面向多业务场景的异构网络信息安全防御技术

陈长松 [1]
CHEN Changsong

摘 要 多业务场景下的异构网络需要处理大量不同类型的数据和流量，这使得网络监控和管理变得复杂，给恶意节点提供攻击机会。为解决多业务场景的异构网络易遭受恶意节点攻击的问题，提出一种面向多业务场景的异构网络信息安全防御方法。通过 K-means 算法获得不同类型的异构网络数据簇，以提高数据加密的效率。利用椭圆曲线加密算法完成各个数据簇的加密，提高异构网络信息的安全性。基于不同业务场景中访问节点的信任值识别出存在恶意攻击行为的节点，并拒绝其访问网络，以完成异构网络信息的安全防御。实验结果表明，所提出方法的网络能耗较低，防御性能较强。

关键词 多业务场景；异构网络；信息安全防御；椭圆曲线加密算法；节点信任值

doi：10.3969/j.issn.1672-9528.2024.10.034

0 引言

伴随着信息技术的快速发展，多业务场景下的异构网络已经成为现代社会的重要基础设施。这些网络由不同类型的设备、系统和协议组成，支持着各种复杂的业务应用 [1-2]。然而，由于异构网络的复杂性和多样性，其信息安全问题突出。恶意节点攻击、数据泄露、隐私侵犯等安全事件频发，给个人、企业带来了严重的损失。因此，针对多业务场景的异构网络安全防御方法研究具有重要意义。相关方法一直是研究的热点。

文献 [3] 方法根据特征相似性展开去噪，利用标签传播算法得到网络节点的伪标签，并对净化图与输入图展开卷积操作，利用对比学习算法实现攻击防御。但该方法中卷积操作的计算开销较大，导致防御控制中的网络能耗较高。文献 [4] 方法基于图像压缩域和稀疏余弦离散系数建立映射神经网络，对余弦系数展开逆变换去除图像中的扰动，通过增加分类损失完成防御。但该方法中神经网络的参数缺乏自适应能力，导致网络防御过程中的丢包率较高。文献 [5] 方法利用攻击混叠卷积神经网络学习网络攻击的特征，通过连续小波变换展开攻击识别，实现网络防御，但该方法受到噪声因素的影响，降低了网络防御的稳定性。文献 [6] 方法通过建立动态变化的安全机制，实施多层次的防御策略，并利用大数据实时发现异常行为和潜在威胁，强化协同防御能力，实现网络防御，但该方法的实施和维护成本相对较高，会增加经济负担。

为了解决上述问题，提出面向多业务场景的异构网络信息安全防御技术。利用 K-means 算法聚类异构网络数据，提升数据加密效率。应用椭圆曲线加密算法加密数据簇，增强安全性。通过节点信任值识别并拒绝恶意节点，实现异构网络的安全防御。

1 异构网络信息安全防御技术

1.1 异构网络数据分类

异构网络中的信息数据来自多个不同的网络和设备，数据间的差异较大且分散性较高，直接对其展开加密的难度较大，因此需要利用 K-means 算法对异构网络数据展开分类，以降低后续数据加密的难度。K-means 算法具有较好的伸缩性，可以处理大规模数据集，同时保持较低的算法复杂度。K-means 聚类主要基于数据间的欧氏距离 [7-8] 对异构网络数据展开分类，其具体过程如下。

步骤 1：假设 C 为采集到的异构网络数据集，该数据集的空间维度为 n，从 C 中任意抽取一个数据 c 作为初始化的聚类中心。

步骤 2：设定 $F(c)$ 为各个异构网络数据到 c 的最短距离，$A(c)$ 表示各个异构网络数据被选取作为第 2 个聚类中心的可能性，$A(c)$ 值最大的数据即是第 2 个聚类中心。对于数据成为聚类中心的可能性 $A(c)$ 的定义如下：

$$A(c)=\frac{F(c)^2}{\sum_{c=1}^{C}F(c)^2} \tag{1}$$

步骤 3：对步骤 1 和步骤 2 展开迭代操作，以获得 L 个聚类中心。

1. 郑州工商学院信息工程学院 河南郑州 451400

步骤 4：设定 c_i 与 u_i 表示异构网络数据 C 中除去聚类中心后的任意两个数据，$f(c, u)$ 表示数据 c_i 与 u_i 之间的欧式距离，$f(c_i, u_i)$ 可通过下式获取：

$$f(c_i,u_i)=\sqrt{\sum_{l=1}^{n}(c_l-u_l)^2} \tag{2}$$

式中：c_l 与 u_l 表示异构网络数据 c_i 与 u_i 中的第 l 个属性值。

利用公式（2）获取异构网络数据中剩余数据和 L 个聚类中心的欧氏距离，并将各个数据划分到欧氏距离最小的聚类中心中。

步骤 5：基于各个异构网络数据的划分结果，获取各个数据簇的中心点，并对初始的 L 个聚类中心展开更新。

步骤 6：迭代步骤 4～5，当数据划分结果不再发生变化时[9]，停止迭代，获得最终的 L 个异构网络数据簇 $C_1, C_2, \cdots, C_L$，完成数据分类。

1.2 基于椭圆曲线加密算法的数据加密

为防御异构网络信息遭受攻击，提高网络整体的安全性，将分类后的各个异构网络数据簇表示为一个数据点，并利用椭圆曲线加密算法对各个异构网络数据点展开加密。椭圆曲线加密算法可以减少存储和传输密钥所需的带宽和存储空间[10]。在异构网络中，由于设备和系统的多样性，数据的存储和传输效率尤为重要。通过减少密钥的大小，有助于降低网络负载，提高整体性能。

设定 a 是一个素数，$\{0, 1, \cdots, (a-1)\}$ 表示模 a 的所有余数集合，则 G_a 是基于 $\{0, 1, \cdots, (a-1)\}$ 关于模 a 的加法与乘法建立的 a 阶素数有限域。位于 G_a 上的椭圆曲线方程式为：

$$o^2=v^3+sv+q \tag{3}$$

式中：常数 $s, q \in G_a$，且满足 $(4s^3+27q^2) \bmod (a) \neq 0$；$o$ 和 v 表示有限域上任意数列的横坐标和纵坐标，且 $o, v \in G_a$。

当数据点 (v, o) 符合公式（3）时，认为该点位于曲线上，并且设定含有一个无穷远点 ∞ 满足公式（1），进而获得椭圆曲线上的数据点集合 $R(G_a)$ 定义如下：

$$R(G_a)=\{(v,o)\in G_a \cup \infty\} \tag{4}$$

Koblitz 概率算法是将异构网络数据簇嵌入椭圆曲线[11]上的典型算法，其实现步骤如下。

步骤 1：将异构网络数据簇 w 通过数 e_w 来表示，对于 e_w 中含有的数值分为 $e_w \leq a-1$ 和 $e_w \geq a$。

步骤 2：当 $e_w \leq a-1$ 时，抽取两个正整数 z 和 k，对于 z 和 k，需要符合 $0 \leq k \leq z-1$ 与 $ze_m+k \in G_a$。

步骤 3：将 z 和 k 代入公式（5），获得异构网络数据簇 w 在椭圆曲线上的坐标 v_k，v_k 的定义如下：

$$v_k=ze_w+k \tag{5}$$

依次计算各个满足条件的 z 和 k 对应的坐标 v_k，并将各个 v_k 值代入公式（3）获得对应的 o_k，当出现第一个满足 $R(G_a)$ 的点 (v_k, o_k) 时，停止计算，点 (v_k, o_k) 即为异构网络数据簇 w 嵌入到椭圆曲线上的点，并将其表示为点 S_{ze_w+k}。

步骤 4：当 $e_w \geq a$ 时，表示 e_w 不位于 G_a 上，此时需要对异构网络数据簇 w 展开分割，以形成若干个异构网络数据簇字段，并使所有字段均位于 G_a 上，然后利用步骤（2）与（3）将各个异构网络数据簇转换为椭圆曲线上的点。

基于上述操作将所有异构网络数据簇嵌入椭圆曲线上后，利用混合密码算法[12]对椭圆曲线上的各个点展开加密，加密过程也分为 $e_w \leq a-1$ 和 $e_w \geq a$ 两种情况。

当 $e_w \leq a-1$ 时，对异构网络第 i 个数据簇 w 对应的椭圆曲线点 S_w 展开加密的过程如下：

$$D_i=S_w+eW_2 \tag{6}$$

式中：D_i 表示加密后的椭圆曲线点；e 表示参数；W_2 表示报文接收方的公钥。

当 $e_w \geq a$ 时，对 S_w 展开加密的过程为：

$$D_i=R_n(S_w^i, W_2) \tag{7}$$

式中：S_w^i 是指切割得到的第 i 个数据簇字段对应的椭圆曲线点；R_n 是指椭圆曲线加密算法。

对于密文椭圆曲线点的解密过程为：

$$e_w=\left\lfloor \frac{v_k}{z} \right\rfloor \tag{8}$$

式中：$\lfloor \cdot \rfloor$ 表示底函数运算。

1.3 面向多业务场景的安全防御技术

对于加密后的异构网络信息，基于其面向多业务场景的要求，需要根据不同业务场景中访问节点的信任值[13]对其展开访问控制，以实现网络的安全防御技术。

不同业务场景的特性和需求不同，导致其访问节点的行为不同，而节点行为直接影响着节点信任值，因此需要对各个访问异构网络的节点展开信任值计算，其具体过程如下。

设定 i 和 j 是两个邻近节点，当 i 和 j 在同一时间对某一信息展开观测时，若 i 感知到的该信息值和 j 的基本一致，则认为 i 成功感知信息的次数 d_i 多一次，即 $d_i=d_i+1$。

访问节点感知数据的一致性能力是衡量该节点信任值的重要指标，对于节点的一致性能力[14]判断方法为：

如果 $0 \leq t_i - t_j \leq \vartheta_{i,j}$，则 $n_i=n_i+1$，且 $y_i=y_j$；如果 $t_i - t_j < 0$ 或者 $t_i - t_j > 0$ $\vartheta_{i,j}$，则 $p_i=p_i+1$。其中，t_i 和 t_j 分别表示节点 i 和节点 j 的感知信息值；$\vartheta_{i,j}$ 为设定的阈值；n_i 表示节点 i 感知信息的一致价值；y_i 和 y_j 分别表示节点 i 和节点 j 的感知时间值；p_i 表示节点 i 感知信息的不一致价值。

当节点 i 和 j 对同一信息的感知均失败时，i 和 j 的感知信息失败次数 g_i 和 g_j 也会多一次，即 $\begin{cases} g_i=g_i+1 \\ g_j=g_j+1 \end{cases}$。

在判断访问节点的信任价值因子一致性时，将 +1 和 -1 作为一致性和不一致性的表示。设定 V_i 为节点单个信任价值因子的一致性价值，对于 $V_i \in [-1,1]$ 的定义为：

$$V_i=(n_i-p_i)/(n_i+p_i) \tag{9}$$

对于单个信任价值因子的感知通信价值 $M_i \in[-1,1]$ 的定义为：

$$M_i=(d_i-g_i)/(d_i+g_i) \tag{10}$$

对于单个信任价值因子的电池使用寿命值 N_i 的范围为[0,1]。假设 E_i 表示上述三个影响因素的权重，且 $E_i \in(0,1]$，若 $N_i \neq 0$，则节点 i 的信任估计值 Y_i' 定义为：

$$Y_i'=\frac{E_1V_i+E_2M_i+E_3N_i}{\sum_{i=1}^{3}E_i} \tag{11}$$

如果 $N_i=0$，则表示此时异构网络已停止工作，因此 Y_i' 的值取 -1。

由于异构网络中节点的信任值是基于全部相邻节点的信任值获得的，假设该异构网络为环状结构，所有节点位于相同区域内，此时节点能相互接收数据，其中随机一个节点都属于这些节点中的一个，因此获得异构网络访问节点的最终信任值 Y_i 定义为：

$$Y_i=\gamma Y_i'/\sum_{j=1}^{h}Y_j+1 \tag{12}$$

式中：h 表示异构网络中能够互相通信的节点数量，Y_j 表示节点 i 的相邻节点 j 的信任值，设定 γ 为判断阈值，即当 $Y_i<0$ 时，判定该节点为具有攻击行为的恶意节点，拒绝其访问异构网络；反之，判定该节点为正常节点，同意其访问申请 [15]，并通过公式（8）的解密过程以及数据在椭圆曲线上的逆转换获得还原后的异构网络数据，按照访问节点的业务场景信息需求将对应的数据信息发送给该节点，以完成多业务场景下的异构网络信息安全防御。

2 实验与分析

为了验证面向多业务场景的异构网络信息安全防御技术的整体有效性，对其展开测试。实验异构网络拓扑图如图 1 所示。

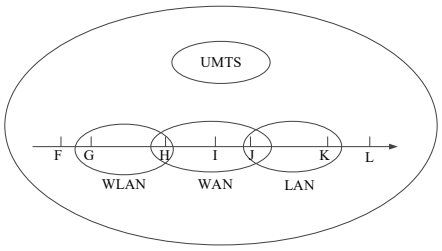

图 1 异构网络拓扑图

图 1 为一个异构网络，其中包含了无线网（WLAN）、广域网（WAN）、局域网（LAN）三种网络，现在该网络中展开本次实验，并设置实验参数：异构网络中共含有 50 个节点，其中 25 个为 WLAN 节点，15 个为 WAN 节点，10 个为 LAN 节点；网络初始能量为 800 J；网络中每个数据包的大小为 50 Byte；每种攻击的持续时间为 5 s。

2.1 网络丢包率

当异构网络受到恶意节点攻击时，恶意节点会产生大量的网络流量，造成网络堵塞，从而导致网络丢包率增大，因此，网络丢包率是评估网络攻击防御效果的指标之一，丢包率越小，表明恶意节点攻击对网络信息传输的影响越小，即网络的攻击防御效果越好。在图 1 中异构网络运行的第 15 s 施加恶意节点攻击，并利用所提方法、文献 [3] 方法和文献 [4] 方法对网络展开防御，网络丢包率的变化情况如图 2 所示。

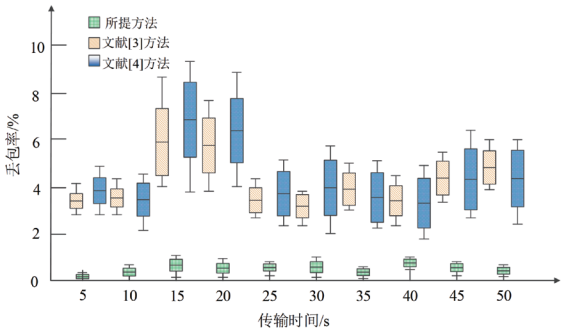

图 2 丢包率

通过图 2 可知，图中箱体的中位线和长度分别反映了网络丢包率的均值和波动幅度。不同时间段内传输数据量不同，网络中的拥塞程度也不同，导致网络丢包率的均值和波动幅度也不同，但在第 15 s 网络遭受到恶意节点攻击时，文献 [3] 方法和文献 [4] 方法中网络丢包率的均值和波动幅度均出现大幅度上升，而所提方法的上升幅度较小，且在整个数据传输过程中的丢包率波动幅度和均值一直远低于其他两种方法，因此，所提方法具有更好的网络信息防御效果。

2.2 网络能耗

为了进一步判断所提方法、文献 [3] 方法和文献 [4] 方法的网络信息安全防御效果，先利用上述三种方法对持续遭受恶意节点攻击的异构网络展开防御控制，防御过程中的网络能耗随防御时间变化的情况如图 3 所示。

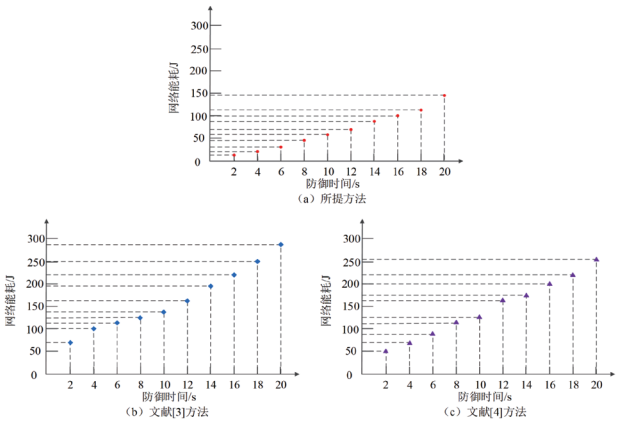

图 3 网络能耗

通过图 3 可知，随着防御时间的增长，防御攻击的开销不断增大，三种方法中的网络能耗逐渐增大，但所提方法的上升幅度最小，且当防御时间相同时，所提方法的网络能耗低于文献 [3] 方法和文献 [4] 方法，表明所提方法的网络防御系统的资源开销较小，网络防御效果更好。

2.3 攻击危害指数

在对异构网络信息展开安全防御的实验中，攻击危害指数反映了攻击对整个异构网络造成的危害程度，攻击危害指数越高，表明攻击对网络造成的危害程度越高，网络信息的安全防御能力越低；反之，攻击危害指数越低，网络信息的安全防御能力越高。设定 h_a 是异构网络的攻击危害指数，对于 h_a 的计算过程为：

$$h_a = (t(V)+t(O)+t(S))\times A \quad (13)$$

式中：$t(V)$、$t(O)$ 和 $t(S)$ 分别表示异构网络信息资产在机密性、完整性和可用性方面的价值；A 表示攻击累计成功概率。现利用所提方法、文献 [3] 方法和文献 [4] 方法对图 1 中的异构网络中的攻击节点展开防御，并根据公式（13）计算不同方法防御下的攻击危害指数，攻击危害指数随网络攻击节点数量变化的情况如表 1 所示。

表 1 攻击危害指数

攻击节点数量	所提方法	文献 [3] 方法	文献 [4] 方法
2	169	289	225
4	173	293	233
6	178	299	241
8	185	308	252
10	191	316	264
12	199	329	273
14	206	337	286
16	213	345	297
18	217	361	315
20	224	385	338

分析表 1 可知，随着异构网络中攻击节点数量的增长，整个网络遭受的攻击强度增大，因此三种方法防御下的攻击危害指数均有所上升，但所提方法的攻击危害指数整体上升幅度最小，且当攻击节点数量相同时，所提方法的攻击危害指数远低于文献 [3] 方法和文献 [4] 方法，表明所提方法的网络信息安全防御能力最强。

3 结语

为了提高异构网络运行的安全性和信息传输效率，提出了面向多业务场景的异构网络信息安全防御技术。通过 K-means 算法对异构网络展开分类，然后利用椭圆曲线加密算法完成数据簇加密，最后根据不同业务场景中的节点信任值完成网络的安全防御。经验证，该方法能够有效降低异构网络的丢包率和能耗，且具有较好的网络防御效果，为后续网络数据的安全传输研究提供了数据支持。

参考文献：

[1] 陈永，刘雯，常婷 . 基于量子密钥的高速铁路异构网络安全切换 [J]. 铁道学报 ,2023,45(11):78-89.

[2] 陈辉定 . 基于计算机网络技术的网络信息安全防护体系构建 [Z]. 现代雷达 ,2023,45(2):I0006-I0008.

[3] 陈娜，黄金诚，李平 . 结合对比学习的图神经网络防御方法 [J]. 计算机科学与探索 ,2023,17(8):1949-1960.

[4] 王佳，张扬眉，苏武强，等 . 基于压缩感知的神经网络实时综合防御策略 [J]. 计算机学报 ,2023,46(1):1-16.

[5]SUN K, QIU W, DONG Y, et al.WAMS-based HVDC damping control for cyber attack defense[J].IEEE transactions on power systems, 2022,38(1):702-713.

[6]ZHENG Y, LI Z, XU X, et al.Dynamic defenses in cyber security: techniques, methods and challenges[J].Digital communications and networks, 2022,8(4):422-435.

[7] 唐林 . 自动采摘目标图像快速识别算法研究：基于 K-means 聚类算法 [J]. 农机化研究 ,2023,45(5):32-36.

[8] 樊燕燕，韩诗雨，江旭，等 . 基于组合赋权－欧氏距离的高原铁路运营期安全系统韧性评价 [J]. 铁道科学与工程学报 , 2023, 20(9):3536-3546.

[9] 董建江，田野，张建兴，等 . 基于随机森林算法的底栖动物高光谱数据分类方法研究 [J]. 光谱学与光谱分析 , 2023, 43(10):3015-3022.

[10] 王华华，郑明杰，陈峰，等 . 基于 LDPC 和椭圆曲线加密算法的密钥协商方案 [J]. 南京邮电大学学报 (自然科学版), 2022, 42(3):30-35.

[11] 陈立军，蒋慧勇 .Feistel 和 SPN 混合轻量级密码算法 [J]. 大连工业大学学报 ,2023,42(4):288-298.

[12] 翟社平，童彤，白喜芳 . 基于区块链的属性代理重加密数据共享方案 [J]. 计算机工程与应用 ,2023,59(8):270-279.

[13] 刘云，宋凯，陈路遥，等 . 均衡评估算法对基于区块链的无线传感网节点信任管理优化 [J]. 山东大学学报 (理学版), 2022, 57(7):73-84.

[14] 陈友荣，章阳，陈浩，等 . 面向车联网异构节点的区块链高效一致性共识算法研究 [J]. 电子与信息学报 , 2022, 44(1): 314-323.

[15] 张迪，曹利，李原帅 . 车联网环境下基于多策略访问树的安全访问控制算法 [J]. 计算机应用研究 ,2023,40(11):3394-3401.

【作者简介】

陈长松（1981—），男，河南驻马店人，硕士，数据库系统工程师，研究方向：网络安全。

（收稿日期：2024-06-03）