这一问题，并考虑这两个假设

$\mathcal{H}_0$: PVT is legitimate, signals are legitimate,

$\mathcal{H}_1$: PVT is fake, signals have been tampered with.

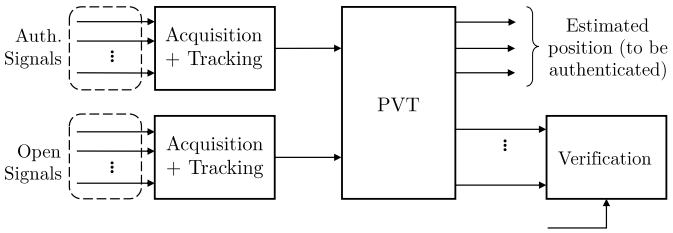


图 2. 基于时间的检查的框图。

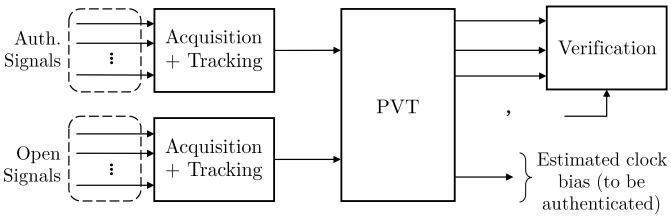


图 3. 基于位置的检查的框图。

对位置、速度和时间解进行的一致性检查会给出两个决策之一

$$\hat{\mathcal{H}}_0: \text{ Check passed, PVT is legitimate}$$
$$\hat{\mathcal{H}}_1: \text{ Check failed, PVT is not legitimate.}$$

这使我们能够将虚警 和 漏检概率定义为

$$p_{\mathrm{FA}} = P(\hat{\mathcal{H}}_1|\mathcal{H}_0) \tag{10a}$$
$$p_{\mathrm{MD}} = P(\hat{\mathcal{H}}_0|\mathcal{H}_1)\,. \tag{10b}$$

在接下来的章节中，我们将介绍用于验证位置、速度和时间（PVT）的各类一致性检查，这些检查也与所需服务相关。

A. 针对导航服务的基于时间的检查

接收机从 M 个不同的全球导航卫星系统收集信号，位置、速度和时间解包含 N_{s} 个时钟偏差，每个全球导航卫星系统时间基准对应一个，因此， $\boldsymbol{p}$ 按附录A中的方法计算。这些时间基准通过系统间偏差相互关联，因此，接收机认为该位置、速度和时间解是真实的，如果

$$\boldsymbol{\theta}_{\mathrm{t}} \triangleq \boldsymbol{C}\boldsymbol{p} \leq \boldsymbol{\delta}_{\mathrm{t}}\,, \tag{11}$$

其中， $\boldsymbol{C}$ 是一个用于选择并关联一对时钟偏差（符号适当）的矩阵，而 $\boldsymbol{\delta}_{\mathrm{t}}$ 包含预期系统间偏差的上限，并可进行调整以满足预先设定的虚警要求。基于时间的检查机制总结于图2。矩阵 $\boldsymbol{C}$ 有 $N_{\mathrm{c}} = 2\,(M-1)$ 行，其中 $\boldsymbol{\delta}_{\mathrm{t}}$ 包含 $M-1$ 个测量的系统间偏差上限。因此， $\boldsymbol{C}$ 具有 $M-1$ 个线性无关行。 $\boldsymbol{C}$ 的第 i行为 $\boldsymbol{c}_i$：它将与 $\boldsymbol{\delta}_{\mathrm{t}}$的第 i 个元素相关联，$\delta_{\mathrm{t},\,i}$，因此第 i项检查将为$\theta_{\mathrm{t},\,i} = \boldsymbol{c}_i\boldsymbol{H}\boldsymbol{r} \leq \delta_{\mathrm{t},\,i}$。例如， [21] 的作者提出通过时间一致性检查来认证计算所得的位置、速度和时间解。具体而言，他们考虑按照附录A所述的流程，结合来自两个星座的信号得到的位置、速度和时间解，其中一个星座发送认证信号，另一个发送开放信号。接着，将分别与每个星座的时间基准相关联的时钟偏差记为 t_1 和t_2 ，并在接收机处检查差值 $|t_1 - t_2|$ 是否与参考系统间偏差一致，以此认证位置、速度和时间解，

$$|(t_2 - t_1) - b - \mathrm{ISB}| < T\,, \tag{12}$$

其中， T 是由接收机设置的阈值， b 是在校准阶段设置的偏差。更多详情请参阅 安全性检查及参数推导的详细信息见 [21]。通过选择相应参数，可将检查式（12）纳入式（11）中，

$$\boldsymbol{C} = \begin{bmatrix} 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 & 1 \end{bmatrix}, \quad \boldsymbol{\delta}_{\mathrm{t}} = \begin{bmatrix} T + b + \mathrm{ISB} \\ T - b - \mathrm{ISB} \end{bmatrix}. \tag{13}$$

这意味着攻击者必须构造一个 $\Delta\boldsymbol{r}_{\mathrm{T}}$ ，使估计的时间偏移量最多改变 $\boldsymbol{\delta}_{\mathbf{t}}$。在本文的其余部分，我们将把这种方案称为基于*ISB*的交叉认证检查。

B. 面向授时服务的基于位置的检查

这里的目标是提供一个基于全球导航卫星系统的安全授时源。我们假设接收机先验知道其位置，其坐标记为 $\boldsymbol{p}_{\mathrm{ref}} = [x_{\mathrm{ref}}, y_{\mathrm{ref}}, z_{\mathrm{ref}}]$：这些坐标可以通过仅使用经由旁路接收的已认证伪距计算位置、速度和时间，也可以简单地预先获知（例如，在静态场景中）。然而，这些旁路都无法提供可靠的授时校正。因此，接收机利用所有可用的测量值，包括已认证的和开放的测量值，并获得位置、速度和时间解$\boldsymbol{p} = [x, y, z, t]$，其中包含所需的时钟偏差校正，如附录 B 所述。为验证其真实性，接收机验证重构的位置是否与其先验位置知识一致，验证

$$\theta_{\mathrm{pos}} \triangleq \sqrt{(x_{\mathrm{ref}} - x)^2 + (y_{\mathrm{ref}} - y)^2 + (z_{\mathrm{ref}} - z)^2} = \sqrt{\boldsymbol{\epsilon}^{\mathbf{T}}\boldsymbol{\epsilon}} \leq \delta_{\mathrm{pos}}\,. \tag{14}$$

其中， $\boldsymbol{\epsilon} \triangleq [x_{\mathrm{ref}} - x, y_{\mathrm{ref}} - y, z_{\mathrm{ref}} - z]$ 表示相对于参考位置的三维位置位移。基于位置的检查总结于图 3 中。如果检查通过，即使用所有信号计算出的位置与参考位置一致，则认为该解是安全的，接收机使用来自 $\boldsymbol{p}$ 的授时校正来校正本地时钟。 [18]描述了此类设置的一个示例。

IV. 提出的攻击策略

在本节中，我们概述攻击者用于在不向受害者接收机发出警报的情况下更改位置、速度和时间解的策略。首先，我们聚焦于理想的无噪声场景，其中攻击者和受害者接收到的信号均不受噪声影响。我们将在第五节中针对更现实的场景对该攻击进行推广。

若要攻击成功，攻击者必须 i）仅更改未受保护的信号，并选择 $\Delta \boldsymbol{r}_{\mathrm{T}}$，使得 ii） $\Delta \tilde{\boldsymbol{p}}$ 通过受害者采用的检查，且 iii）使受害者得到接近目标 $\boldsymbol{p}^{\star}$ 的位置、速度和时间解。在第一阶段，我们假设受害者接收到的信号符合攻击者的预期。此外，我们假设攻击者知道受害者在标称场景下会测得的伪距向量 $\boldsymbol{r}$。在第五节中，我们将分析攻击者无法预先补偿信道、受害者接收到被篡改信号的噪声更大副本的场景。

在以下各节中，我们将介绍针对授时和基于位置的检查的攻击策略。

A. 针对基于时间的检查的生成攻击

我们考虑一个采用第 III-A节所述检查的合法接收机，其中位置、速度和时间解被认为是真实可信的，并且时钟偏差差异与从侧信道导出的系统间偏差相一致。

首先，我们确定一组在接收机处不会触发警报的可行解。接下来，我们选择使接收机估计位置接近目标位置$\boldsymbol{p}^{\star}$的解。

为了确定可行解集，我们得到如下结果。

定理 1。 给定约束向量 $\boldsymbol{\delta}'$，包含所有不会在 (11) 中触发警报的范围改变量的攻击者可行解集合是仿射空间

$$S = \{\Delta \boldsymbol{r}_{\mathrm{p}} + s\,, s \in \mathcal{N}(\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}})\}\,, \tag{15}$$

其中， $\Delta \boldsymbol{r}_{\mathrm{p}}$ 是$\boldsymbol{\delta}' = \boldsymbol{C}\boldsymbol{H}_{\mathrm{O}}\Delta \boldsymbol{r}_{\mathrm{T,O}}$的一个解，而 $\mathcal{N}(\boldsymbol{X})$ 是 $\boldsymbol{X}$的零空间。此外，有

$$\dim(S) = N_{\mathrm{O}} - M + 1\,. \tag{16}$$

证明。 现在，条件 (11) 要求

$$\boldsymbol{C}\tilde{\boldsymbol{p}} = \boldsymbol{C}\hat{\boldsymbol{p}} + \boldsymbol{C}\Delta\tilde{\boldsymbol{p}} = \boldsymbol{C}\hat{\boldsymbol{p}} + \boldsymbol{C}\Delta\boldsymbol{p} + \boldsymbol{C}\Delta\boldsymbol{p}_{\mathrm{T}} \leq \boldsymbol{\delta}_{\mathrm{t}}\,. \tag{17}$$

我们假设在标称场景下，检查 (11) 得以通过，即 $\boldsymbol{C}\hat{}\,\boldsymbol{p} + \boldsymbol{C}\Delta\boldsymbol{p} = \boldsymbol{\delta}'' \leq \boldsymbol{\delta}_{\mathrm{t}}$：例如，这也模拟了防御者的测量值受到噪声影响的情况。因此，为避免触发警报，攻击者可以选择任意改变量，使其引起的变化小于 $\boldsymbol{\delta}_{\mathrm{t}} - \boldsymbol{\delta}''$，也就是说，根据 17，攻击者引起的偏移为

$$\boldsymbol{C}\Delta\boldsymbol{p}_{\mathrm{T}} \triangleq \boldsymbol{\delta}'\,,\ \ \boldsymbol{\delta}' \leq \boldsymbol{\delta}_{\mathrm{t}} - \boldsymbol{\delta}''\,. \tag{18}$$

利用 (5)，并考虑到攻击者只能操纵未受保护的信号，我们有

$$\begin{aligned}\boldsymbol{\delta}' = \boldsymbol{C}\Delta\boldsymbol{p}_{\mathrm{T}} = \boldsymbol{C}\boldsymbol{H}\Delta\boldsymbol{r}_{\mathrm{T}} &= \boldsymbol{C}\begin{bmatrix}\boldsymbol{H}_{\mathrm{A}} & \boldsymbol{H}_{\mathrm{O}}\end{bmatrix}\begin{bmatrix}\boldsymbol{0}\\ \Delta\boldsymbol{r}_{\mathrm{T,O}}\end{bmatrix} \\ &= \boldsymbol{C}\boldsymbol{H}_{\mathrm{O}}\Delta\boldsymbol{r}_{\mathrm{T,O}}\,.\end{aligned} \tag{19}$$

由于 $\boldsymbol{\delta}'$ 由攻击者控制，他可以将其选为满足 $\boldsymbol{\delta}' \in \mathcal{R}($ $\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}})$ 的值，从而使 (19) 至少有一个解。事实上，$\operatorname{rank}(\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}}) = M - 1$，因为 $\boldsymbol{C}$ 有 $M-1$ 个线性无关行。[1] 乘积$\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}}$ 得到的矩阵大小为 $N_{\mathrm{c}} \times N_{\mathrm{O}}$。

[1]我们作出了默示假设，即 $N_{\mathrm{O}} \geq M$，且几何结构使得 $\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}}$ 具有满行秩。

因此，根据 Rouch´e-Capelli定理，(19) 描述了一个具有无穷多个解的线性非定方程组，这些解属于(15)中定义的仿射空间 S，其中 $\Delta \boldsymbol{r}_{\mathrm{p}}$ 是(19)的任意一个特解，例如可以通过高斯消元法求得。此外，由于仿射空间的维数就是其对应线性空间的维数，我们有

$$\begin{aligned}\dim(S) &= \dim(\mathcal{N}(\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}})) \\ &= N_{\mathrm{O}} - \operatorname{rank}(\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}}) = N_{\mathrm{O}} - M + 1 > 1\,.\end{aligned} \tag{20}$$

因此，19 的每个解都取决于 $N_{\mathrm{O}} - M + 1$ 参数。

□

上述定理有两个主要推论。首先，考虑攻击者的最坏情况，此时合法的测距残差 $\Delta \boldsymbol{r}$ 已经产生了 $\boldsymbol{C}\Delta\boldsymbol{p} = \boldsymbol{\delta}$。在这种情况下，攻击者没有任何余地，必须根据 18 选择一个满足 $\boldsymbol{\delta}' = 0$ 的攻击。然而，(15) 表明，通过从零空间 $\mathcal{N}(\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}})$ 中选择测距值，仍然有可能实施成功的攻击。

其次，这表明，合法接收机在计算位置、速度和时间解时使用的信号数量增加，可能会使攻击者拥有更大的自由度来操纵伪造的位置、速度和时间解，因为零空间的维度会随之增大。然而，在遭受攻击时，使用更多开放信号可以提高位置、速度和时间估计的准确性。因此，这里需要在准确性与安全性之间权衡。最后，可能存在 $N_{\mathrm{A}} < 4$的情形，因此根本无法获得完全经过身份验证的位置、速度和时间解。在这些情况下，受害者接收机必须增加用于位置、速度和时间解的开放信号数量，否则就不计算位置、速度和时间解。

接下来，我们推导使受害者接收机到达目标位置 $\boldsymbol{p}^{\star}$ 的实际距离改变量。我们考虑对攻击者而言最坏的情况，即 $\boldsymbol{\delta}' = \boldsymbol{0}$。在这种情况下，(19) 描述了一个线性齐次系统，其解属于线性空间 $S = \mathcal{N}(\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}})$。事实上，只需在计算中加入与特解相关的距离向量 $\Delta \boldsymbol{r}_{\mathrm{p}}$，即可归结为一般情况。因此，属于 S 的任意解都可以写成

$$\Delta\boldsymbol{r}_{\mathrm{T}} = \begin{bmatrix}\boldsymbol{u}_1 & \ldots & \boldsymbol{u}_K\end{bmatrix}\begin{bmatrix}\alpha_1\\ \ldots\\ \alpha_K\end{bmatrix} = \boldsymbol{U}\boldsymbol{\alpha}\,, \tag{21}$$

其中 $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_K$是 S 的一个正交归一基， $\alpha_k \in \mathbb{R}\ \forall k =$1, … , K, 且 $K \triangleq \dim(S)$。注意， $\boldsymbol{U}$是一个具有$3 + M$行和 K列的矩阵。

目标位置和虚假位置通过.....相关

$$\begin{aligned}\tilde{\boldsymbol{p}} - \boldsymbol{p}^{\star} = \Delta\tilde{\boldsymbol{p}} - \Delta\boldsymbol{p}^{\star} &= \boldsymbol{H}\Delta\boldsymbol{r}_{\mathrm{T}} - (\Delta\boldsymbol{p}^{\star} - \Delta\boldsymbol{p}) \\ &= \boldsymbol{H}\boldsymbol{U}\boldsymbol{\alpha} - (\Delta\boldsymbol{p}^{\star} - \Delta\boldsymbol{p})\,,\end{aligned} \tag{22}$$

其中，在最后一步中，我们利用了这样一个事实：攻击者只会采用不会触发警报的距离改变量，即属于（15）的改变量，因此具有（22）中的形式。

通过强制目标位置与伪造位置重合，即 $\tilde{\boldsymbol{p}} = \boldsymbol{p}^{\star}$，我们有

$$\boldsymbol{H}\boldsymbol{U}\boldsymbol{\alpha} = \Delta\boldsymbol{p}^{\star} - \Delta\boldsymbol{p}, \tag{23}$$

并借助摩尔－彭若斯伪逆，我们得到

$$\boldsymbol{\alpha}^{\star} = \left(\boldsymbol{U}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H}\boldsymbol{U}\right)^{-1}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}}\left(\Delta\boldsymbol{p}^{\star} - \Delta\boldsymbol{p}\right). \tag{24}$$

最后，将其代入（21），即可得到目标距离改变量

$$\Delta\boldsymbol{r}_{\mathrm{T}}^{\star} = \alpha_1^{\star}\boldsymbol{u}_1 + \ldots + \alpha_K^{\star}\boldsymbol{u}_K\,. \tag{25}$$

确实，如要求的那样，该攻击不会触发任何警报，同时会将受害者准确带到 $\boldsymbol{p}^{\star}$。

或者，通过利用（22），我们可以直接选择在不会触发警报的解中，使诱导位置与目标位置之间的距离最小的解，即

$$\Delta\boldsymbol{r}_{\mathrm{T}}^{\star} = \underset{\Delta\boldsymbol{r}_{\mathrm{T}}\in S}{\arg\min}\,\|\boldsymbol{H}\Delta\boldsymbol{r}_{\mathrm{T}} - (\Delta\boldsymbol{p}^{\star} - \Delta\boldsymbol{p})\|^2\,. \tag{26}$$

确实，只要空间 S 非空，就可以通过数值方法求解该问题。

针对基于 *GGTO* 的交叉认证检查的攻击：我们考虑[21]中的认证过程，并利用前面的分析推导该攻击。[21]中提出的技术仅考虑来自伽利略和 GPS 的信号，因此我们有 $M = 2$。根据（16），我们预计可以找到一个可行解空间 S，其大小为 $\dim(S) = N_{\mathrm{O}} - 1$。我们考虑攻击者的最坏情况，即$\boldsymbol{\delta}' = \mathbf{0}$。结合（13）和（19），并将 $\boldsymbol{h}_{\mathrm{O},i}$ 记为 $\boldsymbol{H}_{\mathrm{O}}$的第$i$行，我们有

$$\boldsymbol{C}\boldsymbol{H}_{\mathrm{O}}\Delta\boldsymbol{r}_{\mathrm{T,O}} = \mathbf{0} \Leftrightarrow (\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5})\Delta\boldsymbol{r}_{\mathrm{T,O}} = 0\,. \tag{27}$$

因此，$\Delta\boldsymbol{r}_{\mathrm{T,O}}$ 属于零空间 $\mathcal{N}(\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5})$。这对应于由列向量$(\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5})^{\mathrm{T}}$生成的空间的正交补，或者

$$S = \mathcal{N}(\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5}) = \left\langle(\boldsymbol{h}_{\mathrm{O},4} - \boldsymbol{h}_{\mathrm{O},5})^{\mathrm{T}}\right\rangle^{\perp}. \tag{28}$$

考虑到 $\boldsymbol{h}_{\mathrm{O},4}$ 和 $\boldsymbol{h}_{\mathrm{O},5}$ 是长度为N_{O}的列向量，(28)中的零空间显然大小为 $N_{\mathrm{O}} - 1$，并且如预期，$\dim(S) = N_{\mathrm{O}} - 1$。

B. 针对基于位置的检查的攻击

我们考虑第 III-B 节所述的检查类别。在这里，受害者使用 GNSS 进行授时，同时按照附录B 中概述的过程监测自身位置，该过程用于安全检查：例如，[18]中介绍了这样一种场景：在一栋建筑内，使用 GNSS信号对局域网（LAN）的时钟进行同步。事实上，在这种情况下，位置是已知的，因此攻击者只能篡改授时估计，并诱导产生如下类型的位置、速度和时间偏移

$$\Delta\boldsymbol{p}_{\mathrm{T}} = \begin{bmatrix}\xi_x\\ \xi_y\\ \xi_z\\ c\gamma_T\end{bmatrix} = \begin{bmatrix}\xi_x\\ \xi_y\\ \xi_z\\ 0\end{bmatrix} + \begin{bmatrix}0\\ 0\\ 0\\ c\gamma_T\end{bmatrix} = \boldsymbol{\xi} + \begin{bmatrix}0\\ 0\\ 0\\ c\gamma_T\end{bmatrix}, \tag{29}$$

其中，$c\gamma_T$ 是攻击者对受害者时钟施加的时间偏移。为避免触发警报，根据（14），我们需要 $\|\boldsymbol{\xi}\|^2 \leq \delta_{\mathrm{pos}}$。

在接下来的段落中，我们将介绍针对基于位置的检查的中继攻击和生成攻击。使用其中任一种，攻击者都能够诱使目标发生时间偏移。

(29).尽管生成攻击可能更可取，因为例如它不会由于攻击者接收机噪声而在受害者处引入额外噪声，但我们将证明，只有当受害者使用 $N_{\mathrm{O}} \geq 4$ 信号时，才能实施这种攻击。

a) 针对基于位置的检查的中继攻击：从 29 开始，该攻击可以直接从 4 计算得出，如下

$$\Delta\boldsymbol{r}_{\mathrm{T}} = \boldsymbol{G}\Delta\boldsymbol{p}_{\mathrm{T}} = c\gamma_T\mathbf{1} + G\boldsymbol{\xi}\,, \tag{30}$$

其中，$\mathbf{1}$ 是一个与 $\boldsymbol{p}$大小相同的全1向量。在对攻击者最不利的情况下，$\|\boldsymbol{\xi}\| = 0$，或者等价地，$\delta_{\mathrm{pos}} = 0$，即合法接收机不容许位置发生任何变化，则可得

$$\Delta\boldsymbol{r}_{\mathrm{T}} = c\gamma_T\mathbf{1}\,. \tag{31}$$

这意味着，攻击者必须接收、记录并延迟转发经过认证的信号和开放信号，才能实施所需的攻击，这通常也是转发欺骗攻击的做法。另一方面，这也表明，选择 $\boldsymbol{\xi} \neq \mathbf{0}$ 时，我们选取的解与转发欺骗解的差异至多为 $G\boldsymbol{\xi}$。

最后需要注意的是，正如第 II-B 节所指出的，即使测距值经过 SCE 或 SCA 认证，这种攻击仍然可以实施。不过，只有当攻击者距离受害者足够近时，这种方法才可行。反过来，这也可能导致位置计算结果不同，从而引起受害者警觉。然而，尤其是在考虑现实场景时，中继攻击可能会引入额外噪声。因此，如果可能，攻击者甚至会在针对基于位置的检查时采用生成攻击。基于这一原因，下一段将介绍一种针对基于位置的检查的生成攻击策略。

b) 针对基于位置的检查的生成攻击：本节将说明攻击者如何以及何时能够针对基于位置的检查实施生成类攻击。攻击者旨在使估计的时钟偏差产生等于 $c\gamma_{\mathrm{T}}$ 的时间偏移，如式（31）所示。因此，攻击者利用式（5）的线性化过程并结合式（29），必须选择 Δr_{T}，以获得

$$\boldsymbol{H}\Delta\boldsymbol{r}_{\mathrm{T}} = \begin{bmatrix}0\\ 0\\ 0\\ c\gamma_T\end{bmatrix}. \tag{32}$$

事实上，满足（32）的距离改变量 $\Delta\boldsymbol{r}_{\mathrm{T}}$ 仅会导致受害者计算出的 PVT 解中的时间分量发生偏移。我们指出，为便于阅读，本文聚焦于 $\|\xi\| = 0$ 的最坏情况场景。通过在（32）中添加项 $\boldsymbol{G\xi}$，也可以轻松扩展到 $\boldsymbol{\xi} \neq \mathbf{0}$ 的情况。

与第 IV-A 节所概述的过程类似，我们有 32 的可行解集合是仿射空间

$$S = \{\Delta\boldsymbol{r}_{\mathrm{p}} + s\,, s \in \mathcal{N}(\boldsymbol{H})\}\,. \tag{33}$$

其中，根据31，特定解决方案是转发欺骗攻击$\Delta\boldsymbol{r}_{\mathrm{p}} = c\gamma_{\mathrm{T}}\mathbf{1}$。

确实，$\boldsymbol{H}$ 是 $4 \times N$ 且$\mathrm{rank}(\boldsymbol{H}) = 4$，因此

$$\dim(\mathcal{N}(\boldsymbol{H})) = \mathcal{R}(\boldsymbol{H}) - \mathrm{rank}(\boldsymbol{H}) = N - 4. \tag{34}$$

我们指出，为了计算位置、速度和时间， $N \geq 4$ 始终成立，因此 $\dim(\mathcal{N}(\boldsymbol{H})) \geq 0$。因此，任何导致目标时间偏移的测距篡改都可以写成

$$s = c\gamma_{\mathrm{T}}\mathbf{1} + \sum_{n=1}^{N-4} \beta_n \boldsymbol{u}_n = c\gamma_{\mathrm{T}}\mathbf{1} + \boldsymbol{U}\boldsymbol{\beta} \tag{35}$$

其中向量 $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{N-4}$ 构成零空间 $\mathcal{N}(\boldsymbol{H})$ 的一组基，并作为基矩阵 $\boldsymbol{U}$ 的列。

我们的目标是找到属于 S 且无需对已认证伪距进行任何改变量的测距篡改。后一项要求形式化为

$$\boldsymbol{U}_{N_{\mathrm{A}}}\boldsymbol{\beta} + c\gamma_{\mathrm{T}}\mathbf{1}_{N_{\mathrm{A}}} = 0\,, \tag{36}$$

其中， $\boldsymbol{U}_{N_{\mathrm{A}}}$ 和 $\mathbf{1}_{N_{\mathrm{A}}}$ 分别收集 $\boldsymbol{U}$ 和 $\mathbf{1}$ 的前 N_{A} 行。

要使 (36) 至少有一个解，一个充分条件是 $\boldsymbol{U}_{N_{\mathrm{A}}}$（大小为 $N_{\mathrm{A}} \times N-4$）可左逆。当 $N_{\mathrm{A}} < (N-4)$ 时满足此条件，等价地， $N_{\mathrm{O}} > 4$.[2] 此外，这也能保证 $c\gamma_{\mathrm{T}}\mathbf{1}_{N_{\mathrm{A}}} \in \mathcal{R}(\boldsymbol{H})$。在此条件下，使 (36) 成立的系数向量计算如下：

$$\boldsymbol{\beta}^{\star} = -c\gamma_{\mathrm{T}} \left(\boldsymbol{U}_{N_{\mathrm{A}}}^{\mathrm{T}}\boldsymbol{U}_{N_{\mathrm{A}}}\right)^{-1} \boldsymbol{U}_{N_{\mathrm{A}}}^{\mathrm{T}}\mathbf{1}_{N_{\mathrm{A}}}\,. \tag{37}$$

最后，对于生成攻击，攻击者必须选取伪距

$$\Delta\boldsymbol{r}^{\star} = c\gamma_{\mathrm{T}}\mathbf{1} + \sum_{n=1}^{N-4} \beta_n^{\star}\boldsymbol{u}_n\,. \tag{38}$$

事实上，根据 $\boldsymbol{\beta}^{\star}$ 的构造， $\Delta r_n^{\star} = 0$ 对于 $1 \leq n \leq N_{\mathrm{A}}$ 成立，因此只需篡改开放信号。

总之，我们证明了，如果 $N_{\mathrm{O}} \geq 4$，攻击者便可利用刚才描述的流程实施生成型攻击，使受害者时间偏移 γ_{T} 倍，且仅生成开放信号。

V. 现实场景分析

在本节中，我们分析在考虑受害者接收机和攻击者接收机噪声的现实场景下的攻击性能。我们指出，当攻击者执行生成攻击时，伪造信号仅受到受害者接收机所添加噪声的影响。另一方面，当攻击者执行中继攻击时，篡改信号同时受到受害者接收机和攻击者接收机产生的噪声影响。我们假设攻击者和受害者的卫星与接收机之间的信道，以及攻击者与受害者之间的信道，均为加性高斯白噪声（AWGN）信道。我们分别用 σ_{L} 和 σ_{A} 表示受害者接收机和攻击者接收机处的噪声标准差。此外，按照GNSS中的通常做法，我们假设每个信道彼此独立且具有相同的方差。

噪声会影响伪距估计，因此，合法伪距残差和篡改伪距残差的协方差矩阵分别为。

$$\boldsymbol{\Sigma}_{\mathrm{L}} = \mathrm{cov}(\Delta\boldsymbol{r}) \triangleq \sigma_{\mathrm{L}}^2\boldsymbol{I}_N\,, \quad \boldsymbol{\Sigma}_{\mathrm{T}} = \mathrm{cov}(\Delta\widetilde{\boldsymbol{r}}) \triangleq \sigma_{\mathrm{T}}^2\boldsymbol{I}_N\,, \tag{39}$$

[2]在条件 $N_{\mathrm{O}} > 4$下， $\boldsymbol{U}_{N_{\mathrm{A}}}$ 只有当零空间 $\mathcal{N}(\boldsymbol{H})$ 的基向量 $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{N-4}$ 以使 $\boldsymbol{U}_{N_{\mathrm{A}}}$ 具有满行秩的方式选取时才是左可逆的。

其中，当攻击者实施生成攻击时为 $\sigma_{\mathrm{T}}^2 = \sigma_{\mathrm{L}}^2$，当其实施中继攻击时为 $\sigma_{\mathrm{T}}^2 = \sigma_{\mathrm{L}}^2 + \sigma_{\mathrm{A}}^2$。此外，在位置、速度和时间迭代计算收敛时，合法的伪距残差均值为零。考虑到攻击者引入的额外篡改，被篡改伪距的均值为

$$\mathbb{E}\left[\Delta\widetilde{\boldsymbol{r}}|\mathcal{H}_1\right] = \mathbb{E}\left[\Delta\boldsymbol{r} + \Delta\boldsymbol{r}_{\mathrm{T}}\right] = \Delta\boldsymbol{r}_{\mathrm{T}}\,. \tag{40}$$

在接下来的各节中，我们分别讨论针对授时检查和基于位置的检查的攻击。

A. 对基于时间的检查的攻击

我们的目标是在现实条件下对公式 (11) 中定义的向量 $\boldsymbol{\theta}_{\mathrm{t}}$ 进行统计刻画。事实上， $\boldsymbol{\theta}_{\mathrm{t}} = \boldsymbol{C}\boldsymbol{H}\Delta\boldsymbol{r}$ 是一个高斯向量，因为它源自高斯向量 $\Delta\boldsymbol{r}$ 的线性组合。因此，为了对其进行刻画，我们必须计算其均值和协方差，同时考虑合法条件和遭受攻击的条件。

在合法场景中， $\mathcal{H}_0$，均值是

$$\mathbb{E}[\boldsymbol{\theta}_{\mathrm{t}}|\mathcal{H}_0] = \boldsymbol{C}\boldsymbol{H}\mathbb{E}[\Delta\boldsymbol{r}|\mathcal{H}_0] = 0\,, \tag{41}$$

而 $\boldsymbol{\theta}_{\mathrm{t}}$ 在 $\mathcal{H}_0$ 中的协方差是

$$\begin{aligned}\boldsymbol{\Sigma_0} \triangleq \mathbb{E}\left[\boldsymbol{\theta}_{\mathrm{t}}\boldsymbol{\theta}_{\mathrm{t}}^{\mathrm{T}}|\mathcal{H}_0\right] = \mathbb{E}\left[\boldsymbol{C}\boldsymbol{H}\Delta\boldsymbol{r}(\boldsymbol{C}\boldsymbol{H}\Delta\boldsymbol{r})^{\mathrm{T}}|\mathcal{H}_0\right] = \\ \boldsymbol{C}\boldsymbol{H}\mathbb{E}\left[\Delta\boldsymbol{r}\Delta\boldsymbol{r}^{\mathrm{T}}\right]\boldsymbol{H}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}} = \sigma_{\mathrm{L}}^2\boldsymbol{C}\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\,,\end{aligned} \tag{42}$$

其中，在最后一步中，我们使用了式（39）中给出的 $\boldsymbol{\Sigma}_L$ 的定义。

对于受攻击场景， $\mathcal{H}_1$，均值为

$$\mathbb{E}[\boldsymbol{\theta}_{\mathrm{t}}|\mathcal{H}_1] = \boldsymbol{C}\boldsymbol{H}\Delta\boldsymbol{r}_{\mathrm{T}} \triangleq \boldsymbol{\mu}\,, \tag{43}$$

而与 (42) 类似， $\mathcal{H}_1$ 中 $\boldsymbol{\theta}_{\mathrm{t}}$ 的协方差为

$$\boldsymbol{\Sigma_1} \triangleq \mathbb{E}\left[\boldsymbol{\theta}_{\mathrm{t}}\boldsymbol{\theta}_{\mathrm{t}}^{\mathrm{T}}|\mathcal{H}_1\right] = \sigma_{\mathrm{T}}^2\boldsymbol{C}\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{C}^{\mathrm{T}}\,. \tag{44}$$

其中，最后一个等式由（39）中给出的 $\boldsymbol{\Sigma}_T$ 定义得到。此外，第 IV-A 节所述的针对基于时间的检查的攻击是一种生成攻击，因此 $\sigma_{\mathrm{T}}^2 = \sigma_{\mathrm{L}}^2$。

虚警概率和漏检概率分别为，

$$p_{\mathrm{FA}} = \mathrm{P}\left[\bigcup_{i=1}^{N_{\mathrm{c}}}\{\theta_{\mathrm{t},i} > \delta_{\mathrm{t},i}\}|\mathcal{H}_0\right] = 1 - \mathrm{P}\left[\bigcap_{i=1}^{N_{\mathrm{c}}}\{\theta_{\mathrm{t},i} \leq \delta_{\mathrm{t},i}\}|\mathcal{H}_0\right], \tag{45}$$

$$p_{\mathrm{MD}} = \mathrm{P}\left[\bigcap_{i=1}^{N_{\mathrm{c}}}\{\theta_{\mathrm{t},i} \leq \delta_{\mathrm{t},i}\}|\mathcal{H}_1\right]. \tag{46}$$

我们指出，一般而言，指标 $\theta_{\mathrm{t},\,i}$ 和 $\theta_{\mathrm{t},\,j}$（其中 $i \neq j$）在统计上并不独立。

针对基于*ISB*的交叉认证检查的攻击： 我们现在考虑 [21],的检查，其中仅考虑伽利略和GPS。首先，我们忽略偏差 $b+GGTO$，该偏差可以预先从一个测量值中减去。因此，可得 $\delta_{\mathrm{t},1} = \delta_{\mathrm{t},2} = T$。此外，由 13, $\boldsymbol{c}_1 = -\boldsymbol{c}_2$ 可知，因此也有 $\theta_{\mathrm{t},1} = -\theta_{\mathrm{t},2}$，于是 (45) 变为

$$\begin{aligned}p_{\mathrm{FA}} &= 1 - P(\theta_{\mathrm{t},1} < T \wedge \theta_{\mathrm{t},2} < T|\mathcal{H}_0) \\ &= 1 - P(-\delta_1 < \theta_{\mathrm{t},1} < T|\mathcal{H}_0) = 2Q(T/\sigma_0)\,,\end{aligned} \tag{47}$$

其中 $\sigma_0 = \sigma_{\mathrm{L}}\sqrt{\boldsymbol{c}_1\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{c}_1^{\mathrm{T}}}$。接下来，我们可以将上述关系反转，以计算接收机设定的 p_{FA} 的阈值，

$$T = \sigma_0 \mathrm{Q}^{-1}\left(\frac{1}{2}p_{\mathrm{FA}}\right). \tag{48}$$

类似地，将 μ_1 和 μ_2 分别称为 $\boldsymbol{\mu}$的第一和第二个元素，则漏检概率为

$$\begin{aligned} p_{\mathrm{MD}} &= P(\theta_{\mathrm{t},1} \le \delta_{\mathrm{t},1} \wedge \theta_{\mathrm{t},2} \le \delta_{\mathrm{t},2}|\mathcal{H}_1) \\ &= \mathrm{Q}\left(\frac{-T-\mu_1}{\sigma_1}\right) - \mathrm{Q}\left(\frac{T-\mu_1}{\sigma_1}\right) \\ &= \mathrm{Q}\left(-\frac{\sigma_0}{\sigma_1}\mathrm{Q}^{-1}\left(\frac{1}{2}p_{\mathrm{FA}}\right) - \frac{\mu_1}{\sigma_1}\right) - \\ &\quad -\mathrm{Q}\left(\frac{\sigma_0}{\sigma_1}\mathrm{Q}^{-1}\left(\frac{1}{2}p_{\mathrm{FA}}\right) - \frac{\mu_1}{\sigma_1}\right), \end{aligned} \tag{49}$$

其中 $\mu_1 = -\mu_2 = \boldsymbol{c}_1\boldsymbol{H}\Delta\boldsymbol{r}_{\mathrm{T}}$ 和 $\sigma_1 = \sigma_{\mathrm{T}}\sqrt{\boldsymbol{c}_1\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{c}_1^{\mathrm{T}}}$。因此，(49)展示了漏检概率与虚警、合法信道噪声、攻击者信道噪声以及 $\boldsymbol{\mu}$之间的函数关系。特别是， $\boldsymbol{\mu}$ 还与攻击者造成的距离改变量有关，而该改变量是由真实解 $\boldsymbol{p}$ 与目标 $\boldsymbol{p}^{\star}$之间的距离决定的。

在生成攻击场景中，若 $\sigma_0 = \sigma_1$，当 μ_1较小时，由 49 可得 $p_{\mathrm{MD}} = p_{\mathrm{FA}}$，这意味着伪造信号与合法信号无法区分。这表明成功概率取决于 μ_1，即攻击者造成的位移量；因此，攻击者越是试图篡改信号，受害者就越容易检测到攻击。例如，若我们考虑通过选择性延迟进行位置欺骗的中继攻击，则 $\sigma_1 \gg \sigma_0$，也就是说，被篡改伪距的噪声标准差高于合法伪距的噪声标准差， $p_{\mathrm{MD}} \to 0$ 对于任意选定的 p_{FA}，因此接收机始终能够检测到攻击。在第 VI-C节中，我们将对这些观察结果进行数值评估。

B. 针对基于位置的检查的攻击

我们的目标是在现实环境中，即测量值受到噪声影响时，对式（14）中的项 θ_{pos} 进行统计表征。具体而言，我们旨在将安全性能，即误报和漏检，与合法情形和受攻击场景中的信道噪声联系起来， σ_{L}^2 和 σ_{T}^2。请注意，在合法情形下，这一问题等同于 GNSS 定位精度的一般表征问题。

由（14）可得

$$\theta_{\mathrm{pos}}^2 = \boldsymbol{\epsilon}^{\mathrm{T}}\boldsymbol{\epsilon}\,, \tag{50}$$

其中， $\boldsymbol{\epsilon}$ 是相对于参考位置的三维位置位移。我们指出，假设坐标为 $(x_{\mathrm{ref}},\ y_{\mathrm{ref}},\ z_{\mathrm{ref}})$ 的参考位置是已知且无误差的。因此，为了表征检验（14）的性能，我们首先对项 $\boldsymbol{\epsilon}$ 进行建模。实际上， $\boldsymbol{\epsilon}$ 是一个高斯向量，因为位置是由高斯随机向量 $\Delta\boldsymbol{r}$的线性组合得出的，如式（5）所示。在合法情形下，我们有

$$\mathbb{E}[\boldsymbol{\epsilon}|\mathcal{H}_0] = 0\,, \tag{51}$$

因为预计位置、速度和时间解会收敛到参考位置本身。对于协方差，我们有

$$\mathbb{E}[\boldsymbol{\epsilon}\boldsymbol{\epsilon}^{\mathrm{T}}|\mathcal{H}_0] = \sigma_{\mathrm{L}}^2\boldsymbol{H}_{1-3}\boldsymbol{H}_{1-3}^{\mathrm{T}}\,, \tag{52}$$

其中 $\boldsymbol{H}_{1-3}$ 的下标表示我们仅考虑 $\boldsymbol{H}$ 的第 1、2 和 3 行。

在遭受攻击时，我们有

$$\mathbb{E}[\boldsymbol{\epsilon}|\mathcal{H}_1] = \boldsymbol{H}_{1-3}\Delta\boldsymbol{r}_{\mathrm{T}}\,, \tag{53}$$

以及对于协方差，

$$\mathbb{E}[\boldsymbol{\epsilon}\boldsymbol{\epsilon}^{\mathrm{T}}|\mathcal{H}_0] = \sigma_{\mathrm{T}}^2\boldsymbol{H}_{1-3}\boldsymbol{H}_{1-3}^{\mathrm{T}}\,. \tag{54}$$

请注意，(50) 是一个二次型，因此我们可以利用以下定理。

定理 2。 随机变量 $\theta_{\mathrm{pos}}^2 = \boldsymbol{\epsilon}^{\mathrm{T}}\boldsymbol{\epsilon}$，其中 $\boldsymbol{\epsilon} \sim \mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$，可写为

$$\theta_{\mathrm{pos}}^2 = (\boldsymbol{u}+\boldsymbol{b})\,\boldsymbol{\Lambda}\,(\boldsymbol{u}+\boldsymbol{b}) = \sum_i^3 \lambda_i(u_i+b_i)^2\,, \tag{55}$$

其中 $\boldsymbol{u} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{I}_3)$， $\boldsymbol{\Lambda}$ 是由分解 $\boldsymbol{\Sigma} = \boldsymbol{P}\boldsymbol{\Lambda}\boldsymbol{P}_{\mathrm{T}}$ 和 $\boldsymbol{b}^{\mathrm{T}} = \boldsymbol{P}_{\mathrm{T}}\boldsymbol{\Sigma}^{-\frac{1}{2}}\boldsymbol{\mu}$ 得到的对角矩阵。因此，θ_{pos}^2 可表示为自由度为 $\boldsymbol{1}$ 的非中心卡方随机变量的线性组合，其非中心参数为 b_i^2。

证明。关于二次型 $Q(\boldsymbol{X}) = \boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{X}$ 的证明可见 [25,第 3]章，但这里使用的是 $\boldsymbol{A} = \boldsymbol{I}$。 □

实际上，在合法情形下， ϵ 的均值为零，因此， θ^2 实际上是自由度为 1 的（中心）卡方随机变量的线性组合。不过，无法推导出虚警概率或漏检概率的闭式表达式，因此也就无法将指标值 θ_{pos} 与所选阈值联系起来。

若要以应用为导向（但近似地）推导这种关系，我们可以利用几何精度因子（GDOP）的定义 [23, 第 7]章。首先，我们旋转参考系，使前三个坐标轴分别指向东、北、上（ENU）方向。接着，重复（52）中的步骤，可得位置误差

$$\mathbb{E}\left[\Delta\boldsymbol{p}\Delta\boldsymbol{p}^{\mathrm{T}}\right] = \sigma_L^2\boldsymbol{H}\boldsymbol{H}^{\mathrm{T}} = \sigma_L^2\left(\boldsymbol{G}^{\mathrm{T}}\boldsymbol{G}\right)^{-1}. \tag{56}$$

因此，通过求迹运算，我们将 GDOP 定义为

$$\mathrm{GDOP} \triangleq \frac{1}{\sigma_L}\sqrt{\sigma_{\mathrm{E}}^2 + \sigma_{\mathrm{N}}^2 + \sigma_{\mathrm{U}}^2 + \sigma_{\mathrm{t}}^2}\,, \tag{57}$$

其中， σ_{E}^2、 σ_{N}^2和 σ_{U}^2 分别为东向、北向和垂直方向误差的方差，而 σ_{t}^2 为时钟偏差（以米为单位）。为聚焦于位置误差，可以考虑位置精度因子（PDOP）

$$\mathrm{PDOP} \triangleq \frac{1}{\sigma_L}\sqrt{\sigma_{\mathrm{E}}^2 + \sigma_{\mathrm{N}}^2 + \sigma_{\mathrm{U}}^2}\,, \tag{58}$$

这些术语用于对定位误差进行建模，因此也用于预测定位误差，因为精度因子（DOP）值与伪距噪声和几何结构相关。因此，低DOP值通常与高位置、速度和时间相关

精度。关于 DOP 及其推导的进一步深入讨论，可参见 [24, 第 21] 章。

因此，可以使用这一特征来描述$p(\theta_{\mathrm{pos}}|\mathcal{H}_0)$和 $p(\theta_{\mathrm{pos}}|\mathcal{H}_1)$。不过，这些估计仅基于一个近似模型，并不适用于安全性分析。因此，位置检查的性能将仅在第VI-C节中通过数值方法进行评估。

VI. 数值结果

在本节中，我们评估所提出的攻击对第 III 节所讨论的认证机制的效果。具体而言，我们首先介绍数据收集流程和验证阶段。接下来，我们测试第 IV 节中的两种攻击，分别考虑无噪声场景和有噪声场景。

A. 数据收集

该数据集通过使用连接到 A42 Hemisphere 天线的 Septentrio PolarRx5 接收机，在准城市环境中采集信号构建而成。具体而言，测量数据采集自我们实验室的窗台（45.408°N，11.894° E，海拔 30 米）。

对接收机输出进行后处理，得到一个包含来自不同星座的测量值的数据集。我们重点研究了 GPS L1 C/A 和伽利略 E1 BC。该数据集包含 10 分钟的测量值，采集频率为 1 Hz，共计 600 个位置、速度和时间历元。我们将 GPS 信号视为已认证信号（例如，通过 CHIMERA 认证），将伽利略信号视为开放信号；采集到的信号来自视野内的 $N = 8$ 颗不同卫星，且具有 $N_{\mathrm{A}} = 3$ 和 $N_{\mathrm{O}} = 5$。

具体而言，对于每个考虑的历元，数据集包含：伪距测量值、卫星时钟偏差、对流层和电离层延迟（使用 Klobuchar 模型 [26] 估算），以及卫星位置。卫星时钟偏差、大气延迟和卫星位置均根据相应的导航电文得出。

为测试攻击的性能，我们按照附录中的总结实现了一个位置、速度和时间计算模块，并遵循 [27, 第 8] 章的描述。

为验证我们的 PVT区块，我们在图4 中分别报告了由 Septentrio接收机计算的位置（蓝色）以及由我们的 PVT区块计算的位置（红色）。从 Septentrio 接收机获得的位置比我们的结果略为精确：使用 Septentrio 接收机和我们的 PVT区块时，误差标准差分别为 3.03 米和 3.13米。

B. 理想场景条件下的攻击

现在，我们展示无噪声场景下的攻击性能，因此 $\sigma_{\mathrm{L}} = \sigma_{\mathrm{T}} = 0$，并区分针对基于时间的检查和基于位置的检查的攻击。

a) 针对基于时间的检查的攻击：我们展示所提出攻击的结果。具体而言，我们采用以下流程，在每个历元中我们

1) 使用合法测量值计算位置、速度和时间解（合法情形）；

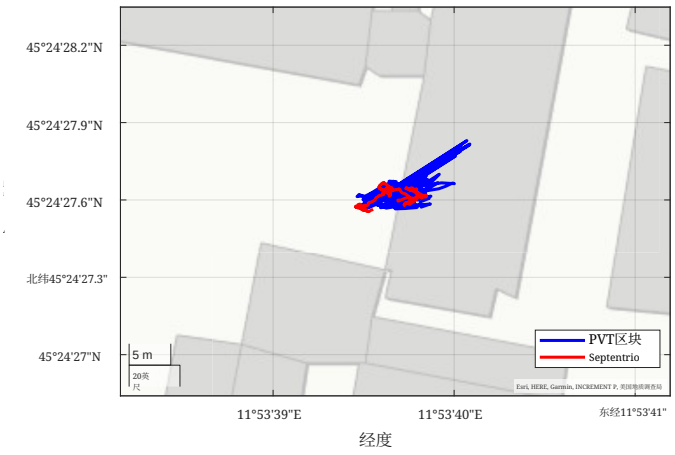


图 4. 对我们的 PVT 区块进行验证：使用我们的 PVT 区块（蓝色）和 Septentrio 软件（红色）计算的位置。

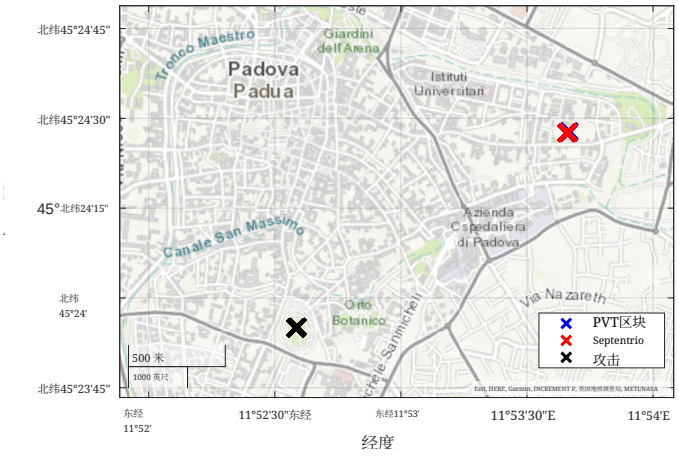


图 5. 合法场景（蓝色）和受攻击场景（黑色）中计算的位置，与真实位置（红色）进行比较。受攻击场景中计算的位置与目标 $\boldsymbol{p}^{\star}$ 重合。

2) 选择目标位置 $\boldsymbol{p}_1^{\star}$；3) 求解问题 (26)，获得篡改后的距离 $\Delta\widetilde{r}$；4) 将篡改后的距离输入PVT区块；5) 使用 基于*ISB*的交叉认证检查 (12) 检查解的真实性。

具体而言，我们将目标位置 $\boldsymbol{p}_1^{\star}$ 设为北纬 45.398°、东经 11.876°，海拔 12 米（意大利帕多瓦的普拉托德拉瓦莱广场）。合法位置与目标位置之间的距离约为 1.7 公里。

请注意，在步骤 3) 和 4) 之间，我们省略了实际的虚假信号生成过程，以及受害者对接收到的信号进行的处理。这意味着我们假设，在攻击过程中，受害者会按攻击者的意图处理被篡改的信号。不过，正如 [5] 和 [6],中的实验结果所证明的那样，确实可以向受害者注入伪造信号，因此我们省略了这些步骤。

图5 展示了在合法场景和受攻击场景下计算出的位置：攻击者始终能够诱导目标位置，并且相对于目标位置仅观察到可忽略的误差。在可用性方面未观察到任何问题，即所有伪造的伪距都导致了

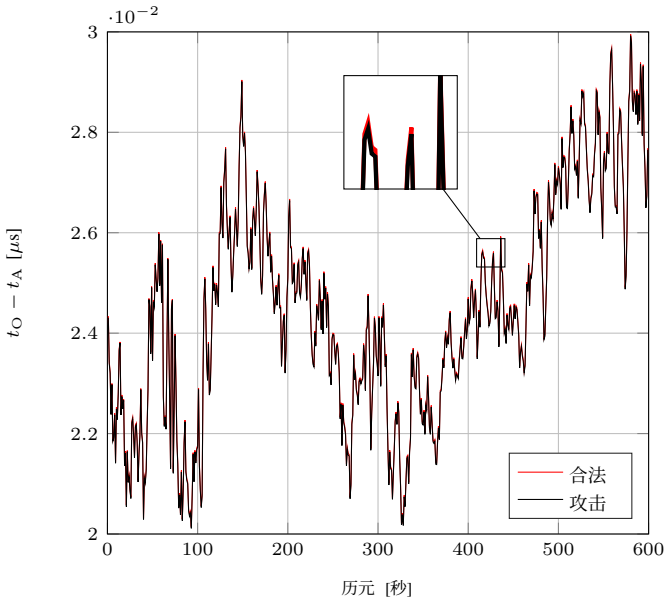


图6.检查（12）的指标：攻击下计算的指标（黑色）与在合法情形下计算的指标（红色）重叠显示。

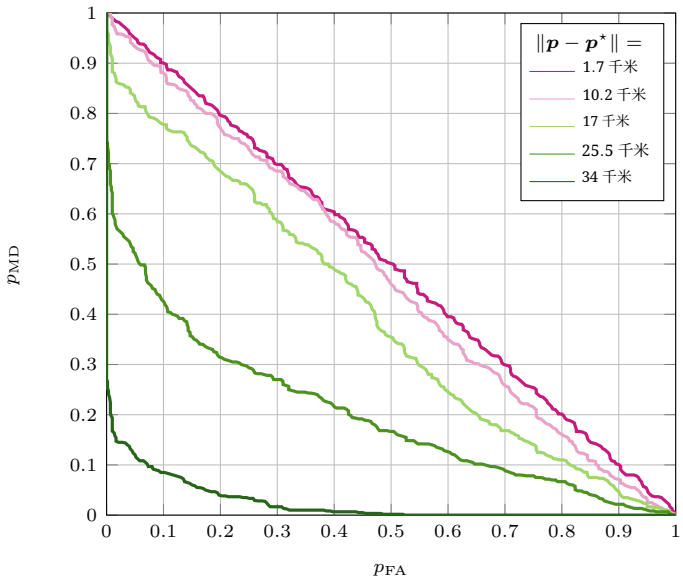


图 7. 针对所提出的生成攻击，基于时间的交叉认证中真实位置与目标位置之间不同距离对应的 DET 曲线。

位置、速度和时间的计算。

图 6显示了在合法情况和受攻击情况下分别计算的、用于安全检查 (12)的时钟偏差 t_O 与t_A 之差。实际上，该检查无法区分合法场景与受攻击场景，因为合法值与伪造值之间的实际差异远低于该指标本身的标准差。因此，对于任何阈值 T，该检查都无法有效检测攻击。基于这些原因，我们得出结论：我们的攻击可以在不被检测到的情况下欺骗受害者的位置。

图 7 展示了目标位置与实际位置之间不同距离对应的检测错误权衡（DET）曲线。事实上，随着该距离增大，受害者更容易检测出欺骗攻击。尤其是当距离大于 10 km 时，攻击成功概率会迅速下降。这与我们在第 II-B 节中的观察一致，进一步证实：当目标位置与真实位置相距过远时，采用线性化过程设计攻击并不可靠。不过，我们要指出，攻击者将目标位置设得过远可能并不合理，因为受害者还可以利用其他机会信号来检查计算得到的位置。

300 400 50

0 600

poch [s]

*b)*针对基于位置的检查的攻击： 我们报告了针对位置交叉认证检查的攻击结果，这些检查在第 IV-B 节的无噪声场景中进行了讨论。具体而言，我们考虑了三种不同的攻击（表 I），其引入的时间偏移和攻击开始时间各不相同。

图 8 显示了受害者估计的时钟偏差发生阶跃变化后的结果。这代表了对防御方最有利的情况，因为通常时间偏移是以斜坡式的方式引入的（例如，参见 [28] 的分类）。事实上，如果所考虑的攻击能够成功，那么更复杂的攻击也同样会成功。在此期间。

表 I 位置交叉认证检查攻击的参数：攻击开始时间为 t_{start}，附加时钟偏差为 $\Delta t - \Delta t_L$。

	攻击 1	攻击 2	攻击3
t_{start}	60 s	100 秒	150 秒
$\Delta t - \Delta t_L$	30 μ秒	10 μ秒	5 μs

合法攻击

在测试中，所有被考虑的攻击都达成了其目的，诱导目标时间发生偏移。另一方面，考虑实际的位置检查，任何攻击都没有诱导出显著的位置偏差，因为该偏差处于厘米级，远低于实际接收机的精度。同样，受害者使用所考虑的交叉认证检查也无法检测到这些攻击中的任何一种。

C 含噪测量结果

在本节中，我们评估所提出的攻击在噪声条件下的性能，并区分基于时间的检查和基于位置的检查。

从实验数据集开始，我们运行蒙特卡洛模拟，将每项实验重复 35 次，因此总共获得 21000 个位置、速度和时间测量值。

*a)*针对基于时间的检查的攻击： 正如第四节 A 部分所证明的，我们表明，攻击者可以利用生成攻击发动成功的攻击。

我们重复采用无噪声场景中的相同攻击仿真流程，但在步骤 3)和4)之间，根据受害者接收机σ_L处的噪声标准差，在合法伪距和伪造伪距上均添加加性高斯白噪声，其取值为 $\sigma_L = 0,1,2,4,$和9m。我们注意到，在这种情况下，攻击者执行的是生成攻击，因此伪距仅受到受害者接收机处噪声的影响。通常，噪声标准差的合理值为 7.1 m

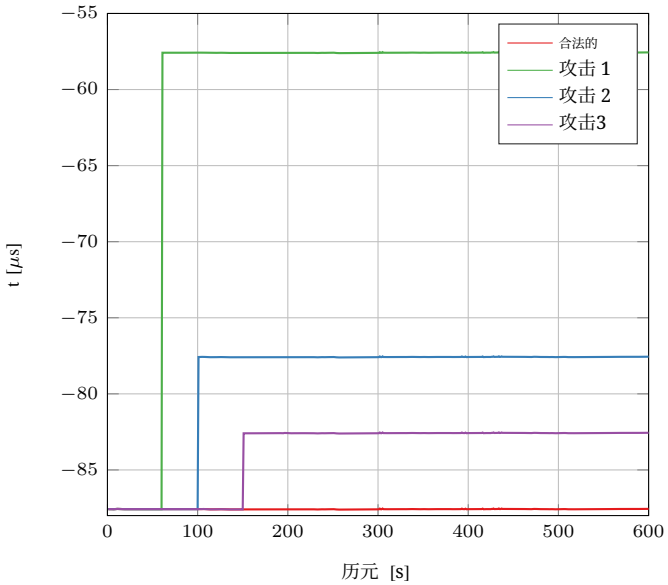


图 8. 时间攻击对受害者估计的时钟偏差的影响：Δt 合法情形（红色）、攻击 1（绿色）、攻击 2（蓝色）和攻击 3（紫色），其参数列于表 I。

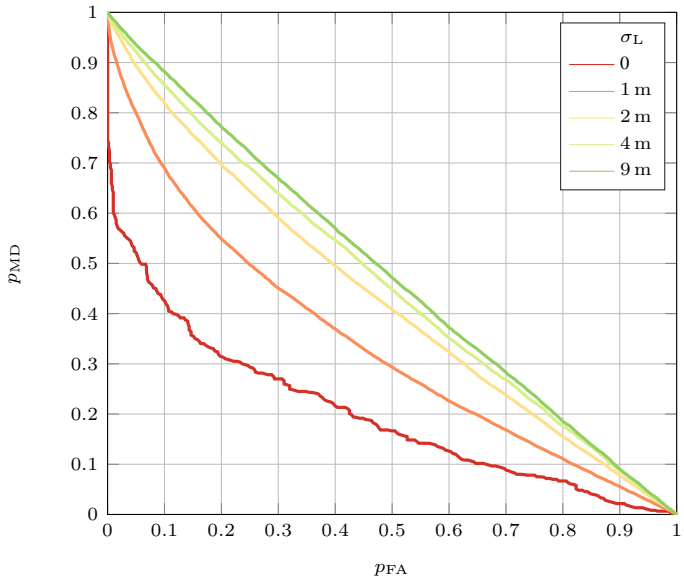


图 9. 针对基于时间的检查的生成攻击的 DET 曲线，其中攻击目标位置与受害者位置相距 25.5 千米，σ_L 取不同值。

[23, 第 7][3] 章。为评估攻击性能，我们考虑一个距受害者接收机位置25。5千米的目标位置。

图9 给出了针对基于时间的检查的生成攻击的 DET曲线，展示了漏检概率 p_{MD} 随虚警概率 p_{FA} 以及 σ_L的不同取值变化的情况。我们注意到，随着受害者接收机处噪声的增加，受害者将无法区分合法信号和伪造信号。然而，结果仍然证实，即使噪声最小，该检查也并非完全可靠，因为即使在这种条件下，要获得 $p_{MD} < 10^{-2}$ 也会导致 $p_{FA} \approx 0.88$，从而拒绝大多数合法信号。

b) 针对基于位置的检查的攻击：如第 IV-B 节和第 IV-B0b 节所述，如果 $N_O < 4$，则只有中继攻击能够在保持较低检测概率的同时造成所需的时钟偏移。相反，当 $N_O \geq 4$ 时，也可以使用生成攻击来实现相同的目标。值得注意的是，当中继攻击和生成攻击都可行时，后者始终是首选方案，因为它涉及信号生成而非转发，因此攻击者不会引入额外噪声，从而在 p_{FA} 和 p_{MD}方面取得更好的性能，正如本节将要讨论的那样。

首先，我们考虑第 IV-B 节中描述的中继式攻击。事实上，这对攻击者而言是最坏的情况。为了展示攻击性能，我们仅对篡改后的距离添加噪声，因此我们考虑 $\sigma_L = 0$。因此，伪造伪距的方差为 $\sigma_T^2 = \sigma_A^2$。

我们考虑攻击者旨在使估计的时钟偏差产生 $\Delta t - \Delta t_L = 10\,\mu s$ 偏移的场景。考虑 $\Delta t - \Delta t_L = 5$ 和 30μs 时，未观察到相关差异。在所有考虑的场景中，受害者接收到篡改信号后，会计算由 the 设置的时钟偏差。

[3]用于人工立场，从我们的测量值中，我们得到略多于 th 约 3 米。计划。

攻击者，且误差微乎其微。因此，每当未发出警报时，攻击都成功了。

图10报告了攻击在 σ_A的几种取值下的DET曲线。实际上，对于 $\sigma_A = 0$，这模拟了攻击者能够执行中继攻击而不增加任何额外噪声的情形，此时被篡改的信号与合法信号无法区分。另一方面，随着 σ_A 的增加，受害者更容易检测到攻击。尽管如此，即使 $\sigma_A = 9\text{m}$，该检查也仅部分有效，因为为了获得较低的漏检值，受害者会经历较高的虚警：例如，为了获得$p_{MD} < 10^{-3}$ （对于安全性应用而言，这并不是一个很低的值），受害者将得到 $p_{FA} > 0.2$。

关于针对基于时间的检查的生成攻击，我们开展了攻击仿真，在虚假距离和合法距离中均加入受害者接收机的加性高斯白噪声，其取值为 $\sigma_L = 0, 1, 2, 4,$ 和9 m。对于噪声标准差的所有考察值，虚假距离均无法与合法距离区分，所有 DET 曲线都塌缩到直线 $p_{FA} = p_{MD}$。

VII. 结论

在这项工作中，我们介绍了针对基于交叉认证的位置、速度和时间机制的一般攻击策略。在此类机制中，受害者接收机使用所有可用信号（包括开放信号和经认证信号）计算位置、速度和时间，并尝试利用某些先验信息评估所计算的位置、速度和时间的真实性。具体而言，我们重点研究了两类检查：授时交叉认证，例如 [21]，，其中通过验证相对于各系统的时钟偏差是否与实际的系统间偏差相关联来执行检查；位置交叉认证，该认证可用于授时服务，即如果位置、速度和时间能够（足够接近地）指向预期位置，则认为其具有真实性。对于这两种场景，我们表明攻击者能够将受害者引导至所选定的目标位置、速度和时间解，即，

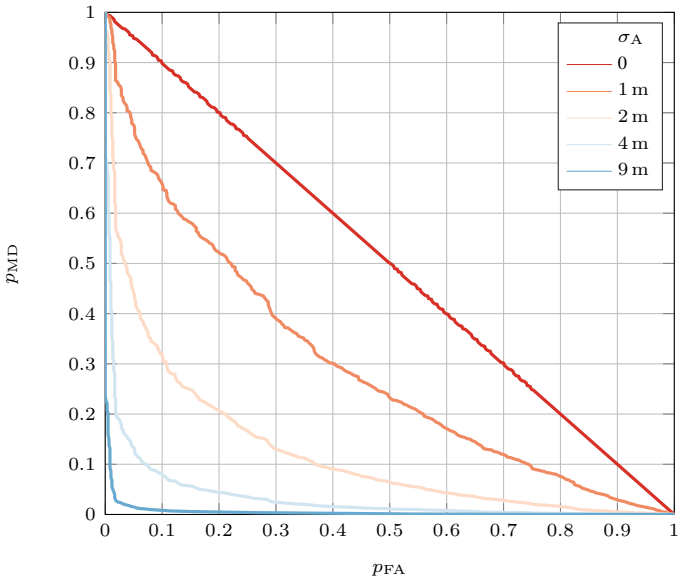


图1。针对位置交叉认证检查的中继攻击的检测错误权衡（DET）曲线，$\Delta t - \Delta t_L = 10\mu s$，$\sigma_A$ 取若干不同值，σ_L 固定。

到目标三维位置或时钟校正。我们表明，攻击的成功取决于接收机使用的开放信号数量以及攻击者条件。不过，在现实条件下，该攻击被证明是成功的。

我们考察了无噪声和有噪声两种场景：在后一种场景中，接收机获得的是被接收机篡改后的信号的噪声更大的副本。数值结果证实，该攻击在所考察的两种场景中均有效，表明此类安全检查无法有效保护接收机。

在若干实际场景中，接收的认证信号可能少于4个，因此接收机无法仅基于认证信号计算位置、速度和时间。我们的工作表明，无法通过基于位置、速度和时间的一致性检查将认证扩展到开放信号，因此接收机只能选择计算不安全的位置、速度和时间，或者完全不进行导航。

参考文献

[1] “伽利略信号空间接口控制文件”，https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo OS SIS ICD v2.0.pdf，[在线；访问日期：3月2023]。[2] “NAVSTAR GPS 空间段/导航用户接口，文档IS-GPS-200”，https://www.gps.gov/technical/icwg/IS-GPS-200M. pdf，[在线；访问日期：3月2023]。[3] S. Miljanovic、F. Ardizzon、L. Crosara、N. Laurenti、L. Canzian、E. Lovisotto、N. Montini、O. Pozzobon和R. T. Ioannides，“对专业GNSS接收机遭受干扰和欺骗攻击的实验测试与影响分析”，载于国际定位与全球导航卫星系统会议（*ICL-GNSS*）论文集，2022年。[4] Z. Wu、Y. Zhang、Y. Yang、C. Liang和R. Liu，“全球导航卫星系统的欺骗与反欺骗技术：综述”，*IEEE Access*，第8卷，第165 444–165 496页，2020年9月。[5] S. Ceccato、F. Formaggio、G. Caparra、N. Laurenti和S. Tomasin，“利用侧信息增强移动电话GNSS定位的弹性”，载于*IEEE/ION*定位与导航研讨会（*PLANS*）论文集，2018年。

[6] M. Lenhart、M. Spanghero 和 P. Papadimitratos，《针对全球导航卫星系统信号的中继/重放攻击》，载于第14届 ACM 无线与移动网络安全与隐私会议论文集。ACM，2021年，第380–382页。[7] I. Fern´andez-Hern´andez、T. Ashur、V. Rijmen、C. Sarto、S. Cancela 和 D. Calle，《迈向可投入运行的导航电文认证服务：OSNMA 协议新增功能的提案与论证》，载于欧洲导航会议（ENC）论文集，2019年，第1–6页。[8] A. Perrig 和 J. D. Tygar，《TESLA 广播认证》。美国马萨诸塞州波士顿：Springer US，2003年，第29–53页。[9] I. Fernandez-Hernandez、T. Walter、A. Neish 和 C. O’Driscoll，《面向高韧性 GNSS接收机的独立时间同步》，载于国际导航学会（ION）国际技术会议论文集，2020年，第964–978页。[10] 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提案》，《NAVIGATION：国际导航学会期刊》，第63卷，第1期，第85–102页，2016年3月。[11] T. E. Humphreys，《用于 GNSS 抗欺骗的密码检测策略》，《IEEE 航空航天与电子系统汇刊》，第49卷，第2期，第1073–1090页，2013年4月。[12] G. Caparra、N. Laurenti、R. Ioannides 和 M. Crisci，《改进安全码估计—重放攻击及其在 GNSS信号中的检测》，载于第7届 ESA 卫星导航技术与欧洲 GNSS信号及信号处理研讨会（NAVITEC）论文集，2014年。[13] 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》，载于国际定位与全球导航卫星系统会议（ICL-GNSS）论文集，2022年，第1–7页。[14] I. Fernandez-Hernandez、J. Winkel、C. O’Driscoll、S. Cancela、R. Terris-Gallego、J. A. L´opez-Salcedo、G. Seco-Granados、A. D. Chiara、C. Sarto、D. Blonski 和 J. D. Blas，《伽利略半辅助信号认证：概念验证与结果》，《IEEE 航空航天与电子系统汇刊》，第1–13页，2023年2月。[15] L. Scott，《民用导航系统的抗欺骗与认证信号架构》，载于国际导航学会（ION）卫星分部第16届国际技术会议（ION GPS/GNSS）论文集，2003年，第1543–1552页。[16] J. M. Anderson、K. L. Carroll、N. P. DeVilbiss、J. T. Gillis、J. C. Hinks、J. J. O’Hanlon、Brady W. and Rushanan、L. Scott 和 R. A. Yazdi，《面向 GPS 民用信号的芯片消息鲁棒认证（CHIMERA）》，载于国际导航学会（ION）卫星分部第30届国际技术会议（ION GNSS+）论文集，2017年，第2388–2416页。[17] G. Caparra 和 J. T. Curran，《论 GNSS 测距码加密可实现的等效安全性》，载于IEEE/ION 定位、位置与导航研讨会（PLANS）论文集，2018年，第956–966页。[18] F. Ardizzon、L. Crosara、N. Laurenti、S. Tomasin 和 N. Montini，《基于伽利略 ACAS 的认证授时协议》，《Sensors》，第22卷，第16期，2022年8月。[19] T. Mina、A. Kanhere、S. Kousik 和 G. Gao，《利用随机可达性分析实现基于 CHIMERA 的连续 GPS 认证》，载于国际导航学会（ION）卫星分部第34届国际技术会议（ION GNSS+）论文集，2021年10月，第4234–4248页。[20] F. Ardizzon、G. Caparra、Fernandez-Hernandez 和 C. O’Driscoll，《多频多星座位置、速度和时间保障蓝图》，载于 ESA 卫星导航技术与欧洲 GNSS信号及信号处理研讨会（NAVITEC）论文集，2022年。[21] B. Motella、M. Nicola 和 S. Damy，《基于 CHIMERA/OSNMA 联合方案的增强型 GNSS 认证》，《IEEE Access》，第9卷，第121 570–121 582页，2021年8月。[22] C. Gioia、J. Fortuny-Guasch 和 F. Pisoni，《GPS至伽利略时间偏差的估计及其在大众市场接收机上的验证》，载于第7届 ESA 卫星导航技术与欧洲 GNSS信号及信号处理研讨会（NAVITEC）论文集，2014年，第1–6页。[23] E. D. Kaplan 和 C. J. Hegarty，《GPS 原理与应用》（第二版）。Artech House，2005年。[24] P. Teunissen 和 O. Montenbruck，《Springer 全球导航卫星系统手册》。Springer International Publishing，2017年。[25] A. Mathai 和 S. Provost，《随机变量的二次型》。Taylor & Francis，1992年。[26] J. A. Klobuchar，《面向单频 GPS 用户的电离层时延算法》，《IEEE 航空航天与电子系统汇刊》，第 AES-23 卷，第3期，第325–331页，1987年5月。

[27] K. Borre、D. Akos、N. Bertelsen、P. Rinder 和 S. Jensen，《软件定义的 *GPS* 和伽利略接收机：单频方法》。Birkh¨auser Verlag，2007年1月。
[28] E. Schmidt、J. Lee、N. Gatsis 和 D. Akopian，《通过稀疏技术抑制平滑型 GPS 时间同步攻击》，《*IEEE* 传感器期刊》，第21卷，第1期，第776–789页，2021年5月。

附录A 使用不同时间基准进行位置、速度和时间计算

我们将介绍位置、速度和时间线性化过程，以及迭代方法中更新位置、速度和时间所需各项的推导，以计算式 5 中的各项。

根据接收信号，我们推导出伪距向量$\boldsymbol{r}$。为便于阅读，我们仅考虑来自两个系统的信号：因此，位置、速度和时间中将包含 t_1 和 t_2，它们是与各时间基准相关的时钟偏差，例如 GPS 系统时间（GPST）和伽利略系统时间（GST）。具体而言，接收机从第一个星座收集 N_1 个信号，从后一个星座收集 $N_2 = N - N_1$ 个信号。

通常，每个伪距建模为

$$r_j = \rho_j + ct_j - ct_1\mathbb{1}_1(j) - ct_2\mathbb{1}_2(j) + D_{\mathrm{atm},j} + \eta\,, \quad (59)$$

其中，ρ_j 是几何距离，即（估计的）接收机位置与第 j 颗卫星位置之间的欧几里得距离，其坐标为（x_j，y_j，z_j），定义如下：

$$\rho_j \triangleq \sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2}\,, \quad (60)$$

c 是光速，t_j 是卫星时钟偏差，$D_{\mathrm{atm},\,j}$表示大气延迟，η 表示其余误差，并将其视为噪声。引入指示函数$\mathbb{1}_1(j)$和$\mathbb{1}_2(j)$以识别卫星星座，即，若卫星 j 属于第一个星座，则$\mathbb{1}_1(j) = 1$，否则为 0；若卫星 j 属于第二个星座，则$\mathbb{1}_2(j) = 1$，否则为 0。请注意，卫星位置（的近似值）x_j、y_j以及 z_j、t_j和$D_{\mathrm{atm},\,j}$均直接从导航电文中获取。

接下来，我们介绍相关术语

$$a_{x,j} \triangleq \frac{x_j - \hat{x}}{\hat{\rho}_j}, \quad a_{y,j} \triangleq \frac{y_j - \hat{y}}{\hat{\rho}_j}, \quad a_{z,j} \triangleq \frac{z_j - \hat{z}}{\hat{\rho}_j}\,, \quad (61)$$

它们表示从（近似的）接收机指向第 j 颗卫星位置的单位向量的分量。这使我们能够引入几何矩阵

$$\boldsymbol{G} \triangleq \begin{bmatrix} a_{x,1} & a_{y,1} & a_{z,1} & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{x,N_1} & a_{y,N_1} & a_{z,N_1} & 1 & 0 \\ a_{x,N_1+1} & a_{y,N_1+1} & a_{z,N_1+1} & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{x,N} & a_{y,N} & a_{z,N} & 0 & 1 \end{bmatrix}. \quad (62)$$

按照例如在 [23,第 2],章中所述的线性化过程，并结合式 (3)，我们得到

$$\Delta r_j = a_{x,j}\Delta x + a_{y,j}\Delta y + a_{z,j}\Delta z - c\,t_1\mathbb{1}_1(j) - c\,t_2\mathbb{1}_2(j)\,, \quad (63)$$

它也可以等价地写成矩阵形式，如式（4）所示。该式将测距残差与位置、速度和时间更新向量 $\Delta\boldsymbol{p} = [\Delta x, \Delta y, \Delta z, \Delta t_1, \Delta t_2]^{\mathrm{T}}$ 联系起来。

请注意，残差按自然顺序排列为

$$\Delta\boldsymbol{r} \triangleq \begin{bmatrix} \Delta r_1 \\ \vdots \\ \Delta r_{N_1} \\ \Delta r_{N_1+1} \\ \vdots \\ \Delta r_N \end{bmatrix} = \begin{bmatrix} \Delta\boldsymbol{r}_1 \\ \Delta\boldsymbol{r}_2 \end{bmatrix}. \quad (64)$$

最后，给定 $\boldsymbol{G}$，我们可以计算其 Moore-Penrose 逆$\boldsymbol{H}$ 并求解（5）。

有关位置、速度和时间推导及其相关其他方面（例如 $\boldsymbol{H}$ 对解算精度的影响）的更多详细信息，可参见 [23,第 2,7]章和 [24, 第 21] 章。

附录 B
使用唯一时间参考进行位置、速度和时间计算

如果系统之间的系统间偏差已知，则可以仅考虑其中一个 M 时间参考来处理并求解 PVT 线性化问题。不失一般性，我们考虑从两个星座采集测量值且接收机已知系统间偏差 $= t_2 - t_1$ 的情况。这对应于同时接收 GPS 和伽利略信号，并从 I/NAV 消息中获取 GGTO 的情况。接下来，(59) 变为

$$r_j = \rho_j + ct_j - ct_1 - c\,\mathrm{ISB}\;\mathbb{1}_2(j) + D_{\mathrm{atm},j} + \eta\,, \quad (65)$$

接下来，我们可以将其视为卫星与同一时间参考同步，因此矩阵 $\boldsymbol{G}$ 变为

$$\boldsymbol{G} \triangleq \begin{bmatrix} a_{x,1} & a_{y,1} & a_{z,1} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ a_{x,N_1} & a_{y,N_1} & a_{z,N_1} & 1 \\ a_{x,N_1+1} & a_{y,N_1+1} & a_{z,N_1+1} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ a_{x,N} & a_{y,N} & a_{z,N} & 1 \end{bmatrix}. \quad (66)$$

其余步骤与附录A中所述的步骤类似。