基于态势感知的 SWIM 服务权限主动移交模型

吴志军，周胜琰，雷缙
（中国民航大学电子信息与自动化学院，天津 300000）

摘 要：为解决广域信息管理（SWIM）服务提供者由于自身故障或受到恶意攻击，造成 SWIM 服务中断、服务时延增加或服务质量下降的问题，提出了一种基于态势感知的 SWIM 服务权限主动移交模型，利用随机森林算法判别 SWIM 服务提供者安全态势，依据安全态势主动移交 SWIM 服务权限，降低突发事件对 SWIM 服务的影响。实验证明，所提模型能够在突发事件发生的情况下保证服务的连续性，与未部署服务移交模型的 SWIM 网络相比，具有更高的可靠性和稳定性。

关键词：广域信息管理；服务移交；态势感知；随机森林；应急响应
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019171

Proactive migration model of SWIM service based on situation awareness

WU Zhijun, ZHOU Shengyan, LEI Jin
College of Electronic Information and Automation, Civil Aviation University of China, Tianjin 300000, China

Abstract: To solve the problem that in the system wide information management (SWIM) network, the SWIM service provider suffers from SWIM service interruption, service delay increase or service quality degradation due to malicious attack or self-failure. Therefore, a proactive migration model of SWIM service was proposed on the basis of situation awareness, which used the random forest algorithm to timely judge the SWIM service provider security situation. SWIM service authority was actively migrated according to security situation, and the emergencies impact on SWIM services were reduces. Experimental results show that the proposed model can guarantee services continuity in an emergency event, which has higher reliability and stability than SWIM network in which the service migration model is not deployed.

Key words: SWIM, service migration, situation awareness, random forest, emergency response

1 引言

为提高 ATM（air traffic management）服务提供者之间的全球互操作性，增强各部门之间信息共享，打破异构服务之间信息交换的瓶颈，1997 年，欧洲航空安全组织首次向美国联邦航空局提出广域信息管理（SWIM, system wide information management）的概念。2005 年，国际民航组织（ICAO, International Civil Aviation Organization）将 SWIM 作为国际航空信息发布系统，美国和欧洲分别于 2007 年部署“下一代航空运输系统”计划和“欧洲单一天空空中交通管理研究计划”，均将 SWIM 作

收稿日期：2018−12−21；**修回日期**：2019−07−01
基金项目：天津市自然科学基金重点基金资助项目（No.17JCZDJC30900）；国家自然科学青年基金资助项目（No.61601467）；2018 年中央高校基本科研业务费基金资助项目（No.3122018D007）
Foundation Items: The Key Program of Natural Science Foundation of Tianjin (No.17JCZDJC30900), The National Science Foundation for Young Scientists of China (No.61601467), The Fundamental Research Funds for the Central Universities of China (No.3122018D34007)

为信息沟通和数据共享的架构[1]。广域信息管理作为下一代空中交通管理的核心[2]，连接了民航信息网络的各个组成部分，整合了民航各类业务资源（包括空域管理、流量管理、交通管理、监控管理、飞行器系统等），对通信数据、导航数据、监控数据、气象信息、全球地理信息和各类飞行对象加以管理，是民航网络信息交互和数据共享的关键组成部分。

随着越来越多的用户通过 SWIM 获取民航服务数据，SWIM 服务的数据交互越发频繁，面临的安全威胁也越来越突出。SWIM 网络安全研究主要集中在 SWIM 安全技术标准[3]、数据安全威胁分析[4]、数据实时交互保障[5]、数据传输加密认证[6]和数据安全与共享[7]，虽然实现了数据安全和隐私保护，但是没有针对恶意攻击、系统故障、突发事件等一系列安全威胁做出应急响应。SWIM 作为一个大规模分布式网络，因其服务提供者的自身硬件性能和地理位置信息各不相同，面临的安全威胁也不尽相同，因此，有必要提出一种从 SWIM 服务提供者角度出发的保护模型，能够结合自身性能特点准确判断安全态势，主动移交 SWIM 服务权限，减少突发事件对 SWIM 服务造成影响。

2 相关工作

目前，服务移交机制的研究已经取得了不少成果，黄遵国等[8]在服务集群内采用多种随机竞争机制实施进程迁移，服务器漂移具有较高的随机性，但攻击者可能发起时间漏隙攻击，同时漂移机制缺乏可控性，容易造成网络振荡。洪小亮等[9]对文献[8]中服务漂移的触发机制和竞争机制进行了改进，可以有效抵抗时间漏隙攻击，但是单一的服务漂移模式降低了服务漂移的随机性。文献[10]提出了一种服务漂移模型，把服务模型抽象为一个部分可观测马尔可夫决策过程，可以计算出使客户获益最高的服务漂移策略，但是该模型触发机制设计不合理，容易造成时间冲突。文献[11]利用各种检测平台的告警信息，提出了一种基于网络可生存性态势感知的主动服务漂移模型，模型未对告警数据进行联合分析，容易发生虚警漂移，增加系统负担[11]。文献[12]提出了一种云计算环境下的最优 Web 服务迁移架构，该架构以负载为移交服务触发衡量标准，触发条件单一，不能保证服务的安全性。由于 SWIM 网络是面向服务的大规模信息网络，面临多种维度的安全威胁，仅从单一角度触发移交机制不适应 SWIM 网络安全需要，本文提出了一种基于态势感知的服务移交触发机制，联合多维安全威胁信息判断安全态势。网络安全态势感知最早是 Tim Bass 提出并广泛应用于航空等领域，是对安全态势数据的不断观测、提取、理解及预测[13]。安全态势评估是态势感知的一部分，安全态势评估算法有模糊综合评价法[14]、机器学习算法[15]、概率模型算法[16]等。本文依据 SWIM 节点安全态势决策是否触发主动移交机制，将安全态势评估由数值型问题转变为分类问题，消除了人为设置安全阈值的主观因素干扰，能够通过真实数据学习训练，更符合真实环境下的安全需求。

3 SWIM 服务权限主动移交模型

在某航班飞行过程中，航空公司作为 SWIM 服务消费者（SC, service consumer），通过 SWIM 网络获取航空监视数据、机场地面信息和航空气象等信息；空管部门提供航空监视数据服务、航空气象服务；机场提供机场地面信息服务。如果该空管单位由于遭受恶意攻击或发生自然灾害导致服务延时增加或服务突然中断，对航班飞行造成安全威胁，那么，必须快速找到一个可靠的空管部门作为移交目标，由它继续提供服务，因此，保证 SWIM 服务的连续性和稳定性是关键。本文在原 SWIM 网络的基础上引入了一种 SWIM 服务权限主动移交模型，如图 1 所示，将 SWIM 网络中服务主题相同的 SWIM 服务提供者（SP, service provider）视为对等服务提供者，在突发事件发生时从对等服务提供者中选择节点继续提供 SWIM 服务，保证了在单点或部分 SP 失效情况下 SWIM 服务的连续性。

1) SC 通过 SWIM 网络获取对应服务，实际上是 SC 通过查询具有全网一致性的服务信息注册列表[17]，将对应服务主题的 SWIM 服务数据发送给 SC，具体由哪个 SP 来提供 SWIM 服务数据对 SC 来说是不可知的。SWIM 旨在融合多元服务数据来提升 SC 联合决策能力，只有保证 SP 的安全运行，才能确保 SWIM 服务的可靠性。各 SWIM 用户之间采用标准的协议交互，相互采用松耦合的方式连接[18]，各 SWIM 用户之间相对独立，因此，通过移交故障节点 SP 的服务权限来保证 SWIM 服务的连续性是可行的。

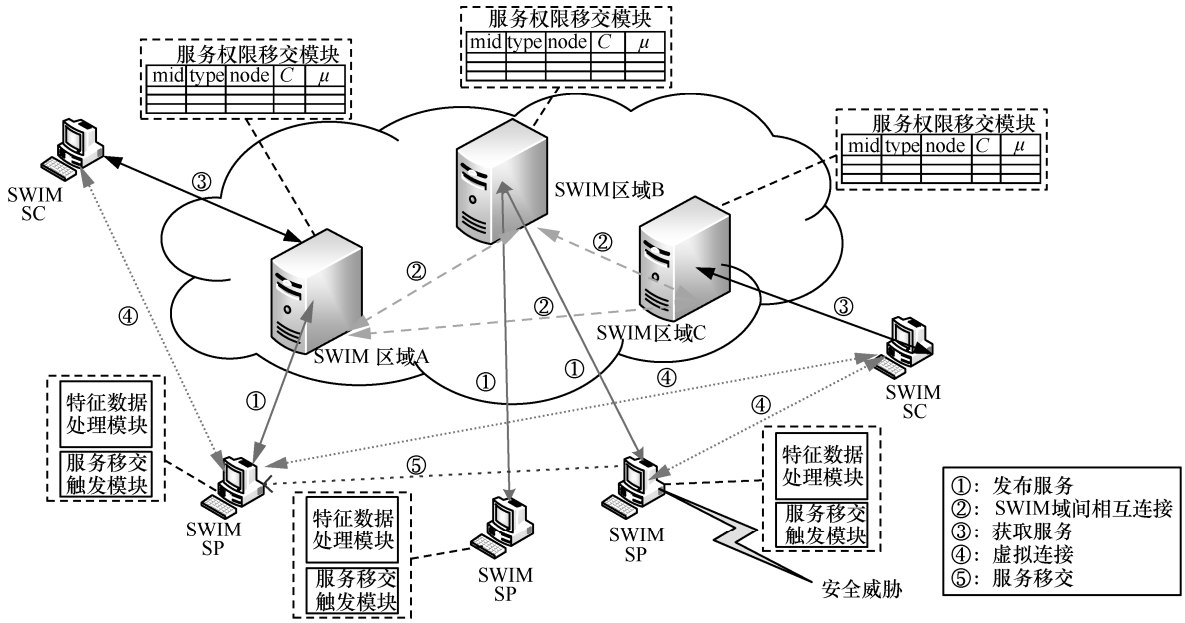


图 1　SWIM 服务权限主动移交模型

2) 如果 SP 自身状态信息实时发送给 SWIM 网络，将增加 SWIM 网络工作负担，占用网络带宽，影响 SWIM 服务质量。另外，SP 的安全态势大部分时间都处于正常状态，实时传输的自身状态信息中存在大量冗余信息，同时考虑到 SP 之间硬件设施和地理环境的差异性，因此，将服务移交触发模块分布在 SP 本地，只有突发事件发生才会向 SWIM 发送状态信息，减轻了 SWIM 网络流量负担，保证了 SWIM 网络带宽的高效利用。

3) SWIM 网络由多个分布式 SWIM 域组成，SWIM 域间相互连接，可以快速获取全网 SP 的安全状态信息，因此将服务权限移交模块部署在 SWIM 核心服务中，依据迁移期望最大化原则选择移交目的 SP，将 SWIM 服务权限无缝地移交至该 SP 上。

4　SWIM 服务权限主动移交机制

SWIM 服务权限主动移交机制如图 2 所示。

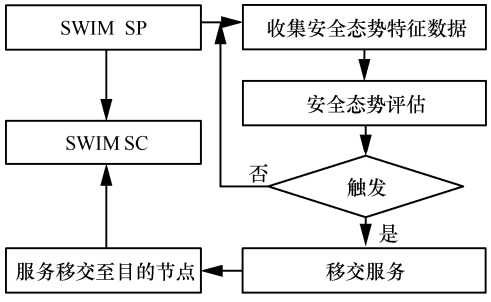


图 2　SWIM 服务权限主动移交机制

首先由某 SP 向 SWIM 用户提供服务，同时周期性地收集安全态势特征数据，并对系统当前所处的安全态势进行评判，依据评估结果触发服务移交机制，当未触发服务移交机制时，继续向 SWIM 用户提供服务并周期收集自身安全态势特征数据，当触发服务移交机制时，从备选服务提供者中选择移交目的节点，由目的节点向该 SWIM 用户继续提供服务。由此可知，实现 SWIM 服务权限主动移交机制需要解决 3 个问题：1) 安全态势特征数据的选取和处理，2) SP 安全态势评估，3) 选择移交对象。本文使用 3 个模块解决上述 3 个问题，具体如下。安全态势特征数据处理模块从多维度收集安全威胁信息并对其进行预处理；服务移交触发模块根据监测安全态势特征数据判断安全态势；服务权限移交模块根据预判结果触发 SWIM 服务权限主动移交机制。

4.1　安全态势特征数据处理模块

SWIM 服务提供者安全态势隐含在海量的监测告警数据中，为了能够在复杂多变的网络环境中准确感知自身安全态势，必须充分考虑影响 SP 安全态势的各种因素，提取关键特征信息。依据 SP 的监测信息判断安全态势，从而根据自身安全态势实施主动防御机制，提升 SWIM 服务的可生存性，考虑到系统硬件性能、恶意攻击、自身漏洞和突发灾害等因素对系统安全态势的影响，本文主要通过负载威胁指数、攻击威胁指数、漏洞威胁指数、环境威胁指数、节点服务威胁指数 5 个特征评估安全态势。

定义 1 负载威胁指数 TL_N。t 时刻，SP 节点 N 的自身负载情况，反映了 SP 处理服务的能力。影响负载变化的硬件参数有很多，本文主要考虑 3 种参数即 CPU 使用率（CPU%）、带宽使用率（Band%）和内存利用率（MEM%）[19]来衡量负载情况。根据 SP 提供服务属性不同，可以分为计算消耗型服务和通信消耗型服务。依据服务类型对硬件资源的消耗程度情况分配权值 w，权值分配如表 1 所示。

表 1 权值分配

节点服务类型	w_1	w_2	w_3
计算消耗型	0.5	0.3	0.2
通信消耗型	0.4	0.4	0.2

在 SWIM 运行过程中不断优化这些参数，则 SP 节点 N 在 t 时刻的负载威胁指数如式(1)所示。

$$\mathrm{TL}_N = w_1\mathrm{CPU}_t\% + w_2\mathrm{Band}_t\% + w_3\mathrm{MEM}_t\% \tag{1}$$

其中，

$$\sum_{i=1}^{3} w_i = 1 \tag{2}$$

定义 2 攻击威胁指数 TA_N。在 $[t-\Delta t, t]$ 时间区间内，SP 节点 N 所受恶意攻击对 SWIM 服务造成的威胁值。SWIM 服务节点部署了多种攻击检测传感器，统计告警信息中攻击 i 的攻击次数 C_i 和攻击强度 D_i，依据 SNORT 用户手册将攻击强度分为低、中、高 3 个等级，分别用 1、2、3 表示，攻击 i 的攻击威胁值如式(3)所示。

$$\mathrm{TA}_{Ni} = C_i \times 10^{D_i} \tag{3}$$

在 $[t-\Delta t, t]$ 时间区间内共有 n 种攻击发生，则可由式(4)计算节点攻击威胁指数。

$$\mathrm{TA}_N = \sum_{i}^{n} C_i \times 10^{D_i} \tag{4}$$

定义 3 漏洞威胁指数 TV_N。t 时刻，系统检测漏洞对 SWIM 节点造成的安全威胁指数。将检测漏洞按照通用漏洞评分系统（CVSS, common vunerability scoring system）的度量标准计算漏洞威胁指数[20]，漏洞威胁指数计算如式(5)所示。

$$\mathrm{TV}_N = \sum_{j=1}^{m} (0.6T_{Mj} + 0.4T_{Bj} - 1.5) f(T_{Mj}) \tag{5}$$

其中，T_{Mj} 是第 j 个漏洞对系统安全态势的影响值，分别从 SP 的机密性 C_j、完整性 I_j 和可用性 A_j 这 3 个方面来考量。

$$T_{Mj} = 10.41\left(1-(1-C_j)(1-A_j)\times(1-I_j)\right) \tag{6}$$

T_{Bj} 是第 j 个漏洞被攻击利用可能性的量化值，分别从攻击途径 A_{Vj}、复杂度 A_{Cj} 和认证 A_{Uj} 这 3 个指标来衡量。

$$T_{Bj} = 20 \times A_{Vj} \times A_{Cj} \times A_{Uj} \tag{7}$$

m 为系统在 t 时刻检测到漏洞的个数。$f(T_{Mj})$ 是对 m 个漏洞对系统安全态势影响值的统计平均后的结果。

$$f(T_{Mj}) = \begin{cases} 0, & T_{Mj} = 0 \\ 0.117\,6, & T_{Mj} \neq 0 \end{cases} \tag{8}$$

系统各漏洞安全态势影响考量要素度量值分配如表 2 所示[20]。

表 2 度量值

要素	分类	属性值
机密性 C_j	无/低/高	0/0.22/0.56
完整性 I_j	无/低/高	0/0.22/0.56
可用性 A_j	无/低/高	0/0.22/0.56
攻击途径 A_{Vj}	远程/本地	0.85/0.2
复杂度 A_{Cj}	高/中/低	0.6/0.8/1.0
认证 A_{Uj}	需要/不需要	0.62/0.85

定义 4 环境威胁指数 TE_N。t 时刻，SP 节点 N 由于自然灾害对 SWIM 服务造成的安全威胁指数。依据相关部门的自然灾害预警信息和环境感知信息计算环境威胁指数 TE_N，如式(9)所示。

$$TE_N = \begin{cases} 1, \text{自然灾害发生} \\ P_t, \quad \text{其他} \end{cases} \tag{9}$$

其中，若 t 时刻已经发生自然灾害，将 TE_N 置 1，否则将 TE_N 置为 P_t，P_t 代表相关预警部门对该 SP 发生自然灾难的估计概率。

定义 5 节点服务威胁指数 TS_N。t 时刻，SP 节点 N 对外提供服务的可能性。若提供服务的下一时间节点为 t_{service}，设置时间阈值 t_q，只有在$[t_{\text{service}}-t_q, t_{\text{service}}]$时间区间内 SP 发生故障才可能对服务造成影响，时刻 t 与 t_{service} 越接近，节点服务威胁指数越大，则节点服务威胁指数 TS_N 为

$$\mathrm{TS}_N = \begin{cases} \left(1-|V|^2\right)^2, & |V| \leqslant 1 \\ 0, & |V| > 1 \end{cases} \tag{10}$$

$$V = \frac{t_{\text{service}} - t}{t_q} \tag{11}$$

其中，t_q=30 s。

4.2　服务移交触发模块

通过计算 SP 各维特征威胁指数，仅从局部衡量了 SP 节点某方面的安全威胁，未能从整体上科学地评估 SP 节点安全态势。本文依据安全态势触发 SWIM 服务权限主动移交机制，将 SWIM 节点的安全态势分为安全和威胁 2 种，对应继续监测和移交服务 2 种响应策略，那么，SP 节点安全态势评估不再是一个数值型问题，而是转化为分类问题，将各维特征威胁指数生成特征向量并利用分类算法评判出节点所处态势。常见的分类算法有随森林算法、逻辑回归算法、KNN（k-nearest neighbor）算法、神经网络算法、贝叶斯分类器等。其中，随机森林算法是一种能够在提升精度的情况下保证运算量的机器学习分类算法，随机森林是在决策树的基础上演化而生的，在随机森林内部构建多个相对独立的决策树，在训练完成后，能够在新样本到来时，决策出样本的类别[21]。随森林算法步骤如下。

1) 初始化原始训练数据集 D，在随机森林内部构造 K 棵决策树，每棵决策树的训练样本个数均为 N，按照 Bootstrap 法从原始训练数据集 D 中有放回地随机抽取 K 个规模为 N 的训练数据子集，利用 K 个训练数据子集分别训练 K 棵决策树。

2) 假设每个训练样本共有 L 个输入特征，从 L 个输入特征中随机选择 l 个(l<L)输入特征，利用这 l 个输入特征决定最优分裂点。

3) 不对分类树作任何处理，使其自由生长。

4) 最终生长出的 K 棵决策树组成随机森林，当有新的样本输入时，随机森林中每棵决策树分别对样本进行分类，最终分类结果由每棵决策树投票决定。

利用随机森林算法，以 Δt 为周期定期观测计算威胁指数，将 SP 节点 N 安全威胁指数生成特征向量 $\boldsymbol{T}_N$=(TL_N, TA_N, TV_N, TE_N, TS_N)，并将其作为随机森林算法的输入，对系统状态进行安全态势评估，依据节点安全态势触发 SWIM 服务主动移交机制。

4.3　服务权限移交模块

服务权限移交模块位于 SWIM 核心服务中，用来管理本地 SWIM 域下的 SWIM 用户。服务权限移交模块的信息列表由五元组(mid, type, node, C, μ)组成，其中，mid 代表移交标识信息，取值为“0”或“1”，“0”表示该 SP 正常提供服务，“1”表示该 SP 需要移交 SWIM 服务权限；type 代表该 SP 提供的服务主题；node 表示该 SP 的节点信息；C 是 n 个订阅该 SP 服务的 SC 节点信息的集合，C=$\{C_j|i$=1,2,⋯,$n\}$；μ 表示该 SP 的相对指数，根据 SP 的各维威胁特征指数，利用模糊多属性决策算法[22]，计算相同服务主题 SP 之间的相对指数，安全性能越强 μ 则越大，当有待移交服务时，更新 μ 值。具体过程如下。

首先，在服务权限移交模块中构造移交目的节点评估矩阵 $\boldsymbol{T}$。

$$\boldsymbol{T}=\begin{bmatrix} T_{11} & T_{12} & \cdots & T_{1m} \\ T_{21} & T_{22} & \cdots & T_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ T_{n1} & T_{n2} & \cdots & T_{nm} \end{bmatrix} \tag{12}$$

其中，T_{ij} 代表 SP 节点 i 的第 j 维安全态势特征值。

为了消除物理单位对数据的干扰，将评估矩阵进行归一化得到 $\boldsymbol{T}_1$。

$$\alpha_{ij}=\begin{cases} \dfrac{\max\limits_i T_{ij}-T_{ij}}{\max\limits_i T_{ij}-\min\limits_i T_{ij}}, & \max\limits_i T_{ij}-\min\limits_i T_{ij}\neq 0 \\ 1, & \max\limits_i T_{ij}-\min\limits_i T_{ij}=0 \end{cases} \tag{13}$$

其中，$i=1,2,\cdots,n$，$j=1,2,\cdots,m$。

$$\boldsymbol{T}_1=\begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nm} \end{bmatrix} \tag{14}$$

依据归一化评估矩阵 $\boldsymbol{T}_1$，分别构造最优特征向量 $\boldsymbol{g}$ 和最差特征向量 $\boldsymbol{b}$，如式(15)和式(16)所示。

$$\boldsymbol{g}=[g_1,g_2,\cdots,g_m]=\left[\max_i\alpha_{i1},\max_i\alpha_{i2},\cdots,\max_i\alpha_{im}\right] \tag{15}$$

$$\boldsymbol{b}=[b_1,b_2,\cdots,b_m]=\left[\min_i\alpha_{i1},\min_i\alpha_{i2},\cdots,\min_i\alpha_{im}\right] \tag{16}$$

分别计算备选节点特征向量与最优节点、最差节点特征向量之间的欧氏距离。

$$d_{ig}=\sqrt{\sum_{j=1}^{m}\beta_j(\alpha_{ij}-g_j)^2} \tag{17}$$

$$d_{ib}=\sqrt{\sum_{j=1}^{m}\beta_j(\alpha_{ij}-b_j)^2} \tag{18}$$

$$\beta=[\beta_1,\beta_2,\cdots,\beta_m] \tag{19}$$

其中，β 是节点各维安全威胁指数对待移交服务的影响程度。

根据各节点的 d_{ig}、d_{ib} 可求的节点 i 相对于其他备选节点的优差程度 μ_i。

$$\mu_i=\frac{1}{1+\left(\dfrac{d_{ig}}{d_{ib}+1}\right)^2} \tag{20}$$

SWIM 服务提供者触发服务权限移交机制后，服务权限移交机制流程如图 3 所示。

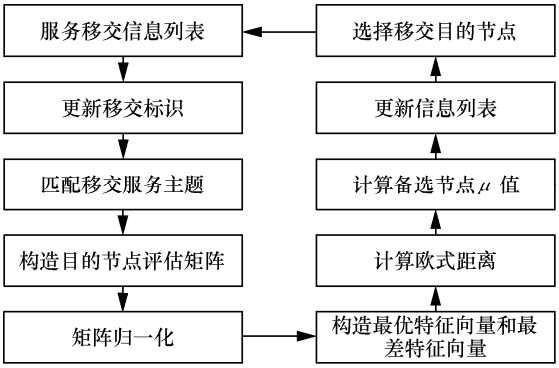


图 3　服务权限移交流程

服务权限移交模块向 SWIM 注册中心请求待移交服务的服务状态信息，SWIM 注册中心收到该请求后，删除待移交 SP 注册发布的服务信息，该 SP 的移交标识信息更新为 1。待移交 SP 可能提供多种服务，降级为多个基础服务，查询移交信息列表，更新相同服务主题 SP 的 μ 值，依据 μ 值选择目的节点。

SWIM 服务权限移交过程包括以下步骤。

1) SWIM 网络根据 SP 发送移交请求信息更新全网移交信息列表，移交信息列表依据时间戳依次完成服务移交。

2) 移交信息列表中待迁移服务节点中每类待移交服务主题分别与移交信息列表匹配，将匹配到的节点组成备选移交目的节点并构建节点评估矩阵。

3) 按照模糊多属性决策算法计算各备选移交目的节点的 μ 值，并将 μ 值更新到服务权限移交模块信息列表，从中选择最大 μ 值节点作为移交目的节点。

4) 服务权限移交模块向移交目的 SP 发送服务状态信息，并将 SC 请求信息转发至目标 SP，或由目标 SP 向原服务的缓存空间传送服务数据。

5　实验结果与分析

为了验证 SWIM 服务主动移交机制的有效性，本文在真实网络环境中根据 SWIM 网络体系结构搭建了仿真平台，其网络拓扑结构如图 4 所示。仿真平台由 PC 机、服务器、路由器和交换机组成。其中，一台 PC 机模拟 SC 获取 SWIM 服务；2 台 PC 机作为 SWIM 接入节点，提供 SWIM 服务注册、查询与管理功能；5 台 PC 机作为 SP 提供 SWIM 服务。

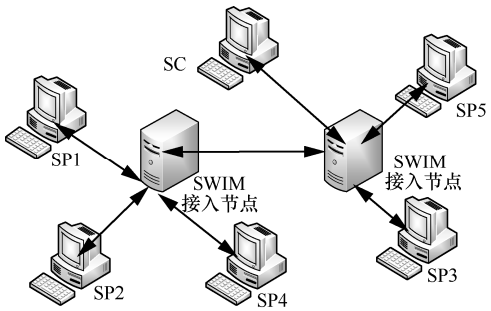


图 4　测试平台网络拓扑

实验 PC 机的硬件配置如表 3 所示。

表 3　　实验 PC 机的硬件配置

名称	操作系统	处理器	内存/GB
SC	Ubuntu 14.04	i5-4590 3.30 GHz	4
SWIM 接入节点	Ubuntu 14.04	P4 2.2 GHz	2
SP	Ubuntu 14.04	i5-4590 3.30 GHz	4

SP 使用 Apache 作为服务器，Mysql 作为数据库存放 SWIM 服务数据。以 SWIM 航班信息交换模型（FIXM, flight information exchange model）[23] 和 SWIM 航空信息交换模型（AIXM, aeronautical information exchange model）[24]为标准，分别提供航班信息服务和航空信息服务。

5.1　随机森林算法性能

首先，验证随机森林算法触发移交机制的可靠性。采用我国某空管分局提供的真实飞行情报服务物理节点安全态势观测数据用于算法训练。在物理节点在对外提供服务数据的情况下，利用多种监测手段定期统计物理节点上服务器的相关数据，包括 CPU、内存和带宽。并从防火墙和入侵检测系统中获得相关攻击数据，利用漏洞扫描系统得到系统漏洞信息。然后，对获得的数据进行统计分析得到安全态势数据，依据服务反馈情况评价该 SWIM 物理节点的安全态势，得到该节点安全态势统计数据，如表 4 所示。

本文将安全态势统计数据进行威胁指数处理后作为训练数据集使用。在实验中，设 Δt=60 s，采用 1 600 组历史数据作为训练数据集，每组历史训练数据包括当前时刻 t 的安全威胁指数监测值 TL_N、TA_N、TV_N、TE_N、TS_N 和对应的 SWIM 节点安全态势；测试数据为 500 组，从 500 组测试数据中随机抽取 10 个分类结果如表 5 所示。

随机森林算法分类结果与真实态势统计类型如表 6 所示。其中，TT 为分类结果为威胁的真实

表 4　　节点安全态势统计数据

时间戳	CPU%	Band%	MEM%	攻击编号	攻击次数/次	攻击类型	漏洞信息	环境威胁	服务时间	是否安全
2018−05−05 15:20:30	0.32	0.28	0.22	A_1	3	1	缓存溢出	0.2	15:23:30	是
2018−05−05 15:21:30	0.24	0.44	0.32	A_2	5	1	缓存溢出	0.2	15:23:30	是
				A_3	2	1				
2018−05−05 15:22:30	0.59	0.71	0.51	A_4	28	3	访问控制错误，权限许可	0.1	15:23:30	否
				A_5	12	2				
				A_6	15	2				
2018−05−05 15:23:30	0.41	0.34	0.36	A_7	3	2	SQL 注入	0.2	15:25:30	是
2018−05−05 15:24:30	0.36	0.42	0.47	A_8	2	3	访问控制错误	0.7	15:25:30	否
2018−05−05 15:25:30	0.45	0.38	0.29	A_9	2	1	权限许可	0.3	15:26:30	否

表 5　　随机森林算法分类结果

序号	TL_N	TA_N	TV_N	TE_N	TS_N	真实态势	分类态势
1	0.56	0	0.114 7	0.1	0.208 7	安全	安全
2	0.62	0	0.221 4	0.6	0.084 7	安全	安全
3	0.66	100	0.342 1	0.1	0.260 1	威胁	威胁
4	0.74	0	0.158 7	0.2	0.360 7	安全	安全
5	0.61	0	0.136 4	0.2	0.538 4	安全	安全
6	0.52	320	0.412 4	0.1	0.634 6	威胁	威胁
7	0.86	0	0.214 1	0.3	0.451 1	威胁	威胁
8	0.71	640	0.542 1	0.2	0.725 5	威胁	威胁
9	0.65	0	0.631 2	0.1	0.491 1	威胁	威胁
10	0.58	0	0.104 7	0.1	0.596 7	安全	安全

威胁的样本个数，FT 为分类结果为安全的真实威胁的样本个数，TF 为分类结果为威胁的真实安全的样本个数，FF 为分类结果为安全的真实安全的样本个数。

表 6　　分类结果与真实态势统计类型

真实态势	分类结果：威胁	分类结果：安全
威胁	TT	FT
安全	TF	FF

具体性能指标计算式如式(21)～式(24)所示。

$$准确率=\frac{TT+FF}{TT+FF+TF+FT} \tag{21}$$

$$漏警率=\frac{FT}{TT+FT} \tag{22}$$

$$虚警率=\frac{TF}{TF+TT} \tag{23}$$

$$F\text{-值}=\frac{2\times TT}{2\times TT+FT+TF} \tag{24}$$

将 500 组测试数据的结果进行统计，并与贝叶斯分类算法的分类结果进行比较分析，得到 2 种分类算法的性能对比结果，如表 7 所示。实验结果表明在采用相同训练数据集和测试集的情况下，随机森林算法的准确率、漏警概率等指标均优于贝叶斯算法。

表 7　　分类算法性能对比

分类算法	准确率	虚警率	漏警率	*F*-值
随机森林算法	94.8%	2.8%	7.2%	94.9%
贝叶斯算法	88.2%	8.3%	15%	88.2%

5.2　主动移交机制性能分析

在 SC 获取 SWIM 服务的过程中，模拟突发故障和恶意攻击，通过与未部署 SWIM 服务主动移交模型的 SWIM 网络（Non-PMM）和传统服务漂移机制（TSMM, traditional service migration mechanism）对比，判断 SWIM 主动移交模型能否满足 SWIM 网络应急响应的需求。主要从吞吐量和服务

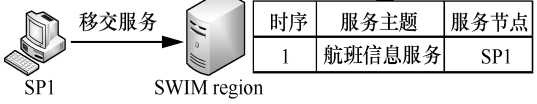
平均时延两方面考察系统性能[25]，其中服务器提供者与服务主题对应关系如表 8 所示。

表 8 服务提供者与服务主题对应关系

SP 编号	服务主题
SP1	SWIM 航班信息服务
SP2	SWIM 航班信息服务
SP3	SWIM 航班信息服务
SP4	SWIM 航空信息服务
SP5	SWIM 航空信息服务、SWIM 航班信息服务

模拟 10 个 SC 用户通过 SWIM 订阅 SWIM 航班信息服务，最初由 SP1 对该订阅用户 SC1 和 SC2 提供服务。当 SP1 突发系统故障对 SWIM 造成安全威胁时，SP1 感知自身安全态势并触发 SWIM 服务权限移交机制，SWIM 收到移交请求后更新全网移交信息列表，全网移交信息列表中包含了 SWIM 网络中所有待移交服务，依据时间戳顺序，依次将服务权限移交至其他节点，同时将服务权限移交模块信息列表中 SP1 的移交标识信息更新为 1，如图 5 所示。

移交标识信息	服主题	服务节点	SC订阅	相对指数
1	航班信息服务	SP1	SC1;SC2	0.841 4
0	航班信息服务	SP2	SC3;SC4	0.825 3
0	航班信息服务	SP3	SC5;SC6	0.887 6
0	航空信息服务	SP4	SC7;SC8	0.912 8
0	航班信息服务 航空信息服务	SP5	SC9;SC10	0.864 1



时序	服务主题	服务节点
1	航班信息服务	SP1

图 5 SWIM 服务移交信息列表

根据图 5 中全网移交信息列表中待移交服务主题，SWIM 服务权限主动移交模块依据目标节点选取策略，获取 SP2、SP3、SP5 的多维安全特征值，并构造移交节点评估矩阵。

$$\boldsymbol{T}=\begin{bmatrix}0.32 & 100 & 0.342\,1 & 0.1 & 0.214\,7\\ 0.41 & 230 & 0.218\,5 & 0.3 & 0.145\,1\\ 0.39 & 110 & 0.114\,2 & 0.3 & 0.471\,2\end{bmatrix} \tag{25}$$

对矩阵 $\boldsymbol{T}$ 进行归一化处理，得到归一化矩阵 $\boldsymbol{T}_1$。

$$\boldsymbol{T}_1=\begin{bmatrix}1 & 1 & 0 & 1 & 0.786\,6\\ 0 & 0 & 0.542\,3 & 0 & 1\\ 0.222\,2 & 0.923\,1 & 1 & 0 & 0\end{bmatrix} \tag{26}$$

节点各维度安全威胁指数对待移交服务的影响程度 β=[0.2 0.3 0.3 0.1 0.1]，分别计算备选节点特征向量与最优节点、最差节点特征向量之间的欧氏距离为

$$d_{ig}=\begin{bmatrix}0.551\,9 & 0.814\,1 & 0.568\,1\end{bmatrix} \tag{27}$$

$$d_{ib}=\begin{bmatrix}0.813\,6 & 0.433\,9 & 0.752\,0\end{bmatrix} \tag{28}$$

计算可得到节点间相对安全指数如式(29)所示。

$$\mu_i=\begin{bmatrix}0.915\,2 & 0.756\,2 & 0.904\,8\end{bmatrix} \tag{29}$$

SWIM 服务权限主动移交模块将相对安全指数更新到信息列表中，选取相对指数最大的 SP 作为移交目的节点，将待移交服务订阅用户 SC1 和 SC2 的订阅请求移交至 SP2 上，移交后的服务移交信息列表如图 6 所示。

移交标识信息	服务主题	服务节点	SC 订阅	相对指数
1	航班信息服务	SP1	Null	0.841 4
0	航班信息服务	SP2	SC1;SC2 SC3;SC4	0.915 2
0	航班信息服务	SP3	SC5;SC6	0.756 2
0	航空信息服务	SP4	SC7;SC8	0.912 8
0	航班信息服务 航空信息服务	SP5	SC9;SC10	0.904 8

图 6 服务移交后的移交信息列表

5.2.1 SWIM 网络吞吐量

SWIM 网络吞吐量指的是单位时间内 SWIM 成功对外传输数据的大小。为了验证本文方法的性能，考虑在发生突发事件情况下 SWIM 网络吞吐量的变化，本文模拟 1 500 个用户订阅 SWIM 航班信息服务，并在 SWIM 正常提供服务后，注入持续性突发故障，仿真结果如图 7 所示。

其中，SC 通过 SWIM 网络获取航班信息服务，在正常情况下，由于实验硬件设施相同，PMM、Non-PMM、TSMM 三者均能够保证较稳定的吞吐量，吞吐量均维持在 450～550 bit/s，在 50 min 时，向 SC 提供服务的 SP1 发生硬件故障，不能继续提供航班信息服务，50 min 后 Non-PMM 的吞吐量急剧下降；而 TSMM 仅是随机控制 SP1、SP2、SP3 向 SC 提供服务，未能感知其中 SP1 硬件故障，当服务权限移交至 SP1 时，网络吞吐量下降至 0，由其他 SP 提供服务时，吞吐量恢复正常；由于 PMM 能够准确判断 SP 安全态势及时移交 SWIM 服务权限，维持 SWIM 服务的正常运行，吞吐量依旧维持在 450～550 bit/s，能够满足 SWIM 服务安全连续的需要。

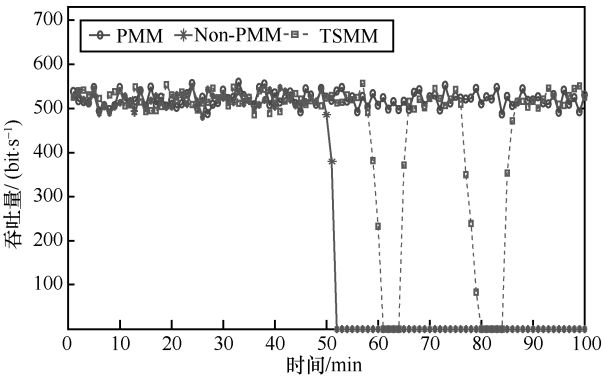


图 7　3 种模型的吞吐量对比

5.2.2　SWIM 服务平均时延

服务时延指的是 SWIM 发送服务数据至订阅用户的时间戳插值。为了验证本文方法的性能，模拟 1 500 个用户订阅 SWIM 航班信息服务，并在 SWIM 正常提供服务后注入持续性突发故障，将订阅用户的服务时延求均值得到服务平均时延，SWIM 航班信息服务平均时延的仿真结果如图 8 所示。

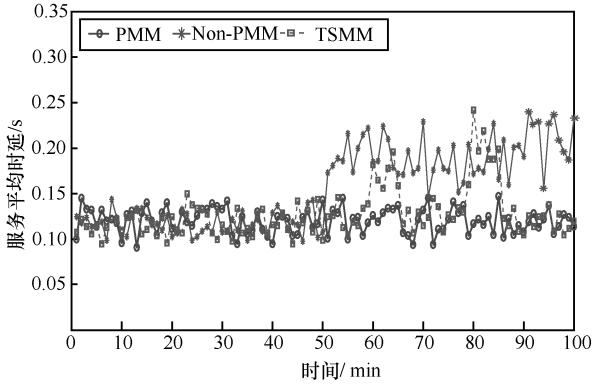


图 8　3 种模型的平均时延对比

如图 8 所示，在 50 min 时，SWIM 网络中提供航班信息服务的 SP1 受到恶意攻击，不能继续提供航班信息服务，Non-PMM 中由该 SP 提供服务的 SC 无法继续获取航班信息服务数据，并得到连接错误返回信息，所以，SWIM 服务平均时延将增大。由受损 SP 对外提供服务时，TSMM 的服务平均时延将增加，由正常节点对外提供服务时，服务平均时延降至正常值；由于 PMM 能够及时移交 SWIM 服务权限，SWIM 服务平均时延依然维持在较稳定的水平。其中，服务响应时间累积概率如图 9 所示，本文提出的模型服务响应时间为 0.14 s 时累积概率为 0.95，即 95%的服务响应时间低于 0.14 s，响应时间明显优于 Non-PMM 和 TSMM 模型。

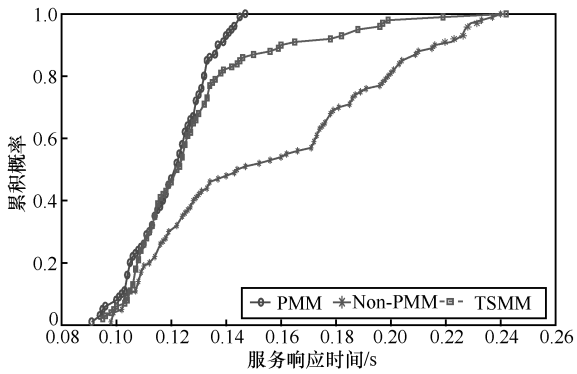


图 9　3 种模型的服务响应时间累计概率对比

通过以上的实验分析可知，SWIM 服务主动移交模型能够在 SP 突发故障或受到恶意攻击时，利用服务移交机制将服务权限移交到相同服务主题的 SP，提升了 SWIM 网络的可生存性，增强了 SWIM 网络应对突发事件的能力，降低了突发事件带来的影响。

6　结束语

SWIM 作为下一代空中交通管理的核心，保证 SWIM 安全运行，实施有效的应急响应机制十分重要。本文提出了一种基于态势感知的 SWIM 服务主动移交模型，特点是利用多维威胁指数联合分析安全态势触发服务移交机制，能够最大程度降低突发事件对 SWIM 用户造成的损失，保证了 SWIM 业务的连续性和服务的可靠性，能够在 SWIM 网络发生突发事件的情况下，执行有效的应急响应机制，本文暂未考虑 SWIM 网络大面积受损和融合数据服务受损的情况，未来将在该方面做进一步研究。

参考文献：

[1] DELOSIERES L, NADJMTEHRANI S. Batman Store and Forward: The Best of the Two Worlds [C]//IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE Press, 2012: 721-727.

[2] DARIO D C, ANTONIO S, GEORG T. SWIM- a next generation ATM information bus-the SWIM-SUIT prototype [C]//14th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW). IEEE Press, 2010: 41- 46.

[3] 吴志军，赵婷，雷璟. 广域信息管理 SWIM 信息安全技术标准的研究[J]. 信息网络安全, 2014 (1): 1-4.
WU Z J, ZHAO T, LEI J. Research on SWIM security technology standards [J]. Netinfo Security, 2014(1):1-4.

[4] 齐鸣，邢文钊. 民航广域信息管理系统数据安全威胁与风险分析方案设计[C]//第十九届全国青年通信学术年会论文集. 北京: 国防工业出版社, 2014: 12-18.

QI M, XING W Z. Scheme design for data security threats and risk analysis of civil aviation system wide information management [C]// Proceedings of the 19th National Youth Communication Academic Conference. Beijing: National Defence Industry Press, 2014: 12-18.

[5] LU X D, KOGA T. Real-time oriented system wide information management for service assurance [C]// 2015 IEEE Twelfth International Symposium on Autonomous Decentralized Systems. IEEE Press, 2015: 175-180.

[6] MOHAMMAD M, CARLOS A, CASTRO P, et al. Information security in the aircraft access to system wide information management infrastructure [C]//2016 Integrated Communications Navigation and Surveillance (ICNS). IEEE Press, 2016: 1-7.

[7] WILAON I, YANG S. Security for system wide information management [C]//2017 Integrated Communications, Navigation and Surveillance Conference (ICNS). IEEE Press, 2017: 1-13.

[8] 黄遵国, 卢锡城, 胡华平. 生存能力技术及其实现案例研究[J]. 通信学报, 2004, 25(7): 137- 145.
HUANG Z G, LU X C, HU H P. The survivability technique and its implementation case study [J]. Journal on Communications, 2004, 25(7): 137-145.

[9] 洪小亮, 郭义喜. 服务漂移机制的研究[J]. 信息工程大学学报, 2008, 9(1): 105-109.
HONG X L, GUO Y X. Research on the mechanism of service migration [J]. Journal of Information Engineering University, 2008, 9(1): 105-109.

[10] 赵二虎, 阳小龙, 彭云峰, 等. CPSM：一种增强 IP 网络生存性的客户端主动服务漂移模型[J]. 电子学报, 2010, 38(9): 2134-2139.
ZHAO E H, YANG X L, PENG Y F, et al. CPSM: client-side proactive service migration model for enhancing IP network survivability [J]. ACTA ELECTRONICA SINICA, 2010, 38(9): 2134-2139.

[11] 陈天平, 孟相如, 崔文岩, 等. 基于网络可生存性态势感知的主动服务漂移模型[J]. 空军工程大学学报: 自然科学版, 2015, 16(6): 64-68.
CHEN T P, MENG X R, CUI W Y, et al. A proactive service migration model based on network survivability situation awareness[J]. Journal of Air Force Engineering University: Natural Science Edition, 2015, 16(6):64-68.

[12] MAO Y C, XU Z Y, WANG L B, et al. An optimal Web services migration framework in the cloud computing[C]//2015 8th International Conference on Intelligent Computation Technology and Automation (ICICTA). IEEE Press, 2015, 153 – 156.

[13] TIM B. Intrusion detection systems and multi sensor data fusion: creating cyberspace situational awareness[J]. Communications of the ACM, 2000, 43(4): 99-105.

[14] 刘磊. 面向服务的网络安全态势评估系统的设计与实现[D]. 哈尔滨: 哈尔滨工程大学, 2010: 14-36.
LIU L. Design and implementation on service-oriented network security situation assessment[D]. Harbin:Harbin Engineering University, 2010:14-36.

[15] 谢丽霞, 王亚超, 于巾博. 基于神经网络的网络安全态势感知[J]. 清华大学学报(自然科学板块), 2013, 53(12): 1750-1759.
XIE L X, WANG Y C, YU J B. Network security situation awareness based on neural networks[J]. Tsinghua Univ (Sci & Technol), 2013, 53(12): 1750-1759.

[16] 韦勇, 连一峰, 冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2009, 46(3):353-362.
WEI Y, LIAN Y F, FENG D G. A network security situation awareness model based on information fusion[J]. Journal of Computer Research and Development, 2009, 46(3):353-362.

[17] HARKNESS D, TAYLOR M S. An architecture for system-wide information management [C]//25th Digital Avionics Systems Conference. IEEE Press, 2006: 1-13.

[18] GARY L, SCOTT L, JON D. Service oriented architecture for the next generation air transportation system[C]// 2007 Integrated Communications, Navigation and Surveillance Conference. IEEE , 2007: 1-9.

[19] 周顺. 面向 Web Service 的动态负载均衡设计与实现[J]. 计算机工程与科学, 2010, 32(12): 152-156.
ZHOU S. Web services-oriented design and implementation of dynamic load balancing[J]. Computer Engineering & Science, 2010, 32(12): 152-156.

[20] PONTUS J, ROBERT L, MATHIAS E. Can the common vulnerability scoring system be trusted? a bayesian analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(6): 1002-1015.

[21] 周志华. 机器学习[M]. 北京: 清华大学出版社, 2016: 179-185.
ZHOU Z H. Machine learning[M]. Beijing: Tsinghua University Press, 2016:179-185.

[22] TONG H X, ZHANG S S. A fuzzy multi-attribute decision making algorithm for web services selection based on QoS[C]// Proceedings of the 2006 IEEE Asia-Pacific Conference on Services Computing. IEEE Press, 2006:51-57.

[23] 周雅琴. 航班信息交换模型 FIXM 研究 I[J]. 中国民用航空, 2013(11): 80-81.
ZHOU Y Q. Research on flight information exchange model[J]. China Civil Aviation, 2013(11): 80-81..

[24] MARY E M, EDUARDO C M, OVID S. Addressing AIXM and IWXXM international challenges [C]// 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC). IEEE/AIAA, 2016: 25-29.

[25] KIRATIPONG O, HIDEORI N, TADASHI K. QoS Implementation in system wide information management (SWIM) Network Model [C]// 2015 IEEE Twelfth International Symposium on Autonomous Decentralized Systems.IEEE, 2015: 25-27.

[作者简介]

吴志军（1965− ），男，河南固始人，博士，中国民航大学教授、博士生导师，主要研究方向为网络空间安全、大数据信息安全和云计算安全等。

周胜琰（1994− ），男，山东临沂人，中国民航大学硕士生，主要研究方向为信息安全等。

雷缙（1982− ），女，四川自贡人，中国民航大学讲师，主要研究方向为信息安全等。