DOI: 10.19650/j.cnki.cjsi.J2311799

时间戳服务到 UTC(NIM)的溯源方法研究*

张 宇[1],贾正森[2],龙 波[1],王玉琢[2]
(1.贵州省计量测试院 贵阳 550003;2.中国计量科学研究院 北京 100029)

摘 要:原子时标国家计量基准 UTC(NIM)由中国计量科学研究院维护和保持,溯源至协调世界时(UTC),是统一全国时间频率量值的最高依据。随着信息技术的不断发展,时间戳服务被广泛应用于司法、医疗、金融、电子商务、知识产权等领域。根据我国在贸易结算、医疗等领域对法制计量的需求,时间戳机构(TSA)提供的时间应溯源至 UTC(NIM)以实现国内统一和国际互认。本文提出使用一种校准器对 TSA 提供的时间进行远程和本地评估。实验结果表明,在局域网进行本地校准时,TSA 与 UTC(NIM)时间偏差的不确定度(k=2)小于 2 ms;在广域网环境下,即使校准器与 TSA 之间相距超过 1 000 km,TSA 与 UTC(NIM)时间偏差的不确定度(k=2)小于 713 ms。

关键词:时间戳;校准;溯源性
中图分类号:TB939 TH714 **文献标识码**:A **国家标准学科分类代码**:410.55

Research on the traceability method of time stamp service to UTC (NIM)

Zhang Yu[1], Jia Zhengsen[2], Long Bo[1], Wang Yuzhuo[2]
(*1. Institute for Metrology and Calibration of Guizhou, Guiyang 550003, China;*
2. National Institute of Metrology, Beijing 100029, China)

Abstract: The time and frequency primary standard UTC (NIM) is maintained by the National Institute of Metrology (NIM) in China, and is traceable to the international time scale coordinated universal time (UTC). With the continuous development of information technology, time stamp service is widely used in justice, health, finance, electronic commerce, intellectual property, etc. According to the Chinese government's demand for legal metrology in areas such as trade settlement and medical, the time provided by time stamp authority (TSA) should be traced to UTC (NIM) for domestic unification and international equivalence. This article proposes a calibrator to remotely and locally evaluate the traceability of TSA to UTC (NIM). When local calibration is implemented on the LAN, the uncertainties (k=2) of the time offsets between UTC (NIM) and TSA are generally less than 2 ms. The uncertainties (k=2) of the time offsets between UTC (NIM) and TSA located in Beijing are generally less than 713 ms on the WAN environment, even if the distance between the calibrator and TSA exceeds 1 000 km.

Keywords: time stamp; calibration; traceability

0 引 言

随着中国数字经济持续快速发展,电子商务与电子政务逐渐普及,时间戳的重要性与日俱增。数字化技术的发展,不仅在某种程度上改变了我们的通讯和生活方式,也产生了新的问题。现今,电子数据被越来越多领域所应用,但由于其易篡改和伪造,人们无法确保其真实性和可靠性,社会对电子数据的广泛使用缺乏安全感。如何使电子数据具有与传统书面文件具有同等的法律效力,是社会发展进程中必需解决的问题。中国电子签名法赋予了电子签名的法律效力,电子签名获得了与现实世界签名同等的地位,时间戳在电子签名中起着至关重要的作用。为了将数据与特定的时间点关联,需借助时间戳机构(time stamp authority, TSA)。TSA 作为可信的第三方机构在某个时刻为特定数据提供了“存在证明”。

收稿日期:2023-08-14 Received Date: 2023-08-14
*基金项目:国家重点研发计划(2021YFF0600102)、贵州省科技计划(黔科合支撑[2019]2881 号)项目资助

TSA 的作用是给数据打上时间戳,从而建立证据,表明该数据在特定时间之前已经存在。“时间戳”是使用数字签名技术产生的数据,时间戳服务器(time stamp server, TSS)是一个用于生成时间戳的系统,由 TSA 管理和服务[1-2]。时间戳服务器可作为数字证书认证系统的组成部分提供 RFC3161[3]中规定的时间戳服务,也可独立提供服务。TSA 作为公钥基础设施(public key infrastructure, PKI)的重要组成部分,广泛应用于司法、医疗、金融、知识产权保护、合同签订、电子投标、股票交易、遗嘱或其他声明、个人文件管理、区块链、检验检测报告等领域[4-9]。

时间戳服务所需的时间来源必须是可信的。可信时间应是“准确的、值得信赖的当前时间值,这个时间值的来源应是高度权威的”[10]。若采用客户自身产生的本地时间加盖时间戳,一方面得不到法律的认可,无法保证自身利益;另一方面无法保障时间的准确性和稳定性,发生错误时造成不可预料的后果。当前,对 TSA 测量方法的研究虽不多,但基本停留在定性测量,对时间偏差的测量仅依靠单向两点时差计算,未考虑单向传输延时引入的不确定度,而是以 TSA 声称的指标假设为不确定度,且在 TSA 网络接口端的测量,校准器并未作为客户端与 TSA 进行直连,而是在交换网络中作为监听者对客户端和 TSA 发出的请求和应答进行记录。总体来说现有研究未从方法原理上对测量不确定度进行评估,而在我国的计量体系下,主要关心对 TSA 的测量方法和不确定度评估方法,使其科学有效溯源[11-12]。时间戳服务在我国应用时间不长,尚无有效的方法保证 TSA 提供时间戳服务的合法溯源性,无法直接证明时间戳服务的时间溯源至 UTC(NIM),体现出我国时间戳服务的能力不足,明显落后于其他发达国家,与未来时间戳服务的需求规模形成巨大反差。

为此,本文将采用一种类似校准网络时间服务器的方法来解决 TSA 到 UTC(NIM)的溯源性问题,采用一台可与 TSA 交互且可溯源的计算机作为校准器,对位于北京的商用 TSA 进行远程校准,并对实验用的 TSA 进行本地校准。评估 TSA 的时间戳服务能力,有利于推动国家数字经济高质量发展,加快计量数字化进程,满足全社会对时间戳服务的需求。

1　时间戳服务原理

时间戳协议(time stamp protocol, TSP)中的请求和响应格式在 RFC3161 中已定义,其格式应符合 RFC5652[13]的要求。RFC3161 声明的时间戳分辨率可为秒、毫秒、微秒。时间戳服务的原理如图 1 所示,通常具备应用服务器的 TSA 可直接接收原始文件进行哈希值计算和时间戳请求的封装,无需客户端自行处理,但 TSA 并不保存客户端上传的原始文件。

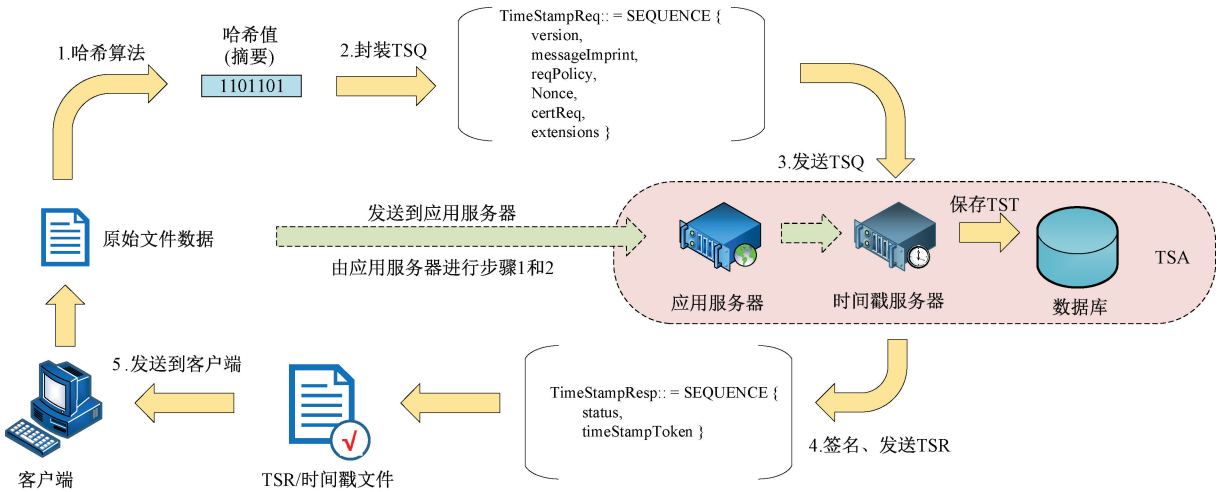

图 1　时间戳服务原理

Fig. 1　Principle of time stamp service

客户端通过哈希算法(SM3、MD5、SHA-256 等)生成原始文件数据的哈希值,将哈希值、版本、安全策略、随机数等信息封装,形成时间戳请求(time-stamp request, TSQ),通过超文本传输协议(hyper text transfer protocol, HTTP)、简单邮件传输协议(simple mail transfer protocol, SMTP)、套接字(socket)、文件传输协议(file transfer protocol, FTP)等方式发送给 TSA。TSA 收到 TSQ 后,对 TSQ 的有效性进行验证。无论验证成功或失败,TSA 都向客户端返回时间戳响应(time-stamp response, TSQ),该响应或是正确的时间戳,或是包含失败信息的时间戳。若 PKIStatusInfo 字段的值为 0 或 1,则 TSR 中应出现时间戳令牌(time stamp token, TST),否则 TSR 中不包含

TST。TST 是 TSA 对哈希值、签名参数、签名时间等进行数字签名后生成的数据。

TST/时间戳文件由 TSA 和客户端保存。当客户端需要验证原始文件时,向 TSA 提供原始文件对应的 TST/时间戳文件和哈希值。

通常,TSA 将生成 TSQ 的步骤集成到 HTTP 应用服务器中,客户端只需将原始文件上传到 TSA 网站,即可获得由 TSR 形成的时间戳文件,无需客户端形成和发送 TSQ。目前商用 TSS 的时间同步方式主要有网络时间协议(network time protocol, NTP)、高速串行计算机扩展总线(peripheral component interconnect express, PCIe)授时板卡、全球导航卫星系统(global navigation satellite system, GNSS)[14-15]和码分多址(code division multiple access, CDMA)等技术,通常具备验证时间戳请求有效性、签发/验证时间戳、内置时间源、密码算法加速、系统管理、设备监控、审计日志管理、Web 管理、时间戳日志保存和查询、负载均衡和双机并行等功能。

2 时间戳服务的校准方法

2.1 校准参数

TSA 对外提供时间戳服务,向客户端提供的电子数据加盖时间戳,等同于传递时间信息,要使 TSA 提供的时间有效溯源至 UTC(NIM),时间偏差是校准 TSA 最基本和重要的参数。

2.2 校准方法

由于 TSA 的应用服务器是为用户方便获取时间戳服务而设立的,TSA 本身的时间戳签发和时间来源由 TSS 决定,为使客户端发送 TSQ 的时间得到控制和记录,在校准过程中客户端需自行封装 TSQ 并调用相关接口直接发送至 TSS。

在时间戳请求和响应期间,客户端和 TSA 将产生 5 个时刻,如图 2 所示,客户端在时刻 T_1 将 TSQ 发送给 TSA,TSA 在时刻 T_2 时接收到 TSQ 并进行解析,生成一个包含签名时间 T_S 的 TSR,并于时刻 T_3 将 TSR 发送给客户端,在时刻 T_4 被客户端接收。t_{12} 和 t_{34} 分别为发送 TSQ 和 TSR 的网络延时。

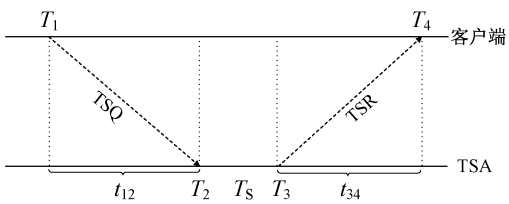

图 2 时间戳协议交换时序

Fig. 2 Timing diagram of a TSP exchange

根据 NTP 服务的校准原理[16]可定义客户端与 TSA 之间的时间偏差及其不确定度,时间偏差 d_{CS} 根据式(1)计算。

$$d_{CS} = T_{Client} - T_{TSA} = \frac{1}{2}[(T_2 - T_1) + (T_3 - T_4)] \tag{1}$$

式中:T_{Client} 为客户端的时间;T_{TSA} 为 TSA 的时间。

往返延时(round-trip delay, RTD) δ 为:

$$\delta = t_{12} + t_{34} = [(T_4 - T_1) - (T_3 - T_2)] \tag{2}$$

由往返延时引入的时间偏差不确定度 u 为:

$$u = \frac{1}{2}\delta \tag{3}$$

为了测量 TSA 的时间偏差,需要一个可溯源至 UTC(NIM)的校准器作为客户端与 TSA 进行 TSP 交互。校准器配置 PCIe 板卡,通过 UTC(NIM)的秒脉冲(1 pulse per second,1 PPS)信号[17]作为参考,或采用一种可远程溯源至 UTC(NIM)的时间频率标准作为参考(时间偏差在纳秒量级),如图 3 所示。

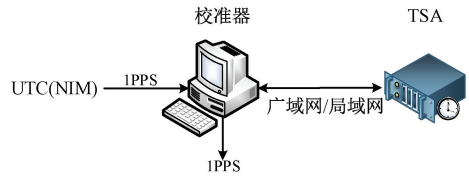

图 3 时间戳服务校准原理

Fig. 3 Schematic for TSP calibration

定义 TSA 与 UTC(NIM)的时间偏差 d_{TN} 为:

$$d_{TN} = T_{TSA} - T_{UTC(NIM)} \tag{4}$$

通过测量校准器输出的 1PPS 信号和 UTC(NIM)输出的 1PPS 信号,校准器与 UTC(NIM)之间的时间偏差 d_{CN} 由式(5)计算。

$$d_{CN} = T_C - T_{UTC(NIM)} \tag{5}$$

式中:T_C 为校准器的时间。

校准器向 TSA 发送 TSQ,并接收 TSA 返回的 TSR。假设 TSA 将接收到 TSQ 的时间作为签名时间 T_S,即 $T_2 = T_S$。通常,TSA 从收到 TSQ 到发出时间戳的解析过程不超过 1 ms[12]。由于商用时间戳服务器没有记录 T_3,故可近似的使 $T_2 = T_3 = T_S$。因此,校准器与 TSA 之间的时间偏差 d_{CT} 为:

$$d_{CT} = T_C - T_{TSA} = T_S - \frac{1}{2}(T_1 + T_4) \tag{6}$$

合并式(5)和(6)后,时间偏差 d_{TN} 等同于:

$$d_{TN} = d_{CN} - d_{CT} \tag{7}$$

3 时间戳服务校准系统的设计

3.1 时间源

在时间戳服务的校准系统中,时间源作为外部参考

时间为校准器提供标准时间信号,是必不可少的。由于 UTC(NIM)位于北京,为方便其他地区能够获得 UTC(NIM)信号,设计采用一种可被 UTC(NIM)驯服的铷原子振荡器(UTC(NIM) disciplined oscillator,NIMDO)作为参考时间源,通过 GNSS 远程时间频率传递技术卫星共视法实时跟踪到 UTC(NIM),时间偏差保持在 5 ns(U = 20 ns,k = 2),输出 1PPS 信号和时间信息(time of day,TOD)供校准器接入。

3.2　校准器

校准器通过与 TSA 进行 TSP 交互,记录发送请求和接收应答过程中产生 T_1、T_2、T_3、T_S 和 T_4,根据时刻信息计算校准器与 TSA 的时间偏差和往返延时,实现对 TSA 时间偏差的测量和不确定度的评估。

校准器本身是一台运行 Windows 10 操作系统的计算机,具有 64 位 3.7 GHz CPU,16 GB RAM 和 PCIe 板卡等。PCIe 板卡主要搭载 CH367 型 PCIe 总线接口芯片,安装在校准器的 PCIe 总线插槽中。CH367 芯片支持 1 个引脚(INT#)的中断请求输入,可配置为电平或边沿中断;提供高速 3 线或 4 线 SPI 串行接口;包含 3 个通用输出接口(GP0、GP00 和 GP01)。校准器通过 PCIe 总线与 CH367 进行数据交互,主要用到 8 个引脚(WAKE#、PERST#和 PECKP 等)。

PCIe 板卡使用 FPGA+ARM 框架设计,内置高精度恒温晶振(oven controlled crystal oscillator, OCXO),根据锁相环原理,将外部参考进行锁相并驾驭 OCXO,使其具备时间保持能力,当外部参考无效时仍然可提供高精度授时服务,可接收 GPS/北斗/PTP/交直流 IRIG-B 码/CDMA/1PPS/10 MHz 等外部参考信号,使用中一般通过接收外部 1PPS 信号获取时间,外部 1PPS 信号可来自 GNSS 或参考时间源,为此需要在校准器上编写驱动程序接收外部 1PPS 的中断信号,从而实现时间同步。驱动程序的中断过程首先由外部 1PPS 向 INT#引脚输出上升沿的中断请求信号;CH367 芯片收到中断信号后,通过 PCIe 总线向校准器申请中断;校准器进入 CH367 芯片的中断服务程序,在中断服务程序中,接收日期和卫星定位信息;当多次中断信号稳定后,在下次中断时对校准器的本地时间进行更新,使校准器的时间与外部参考源一致。

此外,为解决校准器的溯源问题,在校准器上安装另一块搭载 CH367 芯片的 PCIe 输出板卡,用于输出校准器产生的 1PPS 信号,在驱动程序中反复读取秒量级以下的时间 T_x(范围为 0~999.999 ms),若读出的时间在 990.000~999.999 ms 范围内,则进行(999 999 - T_x)μs 的延时,该延时需要用到 Windows 内部一个微秒级高精度定时器,通过调用 QueryPerformanceCounter( )函数查询当前高精度定时器的值,判断是否达到调用 QueryPerformanceFrequency( )函数得到的定时器频率值,从而实现微秒级的延时;当延时结束后即到达了时间上的整秒时刻,校准器通过 PCIe 总线与 CH367 芯片进行交互,控制 CH367 芯片的 GPOR2 通用输出寄存器的值为 0xFF,使 CH367 芯片的 GP0、GP00 和 GP01 引脚均输出高电平 3.3 V,随后延时 100 ms,延时结束后,置 GPOR2 通用输出寄存器的值为 0x00,使 GP0、GP00 和 GP01 引脚均输出低电平 0 V,实现校准器的 1PPS 信号在 GP0、GP00 和 GP01 三路引脚的复现输出。

经过时间间隔计数器测量,校准器与 NIMDO 的时间偏差约为 5 μs。为实现校准器的测量功能,设计还编写了时间戳客户端软件,主要用于产生并发送 TSQ,以及接收 TSA 返回的 TSR,记录各关键节点事件的时间信息,用于后续对 TSA 的时间偏差进行分析。

校准器的设计,使得计算机自身时间得到精确同步,且可验证和溯源,除了在时间戳服务的校准领域应用外,在医疗、金融、司法等领域涉及时间参数的也将得到广泛应用。

3.3　TSA

在远程校准环境下,对位于北京的商用 TSA 进行远程测量,商用 TSA 运行在 Linux 系统下,时间戳签发分辨率为微秒量级,时间同步方式主要采用 NTP 溯源至 UTC(NIM),支持 SM3 哈希算法。用户申请时间戳时,不需要发送用户的原始数据信息,而是只对用户的原始数据信息的哈希值进行时间戳签名,从而保证了用户原始信息的保密性和安全性。此外还具备基于硬件的真随机数芯片生成随机数功能[18],符合通用 RFC3161 标准,具有验证时间戳请求的有效性、根据请求签发时间戳、验证时间戳有效性、时间源管理、时间戳证书管理、系统日志管理以及系统配置管理等功能。

在局域网校准环境中,使用与校准器具有相同硬件配置的计算机作为实验用 TSA,并编写 TSA 服务程序模拟本地时间戳服务[19],具备商用时间戳服务器的基本签发功能,采用 PCIe 板卡进行时间同步。虽然程序支持的时间戳签发分辨率为毫秒量级,但程序中将具有微秒量级的 T_2 和 T_3 发送回校准器,校准器本身可实现 T_1 和 T_4 以微秒量级记录。该实验用 TSA 的时间同步和溯源与校准器相同。整个校准系统的框图如图 4 所示。

4　不确定度评定

在广域网或局域网校准环境下,时间偏差的不确定度主要由 RTD 引入。为评价 TSA 与 UTC(NIM)时间偏差的合成标准不确定度,按式(8)进行计算。

$$u_c^2(d_{TN}) = u_A^2(d_{TN}) + u_B^2(d_{TN}) \tag{8}$$

式中:$u_c(d_{TN})$ 为 TSA 与 UTC(NIM)时间偏差的合成标准不确定度;$u_A(d_{TN})$ 为 TSA 与 UTC(NIM)时间偏差

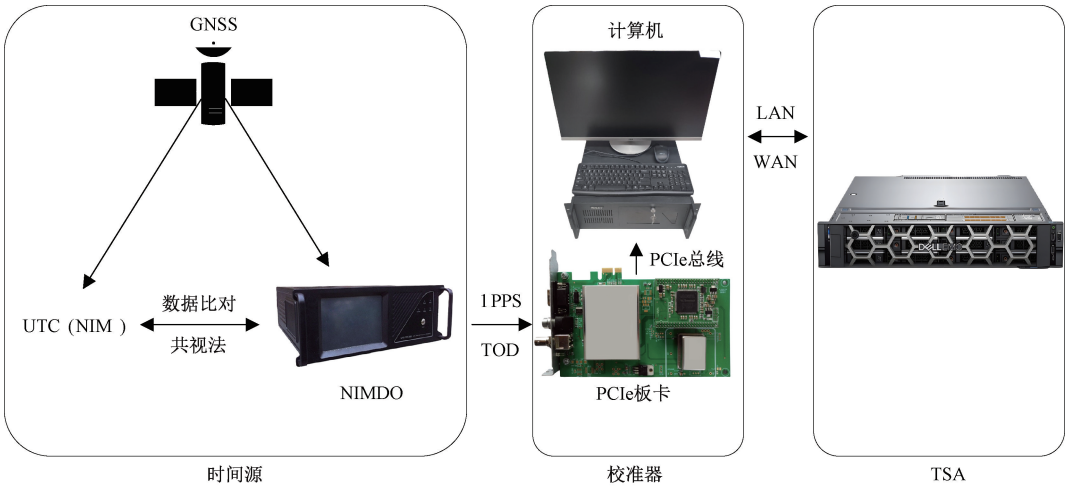

图 4 时间戳服务校准系统框图

Fig. 4 Diagram of the TSP calibration system

测量重复性引入的标准不确定度，用不确定度的 A 类评定方法进行计算；$u_B(d_{TN})$ 主要由 TSA 与校准器之间的往返延时、校准器与 UTC(NIM)的时间偏差引入的不确定度，用不确定度的 B 类评定方法进行计算。

$u_A(d_{TN})$ 用实验标准偏差表示，用贝塞尔公式进行计算，主要为 TSA 和 UTC(NIM)之间时间偏差的抖动，由 d_{CT} 和 d_{CN} 引入。B 类标准不确定度也由 d_{CT} 和 d_{CN} 引入。TSA 和 UTC(NIM)之间时间偏差的各项标准不确定度按式(9)和(10)计算。

$$u_A(d_{TN}) = s(d_{TN}) \tag{9}$$

$$u_B(d_{TN}) = [u_B^2(d_{CT}) + u_B^2(d_{CN})]^{\frac{1}{2}} \tag{10}$$

式中：$s(d_{TN})$ 为贝塞尔公式计算 d_{TN} 的实验标准偏差；$u_B(d_{CT})$ 为时间偏差 d_{CT} 的 RTD 引入的不确定度分量；$u_B(d_{CN})$ 为时间偏差 d_{CN} 引入的不确定度分量。

时间偏差 d_{CT} 的不确定来源主要由基于 TSP 交换的 RTD 引入，其值为：

$$u_B(d_{CT}) = \frac{1}{2}(\delta_{CT} + t_{23}) \tag{11}$$

式中：δ_{CT} 为测量 d_{CT} 引起的 RTD；t_{23} 为 TSA 接收到 TSQ 至发出 TSR 的时间间隔。

时间偏差 d_{CN} 引入的不确定度按 B 类评定方法进行计算，主要考虑两种情况，当校准器的时间参考端直接连接到 UTC(NIM)的 1PPS 信号时，d_{CN} 的引入的不确定度由时间间隔计数器的测量误差和 UTC(NIM)自身时间偏差的不确定度引入；当校准器的时间参考端需要远程溯源至 UTC(NIM)时，d_{CN} 引入的不确定度由时间间隔计数器的测量误差、UTC(NIM)与远程时间频率标准的时间偏差不确定度引入。两种方式中，无论校准器采用哪种方式获得参考时间，校准器与 UTC(NIM)时间偏差 d_{CN} 的不确定度通常不超过微秒量级，相对于 RTD 引入的不确定度，它通常被忽略。

5 实验与结果分析

5.1 远程校准位于北京的 TSA

远程校准的目的是评估 TSA 的远程服务能力。显然，这种方法将数据传输链路的往返延迟作为 TSA 服务能力的一部分，则最终的测量结果必然大于产品供应商声称的指标。

实验采用的时间源 NIMDO 和校准器位于中国贵阳，校准器的时间同步到 NIMDO[20-22]。校准器每间隔 1 h 向位于北京的商用 TSA 发送 TSQ，并记录每次请求和响应产生的 T_1，T_S 和 T_4，共测量 7 天。

图 5 显示了校准器与 TSA(北京)之间的时间偏差，误差条为时间偏差的不确定度($k=2$)。当忽略 d_{CN} 及其不确定度时，图 5 可表示为 UTC(NIM)与 TSA(北京)之间的时间偏差及其不确定度。

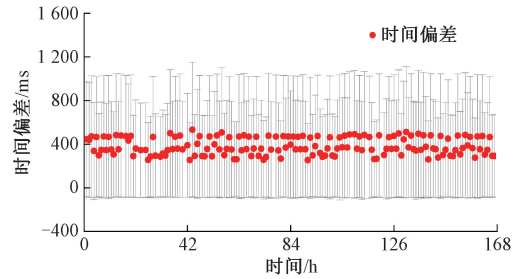

图 5 校准器与 TSA(北京)的时间偏差

Fig. 5 Time offset between calibrator and TSA (Beijing)

7 天的时间偏差平均值为 382.98 ms。实验标准偏差为 78.70 ms。然而 $u_B(d_{TN})$ 范围在 338.56~616.34 ms

之间(由式(10)计算,其中 $u_B(d_{CN})$ 被忽略)。测量数据通过拉依达准则去除异常值,且异常值仅占所有测量数据的 6%。

为了使校准器与 TSA 之间的时间偏差测量结果更加准确,将校准器与 TSA 之间的时间偏差按 24 h 的平均值表示为:

$$\overline{d_{CT}} = \frac{1}{n}\sum_{1}^{n} d_{CT_i} \tag{12}$$

式中:d_{CT_i} 是 1 d 中每小时的时间偏差。$\overline{d_{CT}}$ 的合成标准不确定度可由式(13)表示:

$$u_c^2(\overline{d_{CT}}) = u_A^2(\overline{d_{CT}}) + u_B^2(\overline{d_{CT}}) \tag{13}$$

式中:$u_c(\overline{d_{CT}})$ 为校准器与 TSA 时间偏差的合成标准不确定度;$u_A(\overline{d_{CT}})$ 为校准器与 TSA 时间偏差测量重复性引入的标准不确定度,用 $s(d_{CT})/\sqrt{n}$ 表示;$u_B(\overline{d_{CT}})$ 主要由校准器与 TSA 的往返延时引入不确定度,用不确定度的 B 类评定方法进行计算。由于网络环境是不断变化的,我们将网络链路的不对称性视为矩形分布,因此往返延时引入的标准不确定度为:

$$u_B(\overline{d_{CT}}) = \frac{1}{\sqrt{3}} u_{B,max}(d_{CT_i}) \tag{14}$$

式中:$u_{B,max}(d_{CT_i})$ 为 $u_B(d_{CT_i})$ 中的最大值。

表 1 为 7 天内每天的 TSA(北京)远程校准结果,时间偏差在 365.54~407.96 ms 范围内,不确定度($k=2$)在 655.89~712.55 ms 范围内。文献[11]采用单向两点时差计算方式,校准捷克 1 000 km 内的 TSA,时间偏差平均值为-2.772 s,且未给出不确定度。而本文提出的校准方法不仅在 1 000 km 以上距离的时间偏差测量结果较好,且评定了不确定度。

表 1　TSA 的远程校准结果

Table 1　Remote calibration results of TSA (Beijing)

天数	1	2	3	4	5	6	7
时间偏差/ms	407.96	365.54	376.16	383.47	385.98	393.47	375.59
不确定度($k=2$)/ms	655.89	712.55	686.56	662.41	676.85	692.86	659.47

5.2　本地校准实验用 TSA

为从 TSA 服务提供商的角度评估 TSA 的服务能力,在局域网上使用网络直连对实验用 TSA 进行校准。测量结果不包括广域网环境下服务客户端时数据传输的 RTD。

实验采用的 NIMDO、校准器和实验用 TSA 均部署于中国贵阳同一实验室内,实验用 TSA 采用与校准器相同的硬件配置,且对其编写了 TSA 服务程序用于模拟本地时间戳服务,并使其回送 T_2 和 T_3,因此式(6)和(11)可以改写成:

$$d_{CT} = T_C - T_{TSA} = \frac{1}{2}[(T_2 - T_1) + (T_3 - T_4)] \tag{15}$$

$$u_B(d_{CT}) = \frac{1}{2}(\delta_{CT}) \tag{16}$$

校准器和实验用 TSA 之间的时间偏差和不确定度如图 6 所示。测量过程在局域网环境下进行,因此校准结果比远程环境下理想。Windows 操作系统中的线程调度和轮询可能会引起不确定度的跳变。7 天的时间偏差平均值为 0.64 ms。测量重复性为 0.30 ms,往返延时引入的不确定度范围在 0.48~1.50 ms 之间,与产品供应商声称的指标基本一致。

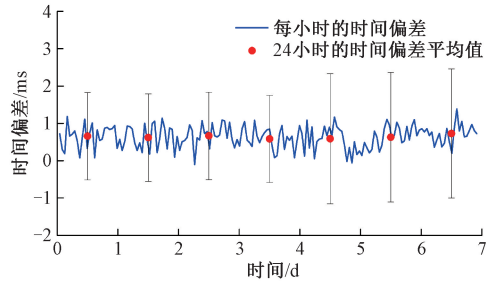

图 6　校准器与 TSA(本地)的时间偏差

Fig. 6　Time offset between calibrator and local TSA

表 2 显示了 7 天内每天的实验用 TSA 本地校准结果,时间偏差在 0.58~0.73 ms 范围内,不确定度($k=2$)在 1.17~1.74 ms 范围内。与文献[12]中校准器作为监听者的单向两点时差计算方式相比,本文采用校准器作为客户端与 TSA 进行直连校准的方式,时间偏差平均值为 0.64 ms,小于现有方案的 1.2 ms,并评定了不确定度。

表 2　实验用 TSA 的本地校准结果

Table 2　Local calibration results of experimental TSA

天数	1	2	3	4	5	6	7
时间偏差/ms	0.66	0.62	0.66	0.58	0.59	0.63	0.73
不确定度($k=2$)/ms	1.17	1.17	1.17	1.17	1.74	1.74	1.73

实验进一步分析,记录 $T_3 - T_2$ 的平均值为 7.98 ms(包括封装 T_2 和 T_3 大约 2 ms 的时间),大于文献[12]中描述的 1 ms。当然这与 TSA 使用的硬件和软件直接相关。实际上,商用 TSS 很难获得 $T_3 - T_2$ 的值,仅能假设 $T_2 = T_3 = T_S$,因此在实际校准中可适当放大 $T_3 - T_2$ 引入的时间偏差不确定度(式(11)中的 t_{23})。

6　结　　论

时间是 7 个国际单位制中准确度最高、应用最广的

基本物理量。国家时间频率计量体系作为国家基础设施,是国家重要的战略资源。独立的国家时间频率计量体系可以确保高速宽带通讯网络的安全正常运行,电网的精确同步,金融交易的准确可靠与安全,卫星导航系统的高精度定位,知识产权保护等。国家时间频率计量体系是提高自主创新水平、推动经济发展、促进社会进步、维护国家安全、增强国家综合国力和实现国防现代化建设的重要技术手段和基础保障。而时间戳在国家时间频率计量体系中表现为逐步可信,逐步发展的态势,是我国数字经济高质量发展的重要一环,其溯源性研究亟需解决。

时间戳作为证据在法律上的应用越来越广泛。将可信时间戳与数字签名相结合,保证了数据内容的完整性和生成时间的可追溯性,解决了数据生成过程中的“Who, What, When”问题。为完善国家时间频率计量体系,推动时间频率更广泛和准确的应用,保障电子数据的真实性、完整性和不可否认性,开展时间戳服务的溯源方法的研究,实现 TSA 到 UTC(NIM)的量值溯源,提出使用校准器来远程和本地评估 TSA 的服务能力,给出了校准器的搭建和设计方案,可有效溯源至 UTC(NIM),时间偏差约为 5 μs。

贵阳到北京的距离超过 1 000 km,位于贵阳的客户端获得北京商用 TSA 的时间戳服务保持在 1 s 以内。往返延时作为 TSA 提供服务的一部分,位于贵阳的客户端无法获得微秒量级的时间戳服务。若在局域网内评估 TSA 的服务能力,往返延时通常在毫秒量级,可有效评估 TSA 声称的服务能力(毫秒或秒量级),但位于广域网上的客户端无法获得满足该指标的服务。

参考文献

[1] DONG D P, GUO W, HUA Y, et al. Study on technical of trusted time authentication server[C]. International Conference on Computer Application and System Modeling (ICCASM 2010), 2010.

[2] GUO W, HUA Y, SONG K X. Study on the Security of Time-Stamping Service Architecture[C]. International Conference on Electronic Commerce and Business Intelligence, F 6-7 June 2009.

[3] ADAMS C, CAIN P, PINKAS D, et al. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)[J]. RFC, 2001, 3161.

[4] ĆOSIĆ J, BAČA M. Improving chain of custody and digital evidence integrity with time stamp[C]. The 33rd International Convention MIPRO, 2010.

[5] MOGAKI S, KAMADA M, YONEKURA T. Minimization of Latency in Cheat-Proof Real-Time Gaming by Trusting Time-Stamp Server[C]. International Conference on Cyberworlds (CW'07), 2007.

[6] NICULESCU A, CIOCIEA V. Trusted time distribution service for the romanian time stamping authoritie[C]. Proceedings of the 20th European Frequency and Time Forum, 2006.

[7] TING P Y, CHU F D, LIAO C S, et al. A digital standard time dissemination architecture for trustworthy time stamping[J]. IEEE Transactions on Instrumentation & Measurement, 2011, 60(7): 2584-9.

[8] VIGIL M, WEINERT C, DEMIREL D, et al. An efficient time-stamping solution for long-term digital archiving[C]. IEEE 33rd International Performance Computing and Communications Conference (IPCCC), 2014.

[9] ZHANG Y, XU C, CHENG N, et al. Chronos^{+}+: An accurate blockchain-based time-stamping scheme for cloud storage[J]. IEEE Transactions on Services Computing, 2020, 13(2): 216-29.

[10] 全国信息安全标准化技术委员会. 信息安全技术公钥基础设施时间戳规范:GB/T 20520-2006[S]. 中国国家标准化管理委员会,2006.

[11] SMOTLACHA V, TYML P, ČERMÁK J, et al. Calibration of time stamp authorities[C]. 15th IMEKO TC-4 International Symposium on Novelties in ELectrical Measurements and Instrumentation, 2024.

[12] SMOTLACHA V, ČERMÁK J, PALACIO J. On calibration of network time services[J]. Metrologia, 2008, 45(6): S51-S8.

[13] HOUSLEY R. Cryptographic Message Syntax (CMS)[J]. RFC, 2009, 5652.

[14] 张继海, 董绍武, 袁海波, 等. GNSS 多系统 PPP 融合时间比对方法研究[J]. 仪器仪表学报, 2020, 41(5): 39-47.
ZHANG J H, DONG S W, YUAN H B, et al. Study on multi-system GNSS data fusion technology in PPP time comparison[J]. Chinese Journal of Scientific Instrument, 2020, 41(5): 39-47.

[15] 朱江淼, 高秀娜, 黄艳, 等. GNSS 接收机抗干扰性能关键指标测试方法的研究与实现[J]. 电子测量与仪器学报, 2020, 32(3): 135-141.
ZHU J M, GAO X N, HUANG Y, et al. Research and implementation of testing method for key anti-interference performance of GNSS receiver[J]. Journal of Electronic

Measurement and Instrumentation, 2020, 32(3): 135-141.

[16] YU Z, YUZHUO W, NIANFENG L, et al. Traceability of network time service to UTC(NIM): Online calibration[J]. Measurement Science and Technology, 2021, 32(5).

[17] HOU L, HU Y, LIU J, et al. Research on computer time synchronization [C]. IEEE International Frequency Control Symposium Joint with the 22nd European Frequency and Time forum, 2009.

[18] 鲁迎春, 韩倩, 刘新颖, 等. 基于可配置异步反馈环形振荡器的真随机数发生器[J]. 电子测量与仪器学报, 2022, 36(11): 126-133.
LU Y C, HAN Q, LIU X Y, et al. True random number generator based on configurable asynchronous feedback ring oscillator generator[J]. Journal of Electronic Measurement and Instrumentation, 2022, 36(11): 126-133.

[19] MISKINIS R, SMIRNOV D, URBA E, et al. Digital time stamping system based on open source technologie[C]. IEEE International Frequency Control Symposium Joint with the 22nd European Frequency and Time forum, 2009.

[20] KUN L, HANG Y, FEI Z, et al. Disciplined oscillator system by UTC(NIM) for remote time and frequency traceabilit[C]. European Frequency & Time Forum, 2015.

[21] 龙波, 王菊凤, 黄徐瑞晗, 等. 基于 NIMDO 及光纤传递的高精度时间同步系统研究[J]. 计量学报, 2019, 40(5): 904-909.
LONG B, WANG J F, HUANG-XU R H, et al. Study of High Precision Time Synchronization System Based on NIMDO and Optical Fiber Transfer[J]. Acta Metrologica Sinica, 2019, 40(5): 904-909.

[22] 吴红卫, 李铎, 顾思洪. 小波滤波在时间同步系统中应用研究[J]. 仪器仪表学报, 2019, 40(2): 182-189.
WU H W, LI D, GU S H. Application research of wavelet filtering in time synchronization system [J]. Chinese Journal of Scientific Instrument, 2019, 40(2): 182-189.

作者简介

张宇,2017 年于贵州大学获得硕士学位,现为贵州省计量测试院高级工程师,主要研究方向为时间频率计量、科研开发等。
E-mail: 617249407@qq.com

Zhang Yu received his M. Sc. degree from Guizhou University in 2017. He is currently a senior engineer at Institute for Metrology and Calibration of Guizhou. His main research interests include research and development, time and frequency metrology, etc.

龙波(通信作者),2002 年于贵州工业大学获得学士学位,现为贵州省计量测试院正高级工程师,主要研究方向为科研开发、能源计量、时间频率计量等。
E-mail: 88392967@qq.com

Long Bo (Corresponding author) received his B. Sc. degree from Guizhou University of Technology in 2002. He is currently a principal senior engineer at Institute for Metrology and Calibration of Guizhou. His main research interests include research and development, energy metrology, time and frequency metrology, etc.