

基于博弈的异构控制器云安全策略研究

胡军台, 武振宇, 付晓, 王逸超

(国网河南省电力公司平顶山供电公司, 河南 平顶山 450052)

摘要: 在软件定义数据中心网络的控制层采用多个异构控制器是提升其安全的一种有效方式。针对网络不同安全需求下控制器的部署策略问题, 提出了一种博弈模型。具体地, 首先, 利用博弈论知识刻画了攻防博弈模型, 求解纳什均衡, 进而指导设计安全策略; 其次, 在均衡基础上分析攻防策略行为对控制层安全状态的影响; 最后, 仿真结果表明提出的均衡策略的有效性, 并描述了攻防策略交互的动态性。

关键词: 软件定义数据中心网络; 控制器; 网络安全; 博弈

中图分类号: TP393.08

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018075

Game model based security strategy of heterogeneous controllers in the cloud

HU Juntai, WU Zhenyu, FU Xiao, WANG Yichao

State Grid Pingdingshan Power Supply Company, Pingdingshan 450052, China

Abstract: Deploying multiple heterogeneous controllers at the control level of a software-defined data center is an effective way to increase security. In view of the deployment strategy of controllers under different security requirements of the network, a game model was presented. Specifically, firstly, the game theory was used to depict the attack and defense game model and solve the Nash equilibrium, and then guided the design of security strategy. Secondly, the impact of the strategy of attack and defense on the security status of the control layer were analyzed. Finally, the simulation results show the effectiveness of the proposed equilibrium strategy, and describe the dynamic interaction strategy.

Key words: softwares defined data center network, controller, network security, game

1 引言

软件定义网络(SDN, software defined network)将控制与转发功能分离, 形成应用层、控制层、数据层, 通过可编程接口开放网络, 促进了网络创新, 其灵活的网络管理以及快速的网络功能部署等特点满足了云数据中心流量控制、自动化网络配置等诸多传统方式下无法解决的网络需求^[1-2]。但与此同时, SDN 网络架构也带来了

新的安全威胁^[3], 尤其控制器作为核心组件, 极易成为攻击者的攻击目标, 一旦控制器被攻击, 将导致其所管控整个网络的信息泄露, 甚至瘫痪。

目前, 控制层的控制器相对静态, 便于攻击者探测分析, 进而发起攻击。单控制器结构极易造成单点失效, 一旦攻击者掌握控制器的漏洞, 通过开放的南北接口实施攻击, 将会造成整个网络瘫痪。目前业界主流的分布式控制器, 如 Onix^[4]以及开源控制器 ONOS^[5]和 ODL^[6], 虽然能够有

收稿日期: 2018-07-15; 修回日期: 2018-08-20

通信作者: 胡军台, hujuntai@163.com

效地解决单点失效问题，但是其在这些分布式结构中，控制器实例是同构的且具有共同的脆弱点，无法应对共模失效安全威胁^[7]。因此，为了应对攻击者的探测以及共模脆弱点问题，业界研究者开始在控制层部署异构冗余的控制器以此增强控制器的安全性与可靠性。

文献[8-9]基于拜占庭容错机制设计实现了抵御面向 SDN 控制器攻击，且具有一定容错能力的控制器系统，在该系统中，交换机不再只受单个控制器控制，而是由多个控制器共同决定交换机中流表的更新。基于拜占庭的更新机制能够保证即使一定数量的受损控制器下发了错误指令，其最终下发到交换机上的流表依然是正确的。然而，这种方法一旦一个控制器被攻击成功，有可能造成攻击感染。文献[10]基于网络空间拟态防御思想，设计开发了一款 MNOS 的网络操作系统架构，通过流一致裁决机制很好地应对了 SDN 典型的流规则篡改攻击，提升了控制层的抗攻击性能。文献[11]提出一种融入动态、异构和冗余性的拟态网络操作系统来消除相关攻击的威胁，此防御架构能够融合现有的单个控制器防御技术，同时能通过多异构网络操作系统之间的协同合作降低同一漏洞后门被攻击者反复有效利用的可能性。考虑网络场景约束条件，文献[12]提出了一种基于负反馈的动态感知调度方法来刻画控制器执行体的切换方式，依据获得的动态策略能较好地根据当前网络环境和网络全局信息来优化运行控制

器组合，从而维持控制层工作在安全性高和失效概率低的模式下。该论文在之前的研究^[13]中提出了一种安全控制层，通过动态地变换控制器进而抵御针对控制器未知安全漏洞等安全威胁。

然而，上述研究者主要针对冗余异构下的控制器调度策略展开研究，缺乏针对不同需求部署相应的控制器数量以及改变攻防行为后的安全性动态变化的相关研究。为此，本文以云网络为背景，提出一种基于博弈的多样化安全策略机制，分析指导网络管理者充分利用异构的控制器以提高网络的安全性。本文主要贡献如下：首先，提出了面向 SDDC 的攻防博弈模型，描述了攻防双方的利益冲突；其次，在上述博弈模型的基础上，计算并分析了两人博弈、三人博弈以及 $N+1$ 博弈等情况下的均衡策略，并分析了相关均衡策略对动态异构控制器架构的安全性；最后，对上述场景进行仿真分析，验证了本文博弈模型的有效性。

2 网络框架

云数据中心对网络提出了灵活、按需、动态和隔离的需求，SDN 的集中控制、控制与转发分离、应用可编程 3 个特点天然地匹配以上需求，软件定义数据中心（SDDC，softwares defined data center）应运而生。用户可通过传统网络接入 SDDC，网络架构如图 1 所示。

混合网络中包含若干传统网络与若干 SDDC，

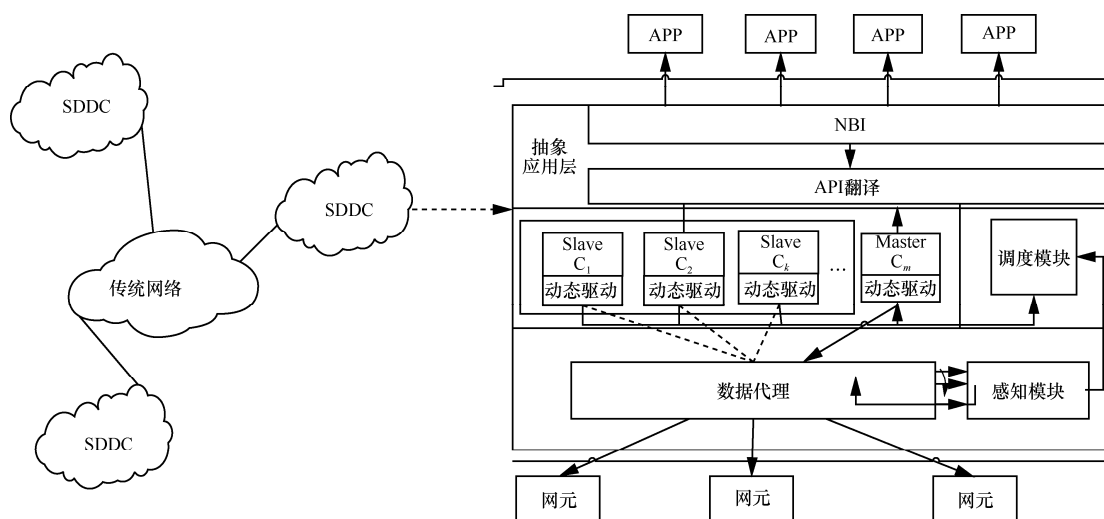


图 1 SDDC 网络架构

其中, 传统网络与现有的保持一致。为了保护 SDDC 中的控制层, 在控制层中部署多个控制器执行体以及一些功能模块^[13]。OpenFlow1.3 支持单台 OpenFlow 交换机同时与多个控制器建立连接, 并选择一个 Master 管理网络^[14], 以避免某个控制器失效导致相关交换机无法正常工作。在 SDDC 中, 调度器动态地依据策略从多个控制器执行体选择一个管理网络, 限制了控制器脆弱性的暴露, 增加了攻击者的攻击成本, 降低了被攻击机会。

本文在文献[13]控制器架构基础上, 从如何利用潜在的异构控制器角度出发, 结合博弈论知识^[15], 提出了一种基于博弈的异构控制器部署策略。

3 威胁模型

假设网络中包括多个 SDDC, 且面临某攻击者的威胁。表 1 为本节的关键符号说明。

表 1	关键符号描述
符号	含义
c_s^D	防御者 (SDDC) D 切换控制器产生的代价
c_f^D	防御者 D 失败的网络损失
c_s^A	改变攻击模式给 A 带来的代价
B^A	A 成功攻击的收益

防御者: 防御者选择一个控制器管理网络。防御者如果切换控制器, 将产生一个代价 c_s^D , 若控制器被攻击成功, 网络服务将面临失败, 网络损失为 c_f^D 。

攻击者: 攻击者探测分析控制层部署的控制器脆弱点, 并发起攻击, 一种攻击模式针对一个控制器。对于攻击者来讲, 如果攻击成功, 攻击者获得收益 B^A 。同样地, 若攻击者改变攻击模式, 则在下一个攻击前攻击者需要重新探测分析, 进而优化针对新控制器的攻击模式, 这为攻击者招致一个代价 c_s^A 。

困境: 为了保证网络的正常运行, 攻击者攻击成功后, 网络防御者面临着下一刻是否依然使用相同的控制器的困境。若考虑使用方便、低耗代价等因素, 则应该尽量不改变控制器。但与此同时, 网络却面临着同一种攻击再次攻击的风险。

如果防御者为了增加攻击者攻击成功的难度而选择切换一个新的控制器, 则势必也会增加操作困难和部署代价等。同样, 攻击者也面临类似的困境。因此, 攻防双方采取策略行为不仅依赖于自私考虑 (如代价、安全等), 也依赖于对手的策略选择。

4 博弈模型

4.1 博弈论概念

博弈是由规则主导, 并解决参与者利益冲突的方法。博弈的基本元素由参与者 N 、策略 S 和收益函数 P 组成, 博弈模型可记为 $G(N, S, P)$ 。参与者是能够在博弈中做出决策的实体, 有 n 方参与的博弈可称为 n 人博弈, 参与者集合为 $N = \{1, 2, \dots, n\}$ 。策略可分为纯策略和混合策略。策略是一种规则, 指导参与者在其信息集内采取的行动。在 n 人博弈中, $s_i \in S_i$ 表示第 i 位参与者的特定策略, S_i 则表示第 i 位参与者所有可选择的策略集合。混合策略是一种详尽的策略计划, 知名参与者采用每个纯策略的概率, 其形式是一种概率分布。收益是指参与者在博弈过程中的期望报酬, 收益可通过收益函数 u 计算得到。

博弈完结后, 每位参与者采取了相应的策略并得到了收益, 而均衡则是一个由所有参与者的最优策略组成的组合, 即最优的策略组合。当所有参与者都采用这个策略组合中属于其的策略时, 没有任何一位参与者能够通过独自采用其他策略而获得更多。对于 n 人博弈 $G(S_1, S_2, \dots, S_n; u_1, u_2, \dots, u_n)$, 策略组合 $s^* = (s_1^*, s_2^*, \dots, s_i^*, \dots, s_n^*)$ 是一个纳什均衡, 当且仅当对于所有参与者 $i \in N$, 在其他 $n-1$ 位参与者分别采用策略 $s_1^*, s_2^*, \dots, s_{i-1}^*, s_{i+1}^*, \dots, s_n^*$ 的情况下, 他的最优策略都是 $s_i^* \in S_i$, 也就是说, 其只有采取策略 s_i^* 才能获取最优收益, 可用公式表述如下。

$$\begin{aligned}
 & u_i(s_1^*, s_2^*, \dots, s_{i-1}^*, s_i^*, s_{i+1}^*, \dots, s_n^*) \\
 & \geq u_i(s_1^*, s_2^*, \dots, s_{i-1}^*, s_i', s_{i+1}^*, \dots, s_n^*), \\
 & \forall s_i' \in S_i, s_i' \neq s_i^*, \forall i \in N
 \end{aligned}$$

4.2 两人博弈

为了方便起见, 首先分析一个 SDDC 与一个攻击者的博弈, 网络包括防御者 D 、攻击者 A 以及 SDDC 中控制层控制器执行体的数量 M 。攻击

者与防御者的状态相互不确定，如果两者匹配，即攻击者的攻击模式是针对此时控制器漏洞的攻击，则攻击成功；否则，攻击不成功。假设攻击者在一个时间上已经成功发起了攻击，下一个时间上存在以下情形。

1) 防御者面临着困境：控制层应该保持此时的状态（此时希望攻击者下次攻击改变攻击模式）或者防御者切换控制器管理网络（此时期望攻击者不改变攻击模式）。

2) 攻击者也面临着相似的困境：攻击者应该以相同的模式发起攻击（认为防御者未切换控制器），或者攻击者切换攻击模式（认为防御者切换控制器，改变了状态）。

基于上述描述，本节研究了二人博弈的纳什均衡。博弈的参与者为攻击者 A 与防御者 D ，攻击者的目标是最小化防御者的收益，防御者恰恰相反。表 2 的收益矩阵刻画了博弈参与者的效用函数，并且阐明了优化目标。

表 2 一个防御者（SDDC）与一个攻击者的收益矩阵

防御者 \ 攻击者	切换	保持
切换	$(c_s^D + \frac{1}{M-1}c_f^D, \frac{1}{M-1}B^A - c_s^A)$	$(c_s^D, 0)$
保持	$(0, -c_s^A)$	(c_f^D, B^A)

4.2.1 纯策略方案

在这种情况下，纳什均衡解与 c_s^D 和 c_f^D 两者密切相关，为了研究纯策略方案，需要考虑 2 种情况。

1) 当 $c_s^D > c_f^D$ 时：从表 2 容易看出，这种情况下，唯一的纳什均衡策略组合是（保持，保持）。

2) 当 $c_s^D < c_f^D$ 时，考虑以下 2 种条件下的情况。

- ① 当 $\frac{B^A}{c_s^A} > \frac{1}{M-1}$ ，则没有纯策略纳什均衡。
- ② $\frac{B^A}{c_s^A} < \frac{1}{M-1}$ ，唯一的纯策略纳什均衡组

合为（ D 切换， A 保持不变），此均衡下，攻击者攻击模式保持不变，防御者选择切换控制器。

4.2.2 混合策略方案

为了寻找混合策略纳什均衡，令攻击者改变攻击模式的概率为 p_s^A ，则保持不变的概率即

$1 - p_s^A$ ，当 D 采取一个混合策略时，其需要在切换和保持不变这 2 个状态保持平衡。 $E[c_D^{\text{switch}}]$ 与 $E[c_D^{\text{stay}}]$ 分别代表 A 选择切换和保持不变情况下 D 的期望代价。依据表 2 的收益函数，计算得出

$$E[c_D^{\text{switch}}] = p_s^A \left(c_s^D + \frac{1}{M-1} c_f^D \right) + (1 - p_s^A) c_s^D \quad (1)$$

同样地

$$E[c_D^{\text{stay}}] = p_s^A \cdot 0 + (1 - p_s^A) c_f^D \quad (2)$$

如上所述，防御者在混合策略纳什均衡下， $E[c_D^{\text{switch}}]$ 与 $E[c_D^{\text{stay}}]$ 相等，求解可得

$$p_s^A = \frac{c_f^D - c_s^D}{c_f^D} \frac{M-1}{M} \quad (3)$$

类似地， D 切换的概率为 p_s^D （保持不变的概率是 $1 - p_s^D$ ）， $E[c_A^{\text{switch}}]$ 和 $E[c_A^{\text{stay}}]$ 分别代表 D 选择切换和保持不变时 A 的期望收益。依据表 2 的收益函数，计算得出

$$E[c_A^{\text{switch}}] = p_s^D \left(\frac{1}{M-1} B^A + c_s^A \right) + (1 - p_s^D)(-c_s^A) \quad (4)$$

同样地

$$E[c_A^{\text{stay}}] = p_s^D \cdot 0 + (1 - p_s^D) B^A \quad (5)$$

如上所述，攻击者在混合策略纳什均衡下， $E[c_A^{\text{switch}}]$ 和 $E[c_A^{\text{stay}}]$ 相等，求解得

$$p_s^D = \frac{B^A + c_s^A}{B^A} \frac{M-1}{M} \quad (6)$$

因此，基于以上分析，对博弈均衡给出定理 1。

定理 1 混合策略纳什均衡下，若网络（ D ）被攻击成功，下一刻应该以概率 $\frac{B^A + c_s^A}{B^A} \frac{M-1}{M}$ 选

择切换为另一个控制器。并且，攻击者在攻击成功之后，其选择改变攻击模式的概率为 $\frac{c_f^D - c_s^D}{c_f^D} \frac{M-1}{M}$ ，实施攻击下一刻的控制器执行体。

4.2.3 均衡的有效性

图 2 给出了攻击成功的概率与防御者策略的关系。防御者以 3 种策略切换控制器：① 保持不变；② 一直切换；③ 以均衡概率切换。

图中的每一种线条形分别对应系统不同的策略: ▨表示防御者保持不变, ■表示防御者总是切换, ▩表示防御者以纳什均衡概率切换。无论防御者采用何种策略, 攻击者均做出最优的回应, 攻击者做出最优的回应如表 2 所示。分析图 2, 显而易见, 当 D 保持不变时, 成功攻击的概率始终为 1, 这是因为攻击者此时最优的回应也是保持, 所以保持了一直攻击成功的状态; 当 D 总是变换时, 攻击成功的可能性降低, 因为虽然攻击者的最优回应也是切换, 但攻击者考虑执行何种模式进行攻击的这种不确定性对 D 是有利的。进一步地分析, 当 D 切换依照均衡策略时, 根据式(6), 攻击成功的概率最低, 此时, 攻击者最优的回应为以概率 p_s^A 改变攻击模式, 这表明了混合策略纳什均衡方法的有效性。而且, 随着 M 不断增加, 纳什均衡下 D 切换时攻击成功的概率接近于 D 总是切换的情况, 这是因为式(6)是 M 的减函数, 若 M 不断减少, 两者的概率开始逼近 1。

从图 2 也可以看出, 防御系统总是一直切换控制器并不是最好的, 而且会导致高昂的代价。图 2 也表明了混合策略解决方案的有效性, 为利用潜在的多样控制器设计最佳随机化技术提供理论基础。

4.3 三人 (2+1) 博弈

当网络中存在 2 个 SDDC, 研究 2 个合理且自私的 SDDC (SDDC1 和 SDDC2) 在一次攻击成功之后, 面临选择切换还是保持不变这种困境。

表 3 和表 4 列出了此次博弈下的收益矩阵。对于 SDDC $_i$, $i \in \{1, 2\}$ 采取混合策略时, 其需要在切换和保持不变 2 种状态之间保持平衡。表 3 和表 4 中, 由于 2 个 SDDC 下的收益矩阵是对称的, 故认为每一个 SDDC 选择切换控制器的概率均为 p_s^d 。定义 SDDC 的切换代价以及失败代价分别为 c_s^d 和 c_f^d , $E[c_i^{\text{switch}}]$ 以及 $E[c_i^{\text{stay}}]$ 分别代表 A 选择切换和保持不变时 i 的期望代价。依据表 3 和表 4 的收益函数。计算得

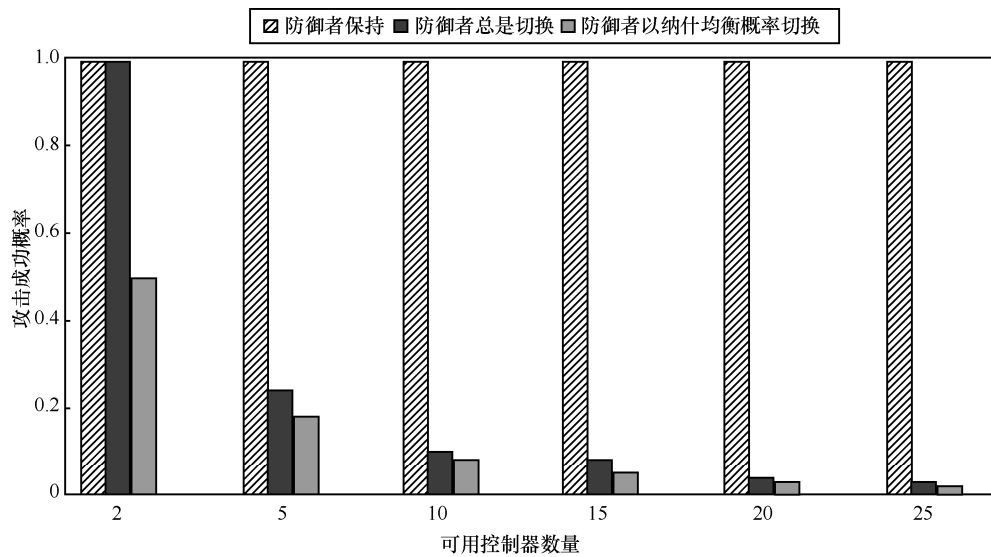


图 2 攻击成功的概率随防御者策略变化

表 3

2 个 SDDC (1 和 2) 与一个攻击者 (选择切换) 的收益矩阵

1 \ 2	2	
	切换	保持
1 切换	$(c_s^d + \frac{1}{M-1}c_f^d, c_s^d + \frac{1}{M-1}c_f^d, \frac{2(M-2)}{(M-1)^2}B^A + \frac{1}{(M-1)^2}B^A - c_s^A)$	$(c_s^d + \frac{1}{M-1}c_f^d, 0, \frac{1}{M-1}B^A - c_s^A)$
1 保持	$(0, c_s^d + \frac{1}{M-1}c_f^d, \frac{1}{M-1}B^A - c_s^A)$	$(0, 0, -c_s^A)$

表4 2个SDDC(1和2)与一个攻击者

		(选择切换)的收益矩阵	
1 \ 2		切换	保持
	切换	$(c_s^d, c_s^d, 0)$	(c_s^d, c_f^d, B^A)
	保持	(c_f^d, c_s^d, B^A)	(c_f^d, c_f^d, B^A)

$$E[c_i^{\text{switch}}] = p_s^A \left[p_s^d \left(c_s^d + \frac{1}{M-1} c_f^d \right) + (1-p_s^d) \left(c_s^d + \frac{1}{M-1} c_f^d \right) \right] + (1-p_s^A) [p_s^d c_s^d + (1-p_s^d) c_s^d] \quad (7)$$

类似地

$$E[c_i^{\text{stay}}] = p_s^A \cdot 0 + (1-p_s^A) [p_s^d c_f^d + (1-p_s^d) c_f^d] \quad (8)$$

如上文讨论, 对 i 来讲, 在混合策略纳什均衡下, $E[c_i^{\text{switch}}]$ 、 $E[c_i^{\text{stay}}]$ 两者相等, 计算得

$$p_s^A = \frac{c_f^d - c_s^d}{c_f^d} \frac{M-1}{M} \quad (9)$$

接着, 考虑在均衡下, SDDC 以概率 p_s^d 切换, 令 $E[c_A^{\text{switch}}]$ 、 $E[c_A^{\text{stay}}]$ 分别代表 i 选择切换或者保持不变 2 种选择下 A 的期望收益。

$$E[c_A^{\text{switch}}] = (p_s^d)^2 \left[\frac{2(M-2)}{(M-1)^2} B^A + \frac{1}{(M-1)^2} B^A \right] + 2p_s^d(1-p_s^d) \frac{B^A}{M-1} + (1-p_s^d)^2 \cdot 0 - c_s^A \quad (10)$$

类似地

$$E[c_A^{\text{stay}}] = 2p_s^d(1-p_s^d)B^A + (1-p_s^d)^2 B^A \quad (11)$$

均衡状态下, $E[c_A^{\text{switch}}]$ 、 $E[c_A^{\text{stay}}]$ 两者相等, 化简之后, p_s^d 可通过以下公式求解。

$$[(p_s^d)^2 - (1 - \frac{p_s^d}{M-1})^2] B^A - c_s^A = 0 \quad (12)$$

基于以上分析, 三人博弈时的均衡定理如下。

定理 2 混合策略纳什均衡下, 若网络 (SD DC, d) 被攻击成功, 下一刻应该以概率 p_s^d 选择切换为另一个控制器。并且, 攻击者在攻击成功之后, 其选择改变攻击模式的概率为 $\frac{c_f^d - c_s^d}{c_f^d} \frac{M-1}{M}$,

实施攻击下一刻的控制器执行体。

4.4 $N+1$ 个参与者博弈

假设网络中包含 D 个 SDDC, 本节将一般化 D 个 SDDC 和一个攻击者的安全模型。每个 SD DC 切换的概率为 p_s^d , 攻击者切换的概率为 p_s^A 。节点 $i \in \{1, \dots, D\}$ 采取混合策略时, 其在切换和保持不变 2 种状态之间保持平衡。令 $E[c_i^{\text{switch}}]$ 和 $E[c_i^{\text{stay}}]$ 分别代表 A 选择切换或者保持不变时, i 的期望代价。

$$E[c_i^{\text{switch}}] = c_s^d + \frac{1}{M-1} c_f^d p_s^A \quad (13)$$

类似地

$$E[c_i^{\text{stay}}] = (1-p_s^A) c_f^d \quad (14)$$

如上文所述, 在均衡状态下, 两者相等, 可得

$$p_s^A = \frac{c_f^d - c_s^d}{c_f^d} \frac{M-1}{M} \quad (15)$$

在均衡下, SDDC 以概率 p_s^d 切换控制层的控制器, 令 $E[c_A^{\text{switch}}]$ 、 $E[c_A^{\text{stay}}]$ 分别代表 d 选择切换或者保持不变时 A 的收益。

$$E[c_A^{\text{switch}}] = \binom{N}{1} p_s^d (1-p_s^d)^{D-1} \left[1 - \left(\frac{M-2}{M-1} \right)^1 \right] B^A + \binom{N}{2} (p_s^d)^2 (1-p_s^d)^{D-2} \left[1 - \left(\frac{M-2}{M-1} \right)^2 \right] B^A + \dots + \binom{N}{N} (p_s^d)^N (1-p_s^d)^{D-N} \left[1 - \left(\frac{M-2}{M-1} \right)^D \right] B^A - c_s^A \quad (16)$$

类似地, 有

$$E[c_A^{\text{stay}}] = \binom{N}{0} (p_s^d)^0 (1-p_s^d) B^A + \binom{N}{1} (p_s^d)^1 (1-p_s^d)^{D-1} B^A + \dots + \binom{N}{N} (p_s^d)^N (1-p_s^d)^{D-N} \cdot 0 \quad (17)$$

均衡时, 两者相等, 使用二项式定理化简,

获得式(18), 进而求最优的 p_s^n 。

$$\left[(p_s^d)^D - \left(1 - \frac{p_s^d}{M-1} \right)^D \right] B^A - c_s^A = 0 \quad (18)$$

5 仿真结果

5.1 实验环境设置

本次实验在配置 Intel(R) Core i7-4790 CPU 3.6 GHz, 16 GB RAM 的主机上进行, 博弈问题的求解均通过 Mathematica 编程实现。

5.2 实验结果分析

本节通过仿真结果分析博弈均衡下的有效性。

为了方便起见, 取 $D=6$, $M=3$, $B^A=1$, 得到如图3所示的结果。图3描述了纳什均衡下 SDDC 切换控制器的概率与攻击者改变攻击模式代价的关系, 容易看出, 两者是正相关关系。进一步地分析, 因为不同控制器执行体可被利用的脆弱点开始有所不同, 所以攻击者不得不重新探测分析, 寻找新的脆弱点, 造成攻击者的代价增加, 即攻击者越来越难以切换攻击模式。所以, 随着控制器执行体可利用的脆弱点更加多样化, 对于防御者来说, 增加切换新控制器的概率将变得更优。

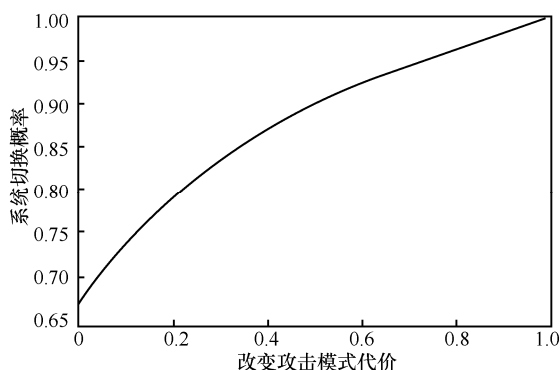


图3 控制器切换概率随改变攻击模式代价变化

图4描述了 SDDC 数量与纳什均衡下 SDDC 切换控制器概率两者的关系。图4中, $M=5$, 从图中可以直观地看出, 当攻击者的切换代价是0或者0.1时, SDDC 的切换概率呈现递减的趋势, 这主要有以下原因: 较低的攻击者切换代价(如不同控制器执行体之间存在共有的漏洞)意味着攻击者切换攻击模式, 攻击

一种新的控制器相对比较容易。而且, 当 M 不变, 随着 SDDC 数量的增加, 其越来越难以通过切换使攻击者不确定其状态, 也就是说, 随着 SDDC 增加, 防御者开始降低切换控制器的概率使攻击者达到供求均衡。然而, 当攻击者的切换代价增加到0.3时, 表示其攻击新的控制器变得更难, 故 SDDC 能够更随意地切换各种控制器防止脆弱点被攻击。

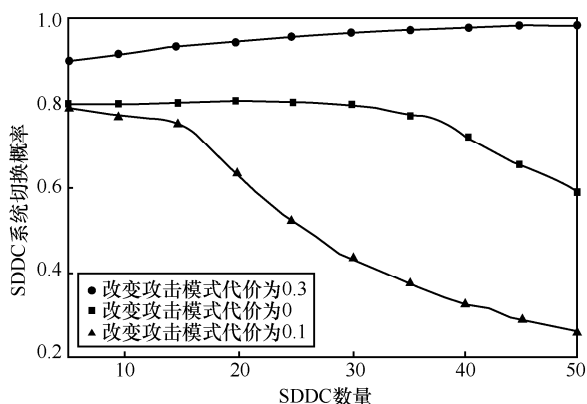


图4 3种攻击代价下控制器切换概率与SDDC数量的关系

图5描述了 SDDC 中控制器异构执行体(M)的数量与纳什均衡下 SDDC 切换概率两者的关系。防御者利用潜在的各种控制器执行体的多样性使攻击者在无法精确攻击。图5中, $D=10$, 可以看出, SDDC 的切换概率随着攻击者切换代价的增加而增加, 此结果与图3相互印证。

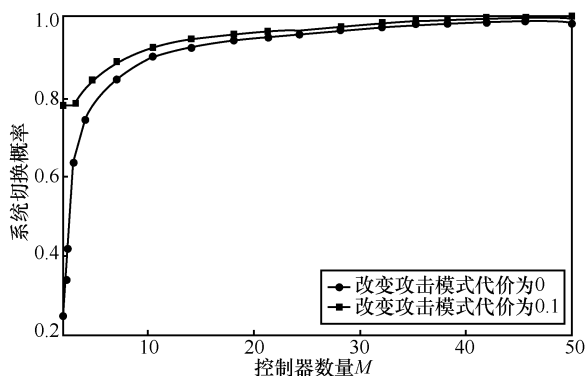


图5 2种攻击改变代价下切换概率与控制器数量的关系

图6描述了攻击者切换概率与执行体数量两者的关系, 从图中可以看出, 两者呈正相关。攻击者改变攻击模式概率的趋势本质上是因为随着 M 的增加, 防御者的切换概率增大。对攻击者来讲, 随着 M 增加, 选择切换一种新的攻击模式比再次使用先前的攻击模式进行攻击更优。

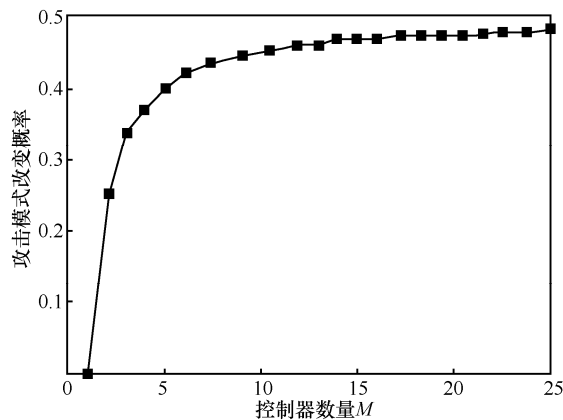


图6 攻击模式改变概率与控制器数量的关系

6 结束语

本文利用控制器的多样性抵御针对SDN控制层的网络攻击。首先，根据不同的安全需求，通过部署不同数量的控制器实例，以及控制器实例间的动态切换，提高攻击者的攻击难度；其次，为求解上述部署策略，提出了一种攻防博弈模型，求解纳什均衡，得到最佳的异构控制部署；最后，分析了均衡策略的有效性。仿真结果表明所提出方法的有效性以及在安全环境下策略交互的动态性，并且通过对动态性分析，防御者可以依据不同的网络条件，调整部署控制器。下一步的工作将以如何部署控制器的调度机制、保持网络调度前后的一致性为主要研究点展开研究。

参考文献：

- [1] WANG T, LIU F, GUO J, et al. Dynamic SDN controller assignment in data center networks: Stable matching with transfers[C]//IEEE INFOCOM 2016- IEEE International Conference on Computer Communications. 2016: 1-9.
- [2] 王蒙蒙, 刘建伟, 陈杰, 等. 软件定义网络: 安全模型、机制及研究进展[J]. 软件学报, 2016, 27(4): 969-992.
WANG M M, LIU J W, CHEN J, et al. Software defined networking: security model, threats and mechanism, software defined networking: security model, threats and mechanism[J]. Journal of Software, 2016, 27(4): 969-992.
- [3] SCOTT-HAYWARD S, O'CALLAGHAN G, SEZER S. SDN security: a survey[C]//Future Networks and Services. 2013:1-7.
- [4] KOPONEN T, CASADO M, GUDE N, et al. Onix: a distributed control platform for large-scale production networks[C]//Unix Conference on Operating Systems Design and Implementation. 2010:351-364.
- [5] BERDE P, HART J, HART J, et al. ONOS: towards an open, distributed SDN OS[C]//The Workshop on Hot Topics in Software Defined Networking. 2014:1-6.
- [6] MEDVED J, VARGA R, TKACIK A, et al. OpenDaylight: towards a model-driven SDN controller architecture[C]//IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks. 2014:1-6.
- [7] AHMAD I, NAMAL S, YLIANTTILA M, et al. Security in software defined networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4):2317-2346.
- [8] LI H, LI P, GUO S, et al. Byzantine-resilient secure software-defined networks with multiple controllers in cloud[J]. IEEE Transactions on Cloud Computing, 2015, 2(4):436-447.
- [9] ELDEFRAWY K, KACZMAREK T. Byzantine Fault Tolerant Software-Defined Networking (SDN) Controllers[C]//Computer Software and Applications Conference. 2016:208-213.
- [10] HU H, PANG L, WANG Z, et al. Orchestrating Network Functions in Software-Defined Networks[J]. China Communications, 2017, 14(2):104-117.
- [11] QI C et al. An intensive security architecture with multi-controller for SDN[C]//INFOCOM Posters, 2016.
- [12] QI C, WU J, HU H, et al. Dynamic-scheduling mechanism of controllers based on security policy in software-defined network[J]. Electronics Letters, 2016, 52(23):1918-1920.
- [13] LU Z, CHEN F, WU J, et al. Poster: A Secure control plane with dynamic multi-NOS for SDN[C]//Network and Distributed System Security Symposium (NDSS). 2017.
- [14] SALIH M A, COSMAS J, ZHANG Y. OpenFlow 1.3 extension for OMNeT++[C]//IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. 2015:1632-1637.
- [15] LIANG L, WU J, COOK W D, et al. The DEA game cross-efficiency model and its Nash equilibrium[J]. Operations Research, 2008, 56(5):1278-1288.

[作者简介]



胡军台（1969-），男，河南禹州人，硕士，国网河南省电力公司平顶山供电公司总工程师，主要研究方向为电力系统及电网规划管理。

武振宇（1971-），男，河北枣强人，硕士，国网河南省电力公司平顶山供电公司教授级高级工程师，主要研究方向为电力系统及电网运行管理。

付晓（1979-），男，河南浙川人，硕士，国网河南省电力公司平顶山供电公司高级工程师，主要研究方向为电网发展与规划。

王逸超（1989-），男，河南平顶山人，国网河南省电力公司平顶山供电公司助理工程师，主要研究方向为电网规划及科技信息管理。