基于网络可生存性态势感知的主动服务漂移模型

陈天平[1]， 孟相如[1]， 崔文岩[1]， 许 媛[2]
(1.空军工程大学信息与导航学院,西安,710077;2.中电集团第39研究所,西安,710065)

摘要 针对现有服务漂移策略存在的不足,提出了一种基于网络可生存性态势感知的服务主动漂移模型。首先采用入侵检测和故障监测等技术手段实时获取网络生存态势信息,在此基础上设计了一种基于态势感知的服务漂移触发机制;然后引入主-从服务器的新概念,在此基础上建立了定向与随机相结合的服务漂移模式,并对该模型的相关算法进行了研究;最后对比分析了文中所提模型的性能。结果表明:该漂移模型既能提高服务漂移的抗毁能力,又大大缩减了漂移过程中带来的服务间断时间,能有效保证突发异常情况下的服务连续、可靠运行。

关键词 网络可生存性;服务漂移;态势感知;主-从服务器
DOI 10.3969/j.issn.1009-3516.2015.06.014
中图分类号 TP309.1 **文献标志码** A **文章编号** 1009-3516(2015)06-0064-05

A Proactive Service Migration Model Based on Network Survivability Situation Awareness

CHEN Tianping[1], MENG Xiangru[1], CUI Wenyan[1], XU Yuan[2]
(1. Information and Navigation College, Air Force Engineering University, Xi'an 710077, China;
2.CETC, NO.39 Research Institute, Xi'an 710065, China)

Abstract: Aimed at the shortages of existing service migration strategies, a proactive service migration model based on network survivability situation awareness is proposed. First, network survivability situation awareness is evaluated by using intrusion detection and failure detection timely, and under these circumstances, a service migration trigger mechanism based on network survivability situation awareness is designed. Then, a new concept "mainly-secondary server" is proposed, and service migration model is found combining directional and random ways, and correlative algorithm is researched. The results show that this service migration model improves not only survivability, but also reduces service break off time largely. And at the same time, this model is the guarantee of continuous and trusty run of service under conditions that something unexpected happens suddenly.

Key words: network survivability; service migration; situation awareness; M-S server

网络可生存性研究是网络安全技术的延续和发 展,主要侧重于研究系统在各种异常突发情况下完

收稿日期:2015-06-22
基金项目:国家自然科学基金资助项目(61201209;614014990)
作者简介:陈天平(1979—),男,四川雅安人,博士生,主要从事信息网络可生存性研究.E-mail:chentianping1979@163.com

引用格式:*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 Tianping, MENG Xiangru, CUI Wenyan, 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.*

成其关键任务的能力，其研究方向有：路由自愈[2-4]、服务漂移[6-15]等，是当前网络安全领域的一个研究热点。

服务漂移技术具有实现简单、抗毁能力强等特点，实现策略较多，传统方法如 DNS 动态解析、HTTP 报文重定向[4]等，虽然实现简单，但其前端调度器可能成为黑客入侵的跳板，安全隐患较大；云平台条件下的服务漂移方法[5-7]较新颖，但它们并不适用于传统 IP 网；黄遵国等[8-12]提出了一种随机漂移方法，但存在 2 点不足：①攻击者可能在较长的‘0’游程期间发起时间漏隙攻击；②漂移触发机制缺乏可控性，一旦漂移频率过快，易造成网络震荡；洪小亮等[10]解决了时间漏隙攻击，并采用 TOKEN 模型来设计服务器竞争机制，但相比于自由竞争机制，该机制降低了目标节点的选取随机性；赵二虎等[11-12]提出了一种新的服务漂移模型，该模型增强了服务抗毁度，减小了服务间断时间，但仍存在 2 点不足：①触发机制设计不合理，容易造成触发时间冲突；②当前服务器明文发送敏感数据给 Client，易导致信息泄漏。此外，以上文献均未考虑到目标节点的差异性对外部攻击行为的遏制效果。

1　问题描述

服务漂移主要针对图 1 中的 IP 端到端服务。图中，服务器集群（Server Cluster）表示为 $SC=\{S_1,S_2,\cdots,S_n\}$，它们互为备份。在何种情况以及何种时机解发服务漂移是一个重要问题，为此本文提出一种科学的漂移解发机制；漂移触发后，会涉及如何选取目标节点的问题，文中考虑到目标节点的多样性，建立一种高效的服务漂移模式；最后，针对现有方法所需时耗较大的问题，对漂移模型进行改进，在确保服务连续性前提下大大降低漂移时耗。

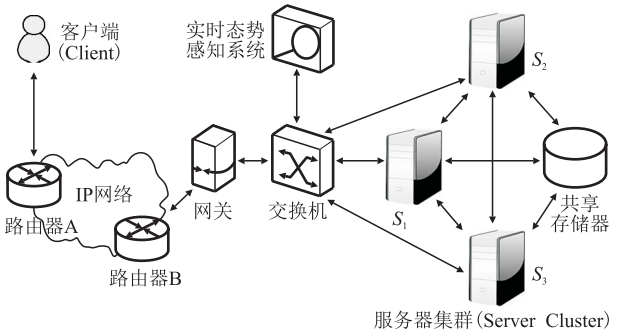

图 1　服务漂移所依据的 IP 网络拓扑结构

Fig.1　IP networktopology that service migration depends on

2　服务漂移模型设计与算法实现

为了确保模型描述的严谨性，先做以下假设：①集群内服务器具有多样性，即体系结构各异，而提供服务的功能相同或相似，且互为备份；②暂不考虑入侵检测和故障监测系统的漏报、误报等问题。

2.1　设计服务漂移触发机制

该模型从遭受外部攻击、网络故障和正常状态 3 个方面来考虑服务漂移触发问题，建立基于网络可生存性态势感知的服务漂移触发机制见图 2。

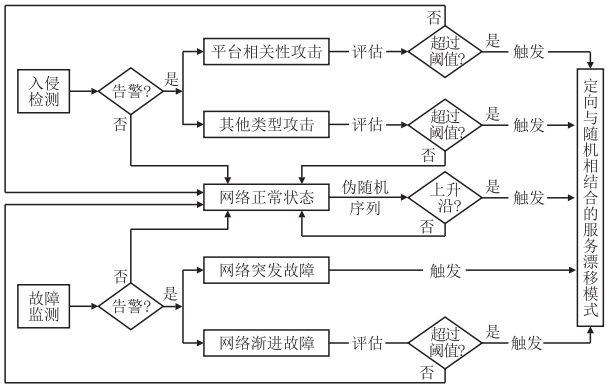

图 2　基于网络可生存性态势感知的服务漂移触发机制

Fig 2　Service migration trigger mechanism based on network survivability situation awareness

将外部攻击分为平台相关性攻击和其他类攻击。平台相关性攻击是指攻击实施效果与目标平台环境（如操作系统、服务软件、端口开放、漏洞等）密切相关的攻击类型，如病毒、木马、缓冲区溢出等；而 DDoS、暴力破解、会话劫持等与目标平台环境相关性小，故为其他类型攻击。当 NIDS 产生告警时，首先判明攻击类型，评价其威胁程度，然后与预定阈值进行比较，一旦超过阈值，就依据攻击类别触发相应的服务漂移模式，否则认为网络处于正常状态。

将网络故障分为突发和渐进 2 类。突发故障是指持续时间短且难以提前预测的故障类型，如服务器遭敌火力毁伤等；渐进故障是指持续时间长且故障状态可监控的故障类型，如服务器健康状态、网络拥塞等。当发生渐进故障时，需对网络健康指数进行评估，一旦超过阈值，就触发服务漂移；当突发网络故障时，直接触发服务漂移。

网络正常状态下，在集群内构建一种伪随机序列触发机制，实现服务主动随机漂移，具体实现过程见文献[12]。此外考虑到 2 次漂移间隔时间过小可能会影响集群的网络稳定性，因此，伪随机序列的启时刻 T_S 应满足：

$$|T_S-T_M|\geqslant\delta_{\min} \tag{1}$$

式中：T_M 表示最近一次服务漂移时刻；$\delta_{\min}$ 表示 2 次服务漂移允许的最小间隔时间。

2.2 定向漂移与随机漂移的对比分析

考虑到现有服务漂移策略采用的随机漂移模式不适用于遏制平台相关性攻击。对此，提出一种考虑节点多样化距离的定向漂移模式，当平台相关性攻击的威胁程度超过阈值时，将服务迁移至与当前服务器多样化距离最大的目标节点，达到有效遏制攻击的目的。

为了比较随机漂移和定向漂移对平台相关性攻击的遏制效果，假设如下服务漂移场景：当前服务器 S_1 遭受蠕虫病毒攻击，其威胁程度持续升高并超过预设阈值，服务漂移被触发，此时考虑 2 种不同的节点选取方法：① 随机漂移，从备份服务器中随机选取一个目标节点，且假定所选节点 S_2、S_3 和 S_4 与当前服务器 S_1 相同或相似；② 定向漂移，将服务漂移至与 S_1 的多样化距离最大的节点 S_5，以上 2 种不同漂移模式对蠕虫的遏制效果对比见图 3。

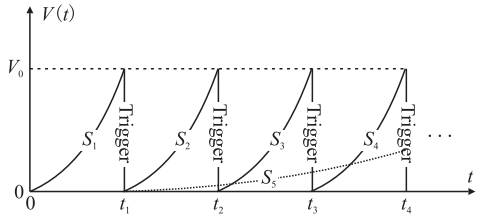

图 3 蠕虫病毒遏制效果对比示意图

Fig.3 Contrast results ofrestraining effect of worm

图 3 中横轴表示时间，纵轴表示对蠕虫威胁程度的实时评价值，V_0 表示威胁程度阈值，$t_1 \sim t_4$ 时段内：实线表示随机漂移模式下蠕虫感染情况，虚线表示定向漂移模式下蠕虫感染情况。由图 3 可知，随机漂移模式下，因为目标平台网络环境相同或相似，蠕虫感染所依赖的条件仍然具备，所以新的目标节点很快又会被感染，造成服务漂移频发；定向漂移模式下，新的目标节点 S_5 相比 S_1 具有较大差异性，蠕虫感染所依赖的条件被彻底破坏，因此蠕虫感染速度明显减慢。

由以上分析可知，定向漂移对平台相关性攻击遏制效果更为明显，但目标节点的选取随机性降低；而随机漂移的节点选取随机性高，目标隐蔽性强。为了使 2 种漂移模式二者优势互补，文中建立定向漂移与随机漂移相结合的服务漂移模式。

2.3 服务漂移模型的相关算法实现

下面先给出 2 个相关定义：多样化距离是指节点间差异化程度的度量。主-从服务器：是指集群内处于前、后台同步运行的 2 台服务器，同时接受 Client 的服务请求，并更新服务状态信息，但只有主服务器对外提供服务，而从服务器保持高度隐蔽。

2.3.1 集群内节点多样化距离量化算法

服务器节点间的多样化距离(D)可通过比较两者在“操作系统(O)”、“网络协议(P)”、“服务提供软件(S)”和“防御措施(F)”这 4 个指标方面的差异来量化。这 4 个指标的分级量化标准见表 1。

表 1 指标分级量化标准表

Tab 1. Classification quantitative standard table of index

指标	大 量化值:0.9	中 量化值:0.5	小 量化值:0.1
O	操作系统类型不同，如 Windows 和 UNIX	操作系统类型相同，但版本不同，且漏洞重合少	操作系统版本相同，且漏洞重合也较多
P	协议类型不同，如 IPX 和 IPv6	协议类型相同，但版本不同	协议版本相同，且漏洞相似
S	服务提供软件类型不同，且开放端口不同	软件类型相同，但版本不同，且配置策略差异大	服务提供软件相同，且服务配置策略较为相似
F	防御手段不同，如防病毒软件：瑞星和卡巴斯基	防御措施实现手段相同，但配置策略差异明显	防御措施相同，且配置策略类似

将服务器 S_i 和 S_j 之间的多样化距离表示为 $D(i,j)$，则：

$$D(i,j) = D(j,i) = \alpha O(i,j) + \beta P(i,j) + \lambda S(i,j) + \mu F(i,j) \tag{3}$$

式中：α、β、λ 和 μ 为权重系数，其取值由专家根据经验给定，并且满足：$\alpha+\beta+\lambda+\mu=1$，$O(i,j)$、$P(i,j)$、$S(i,j)$ 和 $F(i,j)$ 为表 1 中各指标等级量化值。

假定集群内共有服务器 n 台，那么可以计算得到 C_n^2 组多样化距离数据，将这些数据进行加密后保存于共享存储器上。在集群内，节点间的多样化距离是相对固定的，只有当重配置或更换服务器时，才会重新计算一次，因此只需简单调用，而无需实时计算这些数据，从而大大节省时间。

2.3.2 考虑节点多样化距离的定向漂移算法

为了更好地遏制平台相关性攻击，本文提出一种考虑节点多样化距离的定向漂移算法，其算法实现过程主要包括 4 个步骤：

Step1 主、从服务器确定。以当前服务器作为主服务器，负责对外提供服务；主服务器选取集群内多样化距离最大的备份服务器作为从服务器，从服务器运行于后台，接受 Client 服务请求，更新服务状态信息，但不予响应。

Step2 实时监测网络可生存性状态。采用入侵检测、故障监测等技术手段来获取网络可生存性态势信息，并对平台相关性攻击的威胁程度进行量

化评估。

Step3　启动触发机制。当平台相关性攻击的威胁程度超过预设阈值时，立即触发定向漂移模式，否则，继续监测网络状态信息。

Step4　主-从协同交接。漂移触发后，从服务器快速切换至前台运行，并与 Client 建立连接，对 Client 服务请求作出响应；主服务器待从服务器全部接管任务后，自动转换为后台运行，并做好隐蔽。

该漂移算法通过主-从服务器协同交接，最大程度地更新了服务端平台环境，实现了对平台相关性攻击的有效阻断，大大提高了服务漂移的抗毁能力，实现了服务无缝漂移。

2.3.3　定向与随机相结合的漂移算法

除遏制平台相关性攻击使用定向漂移以外，其余情况下触发服务漂移时，文中均采用定向与随机相结合的服务漂移算法，其算法实现过程主要包括以下步骤：

Step1　主、从服务器确定。主服务器确立同上，从服务器选取负载较低者。

Step2　实时监测、评估网络可生存性状态。

Step3　启动触发机制。触发条件包括：①非平台相关性攻击的威胁程度超过阈值；②网络渐进故障导致网络状态健康指数超过阈值；③突发网络故障；④网络正常状态下，伪随机序列出现“上升沿”。

Step4　定向与随机相结合的漂移模式。漂移触发后，首先通过主-从交接方式来实现服务的定向漂移，即从服务器全面接管主服务器对外提供服务；然后在集群内采用布朗运动机制随机选取 1 个备份服务器作为新的主服务器；最后，从服务器再与新的主服务器进行任务交接。

在该漂移过程中，从服务器选取负载较小的备份服务器，有利于在突发异常情况下保持集群内的负载均衡；同时，从服务器充当了“服务摆渡”的功能，保证了主服务器平稳、快速地实现随机漂移，大幅度缩减了服务漂移过程带来的服务间断时间。

3　性能对比分析

文中所提服务漂移模型除了在遏制平台相关性攻击方面具有明显优势外，这里还将文中所提服务漂移模型与文献[8]中的 SASS 模型、文献[10]中的 TOKEN 模型以及文献[12]中的 ISM 模型进行对比分析。

3.1　漂移随机性对比分析

服务抗毁能力 R_S 的计算引用文献[12]中的定义，即：

$$R_S=-\sum_{i=1}^{n}P_i\ln(P_i),n\geqslant 2 \tag{4}$$

式中：n 为集群内的服务器台数；P_i 为服务漂移至第 i 台备份服务器的概率；R_S 值越大说明服务漂移的随机性越高，即服务的抗毁能力也越大。

当服务漂移触发后，SASS 模型从 $n-1$ 台备份服务器中选取 1 个作为新主服务器，假如各备份服务器竞争成为主服务器的概率相等，由式(4)可得出 SASS 模型的 R_S 为：

$$R_S=-\left(\frac{1}{2}\ln\left(\frac{1}{2}\right)+(n-1)\frac{1}{2(n-1)}\ln\left(\frac{1}{2(n-1)}\right)\right) \tag{5}$$

当服务漂移触发后，TOKEN 模型将从 $n-1$ 台备份服务器中选择负载最低计算者作为新的主服务器 R_S，计算为：

$$R_S=-\left(\frac{1}{2}\ln\left(\frac{1}{2}\right)+n_0\frac{1}{2n_0}\ln\left(\frac{1}{2n_0}\right)\right) \tag{6}$$

式中：n_0 表示集群内负载最低的服务器台数，且 $1\leqslant n_0\leqslant n-1$。

在本文所提定向与随机相结合的服务漂移模式中，网络正常状态下，采用伪随机序列的上升沿(即输出‘01’时)作为触发信号，而序列输出‘00’、‘10’或‘11’时，并不会触发服务漂移，仍由当前服务器继续提供服务；此外，采用布朗运动机制从 $n-1$ 台备份服务器中随机选择一台作为新的主服务器，根据布朗运动的性质可知，每台备份服务器被选中的概率相等，因此可得相应的 R_S 为：

$$R_S=-\left(\frac{1}{4}\ln\left(\frac{1}{4}\right)+(n-1)\frac{3}{4(n-1)}\ln\left(\frac{3}{4(n-1)}\right)\right) \tag{7}$$

采用 matlab 对式(5)、(6)和(7)进行仿真分析，可得这 3 种模型的服务漂移随机性对比见图 4。

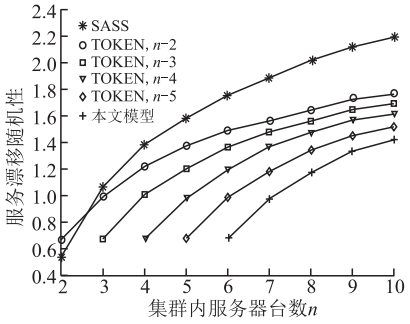

图 4　3 种模型服务漂移随机性对比图

Fig.4　Contrast results of service migration randomicity of 3 models

通过图 4 进行比较可以看出，文中所提模型、SASS 模型和 TOKEN 模型的服务漂移随机性均随着集群内服务器台数 n 的增加而增大；TOKEN 模型的漂移随机性随着 n 的减少而减小；在集群内服务器数量 $n\geqslant 3$ 的情况下，本文所提模型比 SASS

模型和 TOKEN 模型的服务漂移随机性更大,因此表明文中所提模型具有更强的服务抗毁能力。

3.2 漂移时间对比分析

一般情况下,服务漂移时间由 3 部分构成:目标节点时间(T_{os})、送当前服务状态信息的时间(T_{sm})、以及备用服务器与 Client 建立连接的时间(T_{ec})。SASS 模型与 TOKEN 模型和 ISM 模型所需漂移时间的对比分析见文献[15]。文中所提定向漂移模型采用主-从服务器协同交接的方法,不需选取目标节点,节约了目标节点选取时间 T_{os},另外主、从服务器同时接受 Client 服务请求,并同步更新服务状态信息,从而节约了主服务器向从服务器发送当前服务状态信息的时间 T_{sm},因此,本文所提定向漂移模型执行一次服务漂移所需的时间可以表示为 T_{ec},以上 4 种模型的单次服务漂移时间对比见图 5。

由图 5 可知,文中所提模型的单次服务漂移时间明显小于 SASS、TOKEN 和 ISM 模型。

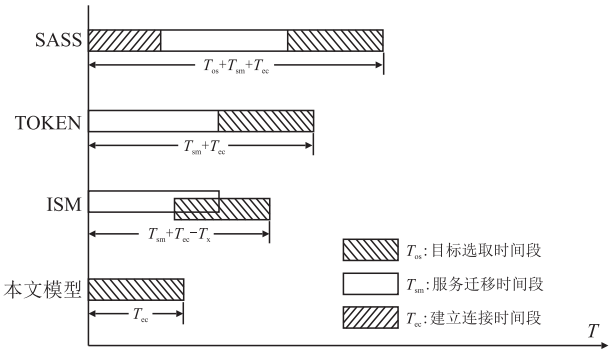

图 5 4 种模型的单次服务漂移时间对比图

Fig.5 Contrast results of service migration time of 4 models onetime

4 结语

针对现有服务漂移策略存在的不足,文中提出了一种基于网络可生存性态势感知的服务主动漂移模型。并对文中所提模型与 SASS、TOKEN 和 ISM 模型进行了性能对比分析。对比分析结果表明,文中所提服务漂移模型具有一定优势:既能提高服务漂移的抗毁能力,又大大缩减了服务漂移过程中带来的服务间断时间,有效保证了突发异常情况下的服务连续、可靠运行。

参考文献(References):

[1] 伍文,孟相如,马志强,等. 基于组合赋权的网络可生存性模糊综合评估[J]. 系统工程与电子技术,2013,35(4):786-790.
WU Wen, MENG Xiangru, MA Zhiqiang, et al. Fuzzy Comprehensive Evaluation of Network Survivability Based on Combinational Weight [J]. Systems Engineering and Electronics, 2013, 35(4): 786-790.(in Chinese)

[2] Su H K. A Local Fast-Reroute Mechanism for Single Node or Link Protection in Hop-by-Hop Routed Networks[J]. Computer Communications, 2012, 35(8): 970-979.

[3] Cho S, Elhourani T, Ramasubramanian S. Lndependent Directed Acyclic Graphs for Resilient Multipath Routing[J]. IEEE/ACM Transactions on Networking. 2012, 20(1): 153-162.

[4] M Mohanned Kazzaz, Marek Rychly. A Web Service Migration Framework [C]//The Eighth International Conference on Internet and Web Applications and Services.2013: 58-62.

[5] Christoph Fehling, Frank Leymann, Stefan T, et al. Service Migration Patterns - Decision Support and Best Practices for the Migration of Existing Service-based Applications to Cloud Environments [J]. Institute of Architecture of Application Systems, 2013, 33 (4): 17-24.

[6] Mao Yingchi, Wang Jiulong, Zhu Lili, et al. Optimization Service Migration Scheme for Load Balance in Cloud Computing [C]//International Conference on Computer Science and Service System.2014: 634-637.

[7] Shiqiang Wang, Rahul Urgaon kar, Ting He, et al. Mobility-Induced Service Migration in Mobile Micro-Clouds [J]. Journal on Communications, 2011, 32(8): 150-158.

[8] 黄遵国,卢锡城. 随机自治可生存调度算法研究 [J]. 计算机工程与科学, 2005, 27 (3): 1-3.
HUANG Zunguo, LU Xicheng. On the Algorithm for Stochastic Autonomous Scheduling Survivability [J]. Computer Engineering & Science, 2005, 27 (3): 1-3.(in Chinese)

[9] 陈建莉. 基于未确知数学的网络安全风险评估模型[J]. 空军工程大学学报:自然科学版, 2014, 15(2): 91-94.
CHEN Jianli. A Network Security Risk Assessment Model Based on Unascertained Mathematics [J]. Journal of Air Force Engineering University: Natural Science Edition, 2014, 15(2): 91-94.(in Chinese)

[10] 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 Xiaoliang, GUO Yixi. Research on the Mechanism of Service Migration [J]. Journal of Information Engineering University, 2008, 9 (1): 105-109. (in Chinese)

[11] 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 Erhu, YANG Xiaolong, PENG Yunfeng, et al. CPSM: Client-Side Proactive Service Migration Model for Enhancing IP Network Survivability [J]. Acta Electronica Sinica, 2010, 38 (9): 2134-2139.(in Chinese)

[12] 赵二虎,阳小龙,徐杰,等. ISM:漂移意图可感知的 IP 网络生存性服务提供模型 [J]. 电子学报, 2011, 39 (12): 2768-2775.
ZHAO Erhu, YANG Xiaolong, XU Jie, et al. ISM: Intent-Perceptible Service Migration Model for IP Network Survivability [J]. Acta Electronica Sinica, 2011, 39 (12): 2768-2775.(in Chinese)

(编辑:徐楠楠)