文章编号:1671-4598(2024)05-0201-07 DOI:10.16526/j.cnki.11-4762/tp.2024.05.029 中图分类号:TP311 文献标识码:A

基于 Docker 容器的航天网络隐私数据安全防护控制研究

全 斌
(中国航天系统科学与工程研究院,北京 100037)

摘要:隐私数据嵌入量过大会导致航天网络主机信息参量提取时间延长,数据安全性下降,所以研究基于 Docker 容器的航天网络隐私数据安全防护控制方法;利用 Docker 容器收集航天网络负载数据,评估 Docker 容器实时负载量,联合目标防护信息实现对航天网络 Docker 容器的调度;根据 Docker 容器调度和 Paillier 同态加密结果,提取静态污点后完成航天网络隐私数据的训练与处理;根据所得到的数据,定义混沌映射关系,通过离散变换的方式生成安全性种子密钥,结合安全防护控制函数求解结果实现航天网络隐私数据安全防护控制;实验结果表明,所提方法能够将隐私数据实时嵌入量控制在 5.5 GB 以下,保证网络主机提取信息参量的时间不超过 0.7 ms,能够有效保证航天网络隐私数据安全性。

关键词:Docker 容器;航天网络;隐私数据;安全防护;负载数据;同态加密;静态污点;混沌映射

Research on Security Protection and Control of Aerospace Network Privacy Data Based on Docker Container

QUAN Bin
(China Aerospace Academy of Systems Science and Engineering, Beijing 100037, China)

Abstract: The excessive embedding of privacy data can lead to prolong the extraction time of host information parameters in aerospace networks and decrease in data security. Therefore, a privacy data security protection control method for aerospace networks based on Docker container is studied. The Docker container is used to collect aerospace network load data, evaluate the real-time load of Docker container, and schedule the Docker container of aerospace networks in conjunction with target protection information. According to the Docker container scheduling and Paillier homomorphic encryption results, it extracts the static stains, and then, trains and processes aerospace network privacy data. Based on the obtained data, the chaotic mapping relationship is defined to generate the security seed key through the discrete transformation, and the solution of the security protection control function is combined to achieve the security protection control of aerospace network privacy data. The experimental results show that the proposed method can control the real-time embedding amount of privacy data to below 5.5 GB, ensuring that the time for network host to extract information parameters does not exceed 0.7 ms, and it effectively ensures the security of aerospace network privacy data.

Keywords: docker container; aerospace network; privacy data; safety protection; load data; homomorphic encryption; static stains; chaotic mapping

0 引言

随着航天网络的快速发展和广泛应用,航天网络中的隐私数据安全问题日益突显。航天网络承载着大量敏感和机密的信息,包括个人身份、通信内容、技术数据等,因此保护航天网络中的隐私数据安全至关重要[1-3]。隐私数据泄露或遭到未经授权访问可能导致严重的后果,如信息泄露、个人隐私暴露、知识产权侵犯等[4-5]。由于航天网络的特殊性和复杂性,其面临的安全威胁也更加严峻和复杂。为了确保航天网络的安全性和可靠性,必须采取有效的安全防护控制措施来保护隐私数据[6]。

为了解决这个问题,国内研究人员提出了一些方法。文献[7]FPGA 配置用 FLASH 型 PROM 数据失效分析及防护措施,其是在 FPGA 芯片的作用下,分析航天网络因素数据样本之间的失效关系,可从失效因素和失效机理两个角度分别确定隐私数据样本在网络体系中的实时传输速率,从而判定网络主机对信息参量的防护处理能力。文献[8]提出了基于关联知识的航天器有效载荷遥测数据安全防护仿真方法,通过求解与隐私数据样本相关的阈值、传输周期及线性关系,并按照多维度关联特征条件,将这些信息参量与数据样本对象对应起来,进而确定防护处理任务在航天网络体系中的执行能力。国外对于这一问题的研究也取得了一定进展,文献[9]提出了基于临时散列签名的 eHealth 记录信息安全保护控制方法,首先,通过数据准备和临时散列签名生成,确保原始数据的完整性和可靠性。

收稿日期:2023-05-25; **修回日期**:2023-07-05。
作者简介:全 斌(1997-),男,大学本科。
引用格式:全 斌.基于 Docker 容器的航天网络隐私数据安全防护控制研究[J].计算机测量与控制,2024,32(5):201-207,214.

然后，生成和管理公私钥对，用私钥对临时散列签名进行签名，生成最终的数字签名。在数据传输和存储过程中，使用加密技术保护数据的机密性，并采取安全措施，如访问控制和数据加密，以防止未经授权的访问和窃取。最后，建立安全审计和监控机制，对数据的访问和操作进行监测和记录，以确保系统的合规性和安全性。文献［10］提出了基于改进深度学习的步态数据集隐私安全保护控制方法，该方法针对深度学习容易受到黑客攻击，因此保护步态数据集的隐私变得困难。为了解决这个问题，提出了一种可逆的步态匿名流水线，通过特征修改来修改步态几何结构，以防止对抗性攻击，从而实现步态数据集隐私安全保护控制。

尽管上述几种方法可以控制隐私数据嵌入量，但其控制程度并不满足实际应用的需求，难以保证网络主机对信息参量的提取时长始终低于标准数值条件。Docker 容器是一种开源型应用容器引擎，能以统一的方式对应用文本进行打包处理，并将其完全移植到容器组织中，以供其他服务器调用和识别。在航天网络中设置 Docker 容器可以促进通信数据的快速传输，并能够大幅提升信息安全级别，所以提出基于 Docker 容器的航天网络隐私数据安全防护控制方法。

1 航天网络 Docker 容器调度

Docker 容器在航天网络中负责处理隐私数据样本，并可以根据信息参量的嵌入程度确定网络主机对数据样本的防护处理能力。本章节将联合容器元件所收集到的负载数据，对其进行按需调度。

1.1 隐私负载数据收集

Docker 容器借助 cAdvisor 逻辑框架（如图 1 所示）收集航天网络隐私负载数据，其可在采集各网络端口内实时负载信息的同时，协调目标信息参量与非目标信息参量之间的传输关系，从而使隐私数据在航天网络中保持绝对稳定的传输状态。

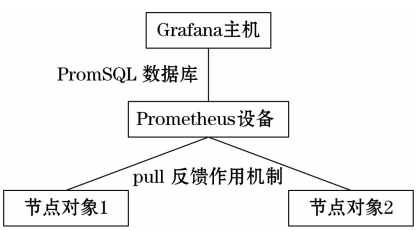


图 1 cAdvisor 逻辑框架

在 cAdvisor 逻辑框架中，由 PromSQL 数据库保障 Grafana 主机和 Prometheus 设备之间的实时连接关系。在 Docker 容器收集航天网络隐私负载数据的过程中，Grafana 主机和 Prometheus 设备同时保持连续运行状态。在这种情况下，节点对象 1 和节点对象 2 在 pull 反馈作用机制的作用下，将混合数据样本中符合隐私数据定义条件的非目标信息参量提取出来，以完成对 Docker 容器负载数据的收集。

规定 δ 表示满足隐私数据定义条件的非目标信息参量定义项，e 表示航天网络中隐私数据样本的实时传输参数，w 表示隐私数据在航天网络中的共享系数，W_δ 表示非目标信息 δ 的实时共享特征，$\overline{W}$ 表示航天网络中非目标信息的共享特征均值。由于 Docker 容器对于航天网络隐私数据的处理满足完全开放的调度需求，所以 e 参数、w 参数的取值同时属于 $(-\infty,0)\cup(0,+\infty)$ 的数值区间。

联立上述物理量，可将隐私负载数据收集结果表示为：

$$E_\delta = 1-\frac{1}{\ln(e\cdot\delta)}\times\sum_{w=1}^{+\infty}\frac{W_\delta}{\delta^2\cdot\overline{W}} \tag{1}$$

W_δ、$\overline{W}$ 同为矢量性指标，其取值符号表示隐私数据在航天网络中的实时传输方向，数值部分才表示数据样本在传输过程中的数量级水平。推导负载数据收集条件时，为满足安全防护的处理需求，只能在同一传输方向上，完成对共享特征参量的取值。

1.2 Docker 容器负载量评估

Docker 容器的负载量指的是其在航天网络中传输数据样本的负载能力。在目标信息参量和非目标信息参量混合的情况下，要评估容器组织对隐私数据的负载能力，必须按照负载数据收集条件 E_δ 分析容器设备中数据样本参量的总负载量。Docker 容器对负载的定义包括传输和识别两个方面。根据传输所定义的负载量是指隐私数据在传输过程中就已经被 Docker 容器收集；而根据识别所定义的负载量，则需要通过 cAdvisor 逻辑框架的完全识别，才能够让 Docker 容器收集隐私数据。

设 R_1 表示传输过程中被 Docker 容器收集的隐私数据样本总量，R_2 表示识别过程中被 Docker 容器收集的隐私数据样本总量，$\bar{\chi}$ 表示 Docker 容器对于负载数据的收集特征。利用上述物理量，推导航天网络隐私数据传输定义条件 r_1、识别定义条件 r_2 计算结果为：

$$\begin{cases} r_1 = \dfrac{R_1}{\sqrt{\sum_{w=1}^{+\infty}\bar{\chi}}} \\ r_2 = w\cdot\bar{\chi}\cdot R_2 \end{cases} \tag{2}$$

联立公式（1）、公式（2），实现 Docker 容器负载量评估，结果如下。

$$Y = E_\delta\sqrt{\frac{\beta\cdot(r_1+r_2)}{|\Delta T|\cdot|\Delta r|}} \tag{3}$$

式中，Δr 表示 Docker 容器中隐私负载数据的单位累积量，ΔT 表示隐私数据在航天网络中的单位传输周期，β 表示实时评估参数。

Docker 容器负载量评估条件是在负载数据收集表达式基础上求解的精准定义条件。对于 Docker 容器设备而言，该项应用条件的计算结果影响容器设备对航天网络的调度能力。此外，由于满足隐私定义条件的非目标信息在航天网络中的传输具有无序性特征，因此在选择负载量评估样本时，往往不进行连续性取值。

1.3 Docker 容器调度

调度表达式是调度航天网络中的 Docker 容器所遵循的

必要执行条件。为了确保其求解结果的准确性，在评估隐私数据负载量时，容器设备只能获得唯一的评估结果。如果结果不唯一或真实性不符合标准，则说明 cAdvisor 逻辑框架对数据对象的提取未能满足安全性标准。完整的航天网络中包含大量的非目标信息，但这些信息参量并不全部符合隐私数据定义条件。这就导致 Docker 容器在负载隐私数据时必须优先过滤掉一部分干扰性信息。与目标信息相比，非目标信息的传输并没有差异性。对于航天网络主机而言，在防护因素数据安全时，无法完全区分符合隐私定义条件的信息参量和不符合的信息参量。因此，在计算调度表达式之前，如果无法将二者区分开来，就会导致 Docker 容器出现错误调度的情况。

$\bar{y}$ 表示非目标信息的隐私定义特征，满足该定义条件的隐私数据取样结果为：

$$\alpha = \frac{\bar{y}}{Y} \tag{4}$$

利用公式（4），推导航天网络 Docker 容器调度表达式如下：

$$U = \min_{\varepsilon \to \infty} \gamma \cdot \left| \left(\alpha \times \frac{1}{u^2} \right)^{\varepsilon - 1} \right| \tag{5}$$

式中，ε 表示过滤参数，γ 表示 Docker 容器对于隐私数据的实时调度权值，u 表示已定义隐私数据的实时调度向量。

在调度 Docker 容器的过程中，航天器隐私数据样本的累积量只会不断增加。尽管容器元件可以对其累积行为进行一定程度的调度处理，但在防护控制隐私数据时，这种数据积累状态的变化形式只能变得较为缓慢，并不可能完全不累积或呈现缩小状态。即便是 Docker 容器停止运行，也不会发生反向变化行为。

2　航天网络隐私数据训练

在 Docker 容器调度原则的基础上，定义 Paillier 同态加密条件，再通过分析静态污点的方式，完成对航天网络隐私数据的训练与处理。

2.1　隐私数据的 Paillier 同态加密

Paillier 同态加密是调度航天网络 Docker 容器所遵循的公钥定义条件[11-12]。所谓同态是指数据样本明文信息参量、密文信息参量始终保持相同的传输状态。对于 Docker 容器而言，其在处理隐私数据的过程中，如果明文、密文信息的传输状态相同，那么码源文本的定义与执行也就遵循相同的密码机制，这就表示 Docker 容器在防护航天网络隐私数据传输行为时，不会影响信息参量的编码格式，符合安全防护的实际应用需求。

随机选取两个与航天网络隐私数据相关的码源文本参量 i、o，且 $i \neq o \neq 0$ 的不等式取值条件恒成立。Q_i 表示基于参数 i 的隐私数据密码定义向量，Q_o 表示基于参数 o 的隐私数据密码定义向量，二者求解结果可分别表示为：

$$Q_i = \varphi_i \times \frac{|i-1|^2}{p \cdot (\tilde{t})} \tag{6}$$

$$Q_o = \varphi_o \times \frac{|o-1|^2}{p \cdot (\tilde{t})} \tag{7}$$

式中，φ_i 表示基于参数 i 的码源参量同态调节系数，φ_o 表示基于参数 o 的码源参量同态调节系数，$\tilde{t}$ 表示航天网络 Docker 容器中隐私传输数据的实时加密特征，p 表示码源参量的安全性考核条件。

联立公式（5）～（7），可将航天网络隐私数据的 Paillier 同态加密结果表示为：

$$P = U^2 + \widetilde{p} \cdot \log \left| \frac{Q_i Q_o}{\varphi_i \varphi_o} \right|^2 \tag{8}$$

式中，$\widetilde{p}$ 表示基于 Paillier 加密结果中的数据样本码源核定参数，φ_i 表示码源文本参量 i 的同态加密向量，φ_o 表示码源文本参量 o 的同态加密向量。

航天网络 Docker 容器对于隐私数据的 Paillier 同态加密处理，要求公钥文本取值必须与码源参量保持数值映射关系，且为满足数据样本的安全防护控制需求，每一加密周期内，也不宜定义过多的码源参量。

2.2　安全防护的静态污点提取

静态污点是具有聚合能力的数据节点。在航天网络中，如果 Docker 容器所调度隐私数据样本总量满足实际消耗需求，那么每一个静态污点周围都会分布大量的隐私信息参量，且这些聚合数据样本的传输行为受到静态污点对象的直接影响。在航天网络覆盖区域足够大的情况下，Paillier 同态加密原则可以将满足同一码源定义标准的隐私数据样本聚合在一起，而这些包装数据结构中间必然包括一个静态污点对象。这个静态污点对象一方面主导加密后信息参量的传输行为，另一方面使隐私信息在网络体系内保持较为均匀的布局状态，从而满足安全防护数据参量的实际控制需求[13-14]。模拟如图 2 所示的静态污点布局结构图，在其中随机选取两个污点对象 A_s^i、A_s^j，联立公式（8），推导静态污点提取表达式，如公式（9）所示。

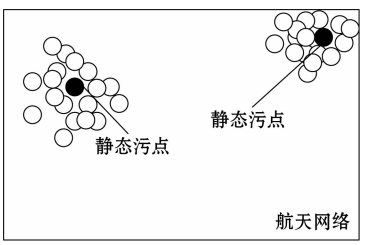


图 2　静态污点模拟图

$$S = a' \left(\sum_{s=1}^{+\infty} P(A_s^i \times A_s^j) \right) \tag{9}$$

式中，a' 表示 Paillier 同态加密原则控制下的污点对象协调参数，s 表示航天网络隐私数据在 Docker 容器内的传输行为规划向量。

训练航天网络隐私数据的主要目的是使 Docker 容器能够对信息参量的安全性进行有效防护，而静态污点作为因素数据样本的核心聚合节点，其对于信息参量的负载能力影响 Docker 容器的实时控制能力。在实际应用过程中，为避免隐私数据样本出现过度消耗的情况，应避免在相邻航天网络区域内，完成对隐私数据参量的取样。

2.3 隐私数据训练

Docker 容器对于隐私数据的训练为航天网络防护数据样本的安全性提供了控制模型。由于一个数据包集合中只包含一个静态污点对象，因此完善隐私数据训练条件时，单个指令周期内所能取得的信息样本数量相对有限。对于航天网络 Docker 容器而言，训练隐私数据可以达到精简静态污点所包含信息参量的目的。在满足种子密钥生成条件的同时，将更多数据样本对象聚合在一起，一方面避免航天网络主机在控制隐私数据传输行为时对信息参量进行多次取样，另一方面也可以充分满足隐私数据在航天网络中的实时传输需求，从而避免非关联性密钥参量对网络体系的安全认证能力造成影响。

对于隐私数据训练条件的定义，应同时考虑信息参量对抗特征与安全防护等级参数两项物理量的直接影响[15-16]。信息参量对抗特征表示为 d'，其影响 Docker 容器对隐私数据安全防护行为的控制能力，取值越大就表示 Docker 容器的控制作用能力越强。安全防护等级参数表示为 g'，其取值的改变，会导致航天网络隐私数据训练强度发生变化，联立公式（9），推导航天网络隐私数据训练公式为：

$$D=\frac{S}{1+d'^{-\iota}+g'^{-\kappa}} \tag{10}$$

式中，ι 表示隐私数据对抗性定义参数，κ 表示隐私数据传输安全性定义参数。

设计安全防护控制方法，要求所取样的航天网络隐私数据必须满足 Docker 容器对于信息参量的实时训练条件，且不同数据训练结果所对应的防护控制方法的执行结果也有所不同。

3 安全防护控制方法设计

航天网络隐私数据安全防护控制方法设计，利用 Docker 容器定义数据对象之间的混沌映射关系，再联合离散变换原则，生成种子密钥，完成对安全防护控制函数的求解。

3.1 防护控制的混沌映射关系定义

在实施航天网络隐私数据安全防护控制时，混沌映射关系决定了已取样数据样本的分布形式。Docker 容器在调度该项信息对象并对其进行训练处理时，确保混沌映射条件计算结果的唯一性是实现隐私数据安全防护的前提。

当混沌映射参数取值小于零，表示隐私数据样本之间的混沌映射关系符合逆向定义原则。在设计安全防护控制方法时，静态污点所代表信息的传输方向与其他信息参量的传输方向相反，因此 Docker 容器的单位响应周期也就相对较长；反之，当混沌映射参数取值大于零时，隐私数据样本之间的混沌映射关系也就符合正向定义原则，在这种情况下，静态污点所代表信息的传输方向与其他信息参量的传输方向完全相同，Docker 容器在控制隐私数据安全防护行为时，可以在同一方向内完成对样本对象的取值，故其响应周期也就相对较短[17-18]。

航天网络隐私数据防护控制的混沌映射关系定义式为：

$$G=\frac{fh_{\iota}(1-j_{\iota})^{\iota}}{D} \tag{11}$$

式中，ι 表示隐私数据的混沌传输指征，h_{ι}、j_{ι} 分别表示航天网络中的数据样本控制参数与防护参数，f 表示唯一性映射关系判别参量。在航天网络中，Docker 容器为实现对数据样本的安全防护，不会停止对信息参量的调度行为，所以 ι 系数取值不可能为零。

3.2 控制行为离散变换

对于航天网络隐私数据而言，离散变换可以有效保障数据样本对象之间的混沌映射关系。在设计安全防护控制算法的过程中，离散变换能够凸显数据样本明文信息和密文信息之间的相关性，从而使得防护控制函数求解结果满足实际控制需求。离散是指隐私数据在航天网络中的分布状态。Docker 容器在实施数据样本安全防护控制时，离散程度越大，表示信息参量的分布密度越小，单位时间内满足防护控制混沌映射关系定义条件的数据样本总量也就越少[19]。

K 表示航天网络隐私数据的取样集合，k_1、k_2、…、k_n 表示集合 K 内的 n 个隐私数据对象，且 $k_1\neq k_2\neq\cdots\neq k_n$ 的不等式条件恒成立。λ 表示隐私数据的离散分布参数，η 表示 Docker 容器对航天网络隐私数据的调度效率，H 表示航天网络主机对隐私数据样本的训练处理权限，$\tilde{J}$ 表示数据样本的离散度量值。在上述物理量的支持下，联立公式（11），推导航天网络隐私数据的控制行为离散变换表达式为：

$$L=\tilde{J}\times\left[\frac{(2\lambda+1)\eta HG}{k_1\times k_2\times\ldots\times k_n}\right] \tag{12}$$

离散变换的目的是使隐私数据在航天网络中的分布密度保持在既定数据区域之内。这样一方面不会使 Docker 容器因过度调度数据对象而出现延迟运行的情况，另一方面保持离散分布状态的信息参量能够更好满足航天网络安全防护控制隐私数据的实际应用需求[20]。此外，由于隐私数据对象的取样对应防护控制的混沌映射关系，所以离散变换原则的定义还可以验证已知混沌映射关系的可行性。

3.3 安全性种子密钥生成

安全性种子密钥是安全防护控制算法在筛选隐私数据对象时所遵循的判别条件。在信息参量离散变换原则保持不变的情况下，保证种子密钥与所筛选数据对象之间的对应关系是实现安全防护控制算法的基础环节。

以航天网络隐私数据作为自变量、防护控制对象作为因变量，可将安全性种子密钥生成原则描述为图 3。

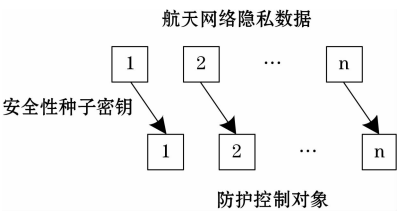


图 3 安全性种子密钥原则

图 3 中，每一个节点对象只对应一个数据样本，且所

选取航天网络隐私数据只有在安全性种子密钥的作用下，才能与 Docker 容器的防护控制对象保持对应性关系。种子密钥文本定义的特性决定了在防护控制算法应用过程中，信息参量的取样对应关系只能由航天网络隐私数据指向防护控制对象[21]。

对于安全性种子密钥生成条件的求解满足如下表达式：

$$Z=\frac{\sqrt{(\mu-1)}}{\bar{\nu}_1\cdot\bar{\nu}_2}\times x'\left|\frac{\vec{l}}{L}\right|^2 \tag{13}$$

式中，μ 表示种子密码定义参数，$\bar{\nu}_1$ 表示 Docker 容器对航天网络隐私数据的平均取值结果，$\bar{\nu}_2$ 表示 Docker 容器对防护控制对象的平均取值结果，x' 表示数据传输行为的安全性判别条件，$\vec{l}$ 表示 Docker 容器中航天网络隐私数据防护控制对象密钥的安全性导出向量。

生成安全性种子密钥，要求航天网络隐私数据、防隐私信号检测原理如下：

护控制对象的选取必须符合相同的控制行为离散变换条件，且为满足种子密钥文件对信息参量的无差别取样需求，在确定平均取值结果时，应选取大量数据样本以用于计算该项物理参数的实际取值[22]。

3.4　安全防护控制函数计算

安全防护控制函数计算包括防护阈值、控制强度两个基础设置环节。

防护阈值设置就是根据 Docker 容器对航天网络隐私数据的承载能力确定安全性边界条件。在计算安全防护控制函数时，防护阈值指标的选取还要参考安全性种子密钥定义条件[23]。

防护阈值设置：

$$\bar{\omega}=Z\cdot\frac{b\cdot\widetilde{V}}{\sqrt{\vartheta^2-1}} \tag{14}$$

$\widetilde{V}$ 表示航天网络隐私数据的安全性防护特征，b 表示阈值取样参数，ϑ 表示数据样本的边界取样值。

控制强度设置是根据 Docker 容器承载能力，所定义的安全防护控制执行频度标准[24]。对于航天网络而言，对隐私数据传输行为的高强度控制，更利于防护数据样本安全性。

控制强度设置：

$$\theta=\sum_{-\infty}^{+\infty}\sigma(\|B\|^2\times Z) \tag{15}$$

式中，σ 表示安全防护控制的实时执行频度，B 表示 Docker 容器的控制能力定义项。

联立公式（14）、公式（15），推导安全防护控制函数为：

$$M=\zeta\cdot\frac{\bar{\omega}\times\theta}{\log[1+\sqrt{2(N)}]} \tag{16}$$

式中，ζ 表示安全防护能力评定参数，N 表示防护控制指令的执行项参数。

基于 Docker 容器的航天网络隐私数据安全防护控制方法准确定义了安全防护控制函数，在隐私数据连续传输的过程中，航天网络对于数据样本的安全防护能力也就得到了保障。

4　实例分析

4.1　实验环境

航天网络中，隐私数据嵌入量过大会造成网络主机提取信息参量耗时过长的情况，这是导致网络体系无法安全防护隐私数据样本的主要原因。本次实验的目的就是根据隐私数据嵌入量及网络主机提取信息参量的耗时，来判断航天网络体系对隐私数据样本的安全防护能力。

隐私数据传输是航天网络通信中必然存在的现象。将隐私信号检测设备接入航天网络中，当检测器屏幕显示异常连接时，异常信号经由双绞线传输至信号显示装置中，此时响应器信号灯亮起，表示航天网络体系中存在隐私数据嵌入量过大的问题，可以开始实验。其中，隐私信号检测原理如图 4 所示。

隐私信号检测原理如下。

1）接收信号：航天器和地面通信设备之间的通信会产生电磁波信号，这些信号会被接收器捕获。

2）信号转换：接收到的电磁波信号经过接收器转换为电信号。

3）解调：对电信号进行解调，将其还原为原始信号。

4）分析信号特征：对解调后的信号进行分析，提取信号的频率、强度、调制方式等特征。

5）信号识别：将分析得到的信号特征与预先定义的信号模式进行比对和匹配，以确定信号的类型和来源。

6）检测结果输出：提取隐私信号，并将隐私信号检测结果输出。

信号显示装置原理如图 5 所示。

信号显示装置原理如下：

将隐私信号输入至低通滤波器中进行缓冲和前置放大处理，将处理后的信号输入至高通滤波器和陷波器，从而消除于消除或减少噪声、干扰或不需要的频率成分。将处理后的信号用户后续处理，利用 AD 转换器将模拟信号到数字信号，在 STC 单片机的支持下实现隐私信号存储、响应和液晶显示，从而达到隐私信号显示的目标。

本次实验的具体实施流程如下：

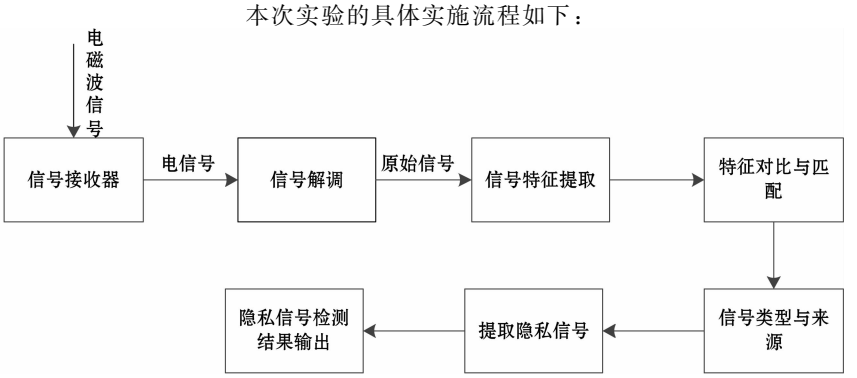


图 4　隐私信号检测原理

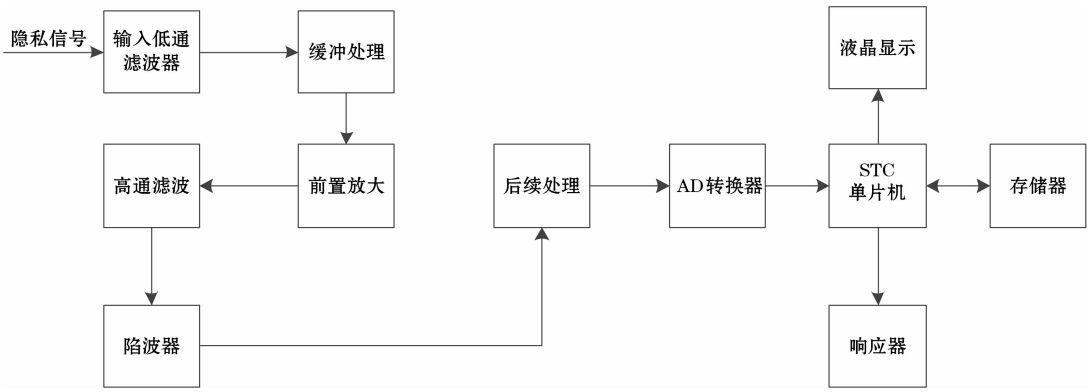


图 5 信号显示装置原理

1）顺次连接隐私信号检测装置与信号显示装置，确保信号灯亮起后，开始实验。

2）在 Windows 主机中输入基于 Docker 容器的航天网络隐私数据安全防护控制方法的执行程序，记录该方法作用下，隐私数据嵌入量的数值变化情况，所得结果为实验组变量。

3）退出 2）方法执行程序，在 Windows 主机中输入 FPGA 配置用 FLASH 型 PROM 数据失效分析及防护措施的执行程序，记录该方法作用下，隐私数据嵌入量的数值变化情况，所得结果为（A）对照组变量。

4）退出 3）方法执行程序，在 Windows 主机中输入基于关联知识的航天器有效载荷遥测数据仿真方法的执行程序，记录该方法作用下，隐私数据嵌入量的数值变化情况，所得结果为（B）对照组变量。

5）对照数据嵌入量与提取时间的对应关系，分析 3 组实验方法在防护隐私数据方面的实用能力。

4.2 隐私数据嵌入量

实验组、对照组航天网络隐私数据实时嵌入量的数值变化情况得出过程如下。

1）数据采集：从航天网络中收集隐私数据，主要包括个人身份信息、敏感数据等。

2）隐私数据嵌入算法：使用隐私数据嵌入算法将隐私数据嵌入到其他非敏感的数据中，以确保隐私数据在嵌入过程中的安全性和保密性。

3）实时监测与分析：将嵌入后的数据发送到信号显示装置中，这一装置连接了计算机，用以实时监测和分析技术来监控隐私数据的嵌入量。

4）数据统计和可视化：通过对实时监测数据进行统计和分析，可以得出隐私数据实时嵌入量的数值变化情况。结合波形图绘制随时间变化的曲线图，即波形图，从而展示数据随时间的变化的情况，以便能够直观地了解隐私数据嵌入量的变化趋势。

但是在航天网络隐私数据实时嵌入量的数值变化情况的得出过程中，可能存在一些不足之处，具体如下：

1）数据采集过程中存在漏采或遗漏，会导致得出的嵌入量数值不准确或不完整。

2）实时监测技术可能受到资源、带宽、延迟等方面的限制，导致监测的准确性和实时性下降。

为了克服这些不足，本文主要在数据采集过程中确保完整性和准确性，避免漏采和遗漏，选择传输速率更高、受到外部环境影响较小的无线传感网络，从而保证降低资源、带宽、延迟等方面的限制对于实验结果的影响。

图 6 反映了实验组、对照组航天网络隐私数据实时嵌入量的数值变化情况。负号仅用来描述航天网络隐私数据的实时传输方向，不影响其取值结果。

分析图 6 可知，由于航天网络隐私数据同时存在正向与负向传输行为，所以在实验过程中，该指标在正、负两个方向上都能取得最大值。随着数据传输周期的延长，实验组、（A）对照组、（B）对照组航天网络隐私数据实时嵌入量均保持来回波动的数值变化状态，整个实验过程中，实验组正向最大值为 5.5 GB、负向最大值为－4.7 GB。（A）对照组正向最大值为 8.9 GB、负向最大值为－7.8 GB，高于实验组数值水平。（B）对照组正向最大值为 9.6 GB、负向最大值为－9.0，也高于实验组数值水平。

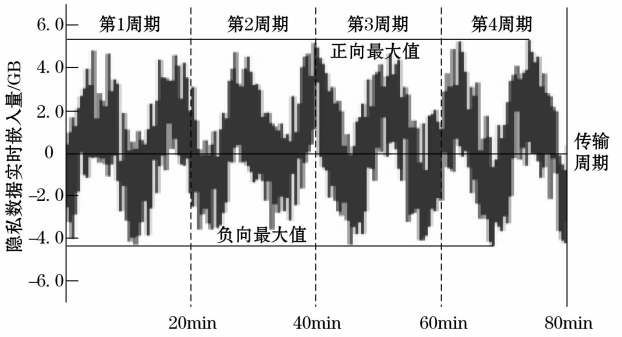
4.3 网络主机对信息参量的提取时长

表 1 为隐私数据实时嵌入量与网络主机对其提取时间的数值对应关系。

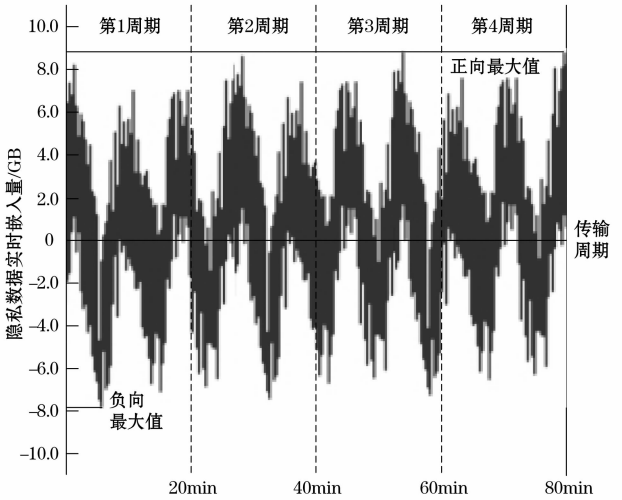
表 1 航天网络主机对隐私数据的提取时长

隐私数据实时嵌入量/ GB 正向传输	提取时长/ms	隐私数据实时嵌入量/GB 负向传输	提取时长/ms
0～2.0	0.2	0～2.0	0.3
2.0～4.0	0.4	2.0～4.0	0.5
4.0～6.0	0.6	4.0～6.0	0.7
6.0～8.0	0.8	6.0～8.0	0.9
8.0～10.0	1.0	8.0～10.0	1.1
大于 10.0	大于 1.0	大于 10.0	大于 1.1

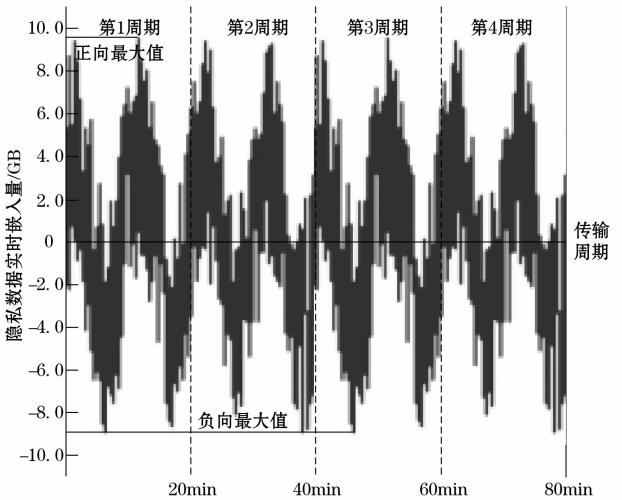
将图 6 中隐私数据实时嵌入量最大值与表 1 对照可知，实验组正向提取时长为 0.6 ms、负向提取时长为 0.7 ms。（A）对照组正向提取时长为 1.0 ms、负向提取时长为 0.9 ms，高于实验组数值水平。（B）对照组正向提取时长为 1.0 ms、负向提取时长为 1.1 ms，也高于实验组数值水平。



(a) 实验组



(b) 对照组



(c) 对照组

图 6　隐私数据嵌入量

4.4　结论

综上可知本次实验结论为：

1）FPGA 配置用 FLASH 型 PROM 数据失效分析及防护措施的方法以及基于关联知识的航天器有效载荷遥测数据仿真方法的应用，并不足以解决由于隐私数据嵌入量过大，而造成的网络主机对信息参量提取时间延长的问题。因此不能满足维护航天网络对隐私数据样本安全防护能力的实际应用需求。

2）基于 Docker 容器的航天网络隐私数据安全防护控制方法的应用，能够有效控制隐私数据的实时嵌入量，可以避免网络主机对信息参量的提取时间不断延长的情况，实现了航天网络对隐私数据样本的安全防护。

5　结束语

基于 Docker 容器的航天网络隐私数据安全防护控制方法的设计，通过训练隐私数据样本的方式，提取必要的静态安全防护污点，联合安全性种子密钥，定义安全防护控制函数。相较于 FPGA 配置用 FLASH 型 PROM 数据失效分析及防护措施和基于关联知识的航天器有效载荷遥测数据仿真方法，这种新型控制方法解决了隐私数据实时嵌入量过大的问题，能够使网络主机在较短时间内完成对信息参量的提取，符合保障航天网络安全防护隐私数据样本的实际应用需求。

参考文献：

[1] 李雅兰，王　倩，袁　可，等. 雾辅助的隐私保护分层多维数据聚合研究 [J]. 小型微型计算机系统，2022，43 (7)：1499 - 1504.

[2] 李贺男，闵庆学. 面向物联网系统的隐私防护安全架构及技术 [J]. 通信电源技术，2021，38 (12)：186 - 188.

[3] 刘　东，任海玲. 基于差分隐私的大数据安全访问权限认证仿真 [J]. 计算机仿真，2021，38 (8)：421 - 424.

[4] 冯绮航. 考虑属性加密的物联网隐私数据跨域安全共享模型 [J]. 现代电子技术，2023，46 (1)：91 - 95.

[5] 潘　雪，袁凌云，黄敏敏. 主从链下的物联网隐私数据跨域安全共享模型 [J]. 计算机应用研究，2022，39 (11)：3238 - 3243.

[6] 刘　峰，杨　杰，李志斌，等. 一种基于区块链的泛用型数据隐私保护的安全多方计算协议 [J]. 计算机研究与发展，2021，58 (2)：281 - 290.

[7] 刘　浩，段红亮，张雪峰，等. FPGA 配置用 FLASH 型 PROM 数据失效分析及防护措施 [J]. 导弹与航天运载技术，2021，382 (4)：117 - 121.

[8] 蔡晓玮，智　佳，陈志敏，等. 基于关联知识的航天器有效载荷遥测数据仿真方法 [J]. 计算机工程与设计，2022，43 (7)：2095 - 2101.

[9] SARAVANAGURU R A K, ARAMUDHAN M, CHARANYA R. Information security protection for eHealth records using temporal hash signature [J]. International Journal of Intelligent Enterprise, 2021, 1 (1): 1 - 11.

[10] PARASHAR A, SHEKHAWAT R S. Protection of gait data set for preserving its privacy in deep learning pipeline [J]. IET Biometrics, 2022, 11 (6): 557 - 569.

[11] 华斯亮，张惠国，王书昶. 用于全同态加密的数论变换乘法蝶形运算优化及实现 [J]. 电子与信息学报，2021，43 (5)：1381 - 1388.

[12] 李文卿，马　锐，张文涛. 基于共用密钥的高效多密钥同态加密方案研究 [J]. 计算机工程与科学，2023，45 (2)：252 - 260.

(下转第 214 页)