

基于 NFV 的新的协作式 DDoS 防御技术

许传丰^{1,2}, 林晖^{1,2}, 郭烜成^{1,2}, 汪晓丁^{1,2}

(1. 福建师范大学数学与信息学院, 福建 福州 350117;
2. 福建师范大学福建省网络安全与密码技术重点实验室, 福建 福州 350117)

摘要: 在采取网络功能虚拟化技术构建的协作式网络抵御分布式拒绝服务攻击的过程中, 由于协作网络中的资源有限, 协作网络中的参与者存在为了自身安全而采取自私行为的问题, 进而减弱协作网络缓解 DDoS 攻击能力。针对上述问题, 提出了一种新的缓解 DDoS 攻击策略。该策略在协作网络中构建重复囚徒困境博弈模型, 引入奖罚分明激励机制加强协作网络的协作性, 并采取基于社会信誉值评估的动态资源分配机制。仿真实验表明, 新的协作式 DDoS 攻击防御技术在分组丢失率、协作性和资源分配率方面优于现有方案, 提高了 DDoS 攻击防御的有效性。

关键词: 分布式拒绝服务攻击; 网络功能虚拟化; 协作网络; 自私行为; 囚徒困境博弈

中图分类号: TP393.08

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019018

New collaborative DDoS defense technology based on NFV

XU Chuanfeng^{1,2}, LIN Hui^{1,2}, GUO Xuancheng^{1,2}, WANG Xiaoding^{1,2}

1. School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350117, China
2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350117, China

Abstract: To solve the problem of selfish behavior for self-security due to limited resources in the process of resisting distributed denial of service (DDoS) attacks by a collaborative network built with network function virtualization (NFV) technology, a new collaborative DDoS defense network model was proposed. a repeat prisoner's dilemma game model was built in the collaborative network, a reward and punishment incentive mechanism was introduced to strengthen the cooperation of the collaborative network, and a dynamic resource allocation mechanism based on social reputation value assessment was adopted. Simulation results show that the new collaborative DDoS attack

收稿日期: 2018-11-20; 修回日期: 2019-01-25

通信作者: 林晖, linhui@fjnu.edu.cn

基金项目: 国家自然科学基金面上资助项目(No.61772008); 福建省引导基金资助项目(原工业重点基金资助项目)(No.2016Y0031); 福州市科技局基金资助项目(2017-G-79); 福建省自然科学基金资助项目(2016J01289)

Foundation Items: The National Natural Science Foundation of China (No.61772008), Fujian Province Guiding Project (formerly Key Industrial Project) (2016Y0031); Fuzhou Science and Technology Bureau Project (No.2017-G-79), The Natural Science Foundation of Fujian Province (No.2016J01289)

论文引用格式: 许传丰, 林晖, 郭烜成, 等. 基于 NFV 的新的协作式 DDoS 防御技术[J]. 网络与信息安全学报, 2019, 5(2): 66-76.
XU C F, LIN H, GUO X C, et al. New collaborative DDoS defense technology based on NFV[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 66-76.

defense technology outperforms existing solutions in terms of packet loss rate, cooperation, and resource allocation rate, improving the effectiveness of DDoS attack defense.

Key words: distributed denial of service attack, network function virtualization, collaborative network, selfish behavior, prisoner's dilemma game

1 引言

由于分布式拒绝服务(DDoS)攻击发起简单、破坏性大的特点,目前正被世界范围内的攻击者广泛使用^[1]。随着攻击规模越来越大,尽量减轻攻击者对受害主机的危害程度、尽快恢复正常服务能力是当今DDoS攻击防御研究的重点话题之一^[2]。显然,面对大量数据时,在不影响系统能力的前提下,有效过滤异常流量是DDoS攻击防御的关键技术^[3]。传统用于缓解DDoS攻击的设备(如IPS等),具有成本较高、计算能力有限的

限制,而网络功能虚拟化(NFV)作为一种新兴技术,通过在商用服务器上运行的虚拟机实现网络功能,可以代替传统设备灵活地缓解DDoS攻击^[4]。现有的基于NFV的协作式防御网络依靠网络中的参与者通过资源共享增强对大规模DDoS攻击的抵抗力^[5],如图1所示。

协作式防御网络能有效缓解DDoS攻击主要依赖资源分配机制实现。即通过资源请求者和资源提供者构建多领导多跟随的Stackelberg博弈,通过研究所有参与者的最优策略,推导出纳什均衡使现有资源合理分配,并通过衡量历史信誉值判定恶意参与者。但现有的解决方案基于这样的

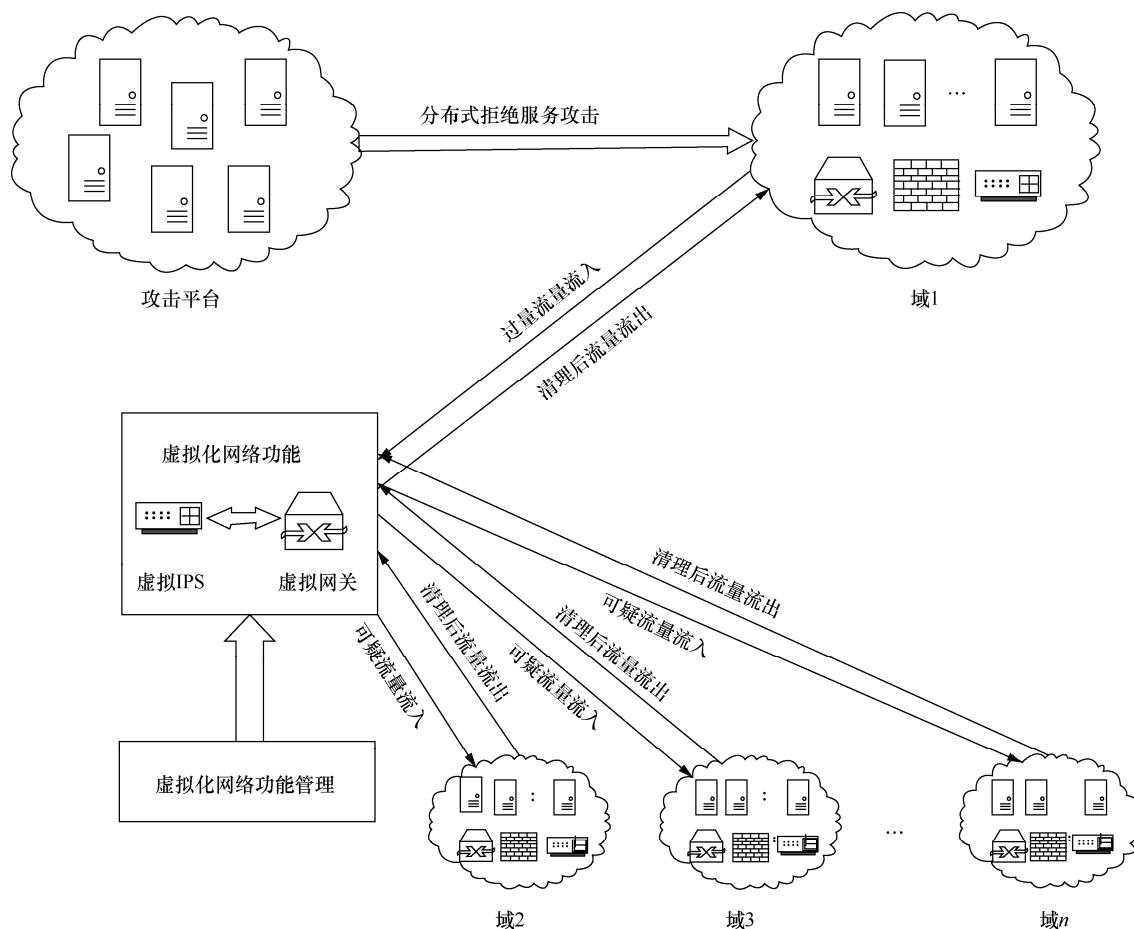


图1 基于NFV的协作式防御网络架构

假设,即协作网络中的参与者是顾全大局的,忽略了协作网络中参与者具有个体理性的特点,而由此引发的部分参与者采取自私行为谋取自身最大利益,造成协作网络抵御 DDoS 攻击的能力大幅下降^[6]。参与者采取自私行为具体包括:①不合作行为,不合作行为包括丢弃流量和拒绝帮助,即参与者在协作网络中无作为;②共谋行为,共谋行为包括个人自私和社交自私。即协作网络在进行资源分配时,参与者和参与者通过“勾结”行为得到更多资源。

基于上述分析,本文针对协作式防御网络在缓解 DDoS 攻击时存在的自私行为问题,提出了一种新的缓解 DDoS 攻击技术。该技术提出了一种公平、激励的资源分配方式,具体包括对协作式防御网络构建重复囚徒困境博弈(PD, prisoner's dilemma)模型,通过引入奖罚分明激励机制引导博弈中的参与者采取合作策略,且在资源分配方式中添加社会信誉值评估方法,遏制共谋行为,提高防御 DDoS 攻击的有效性。这项工作主要贡献如下。

1) 针对协作网络中存在不合作行为问题,构建重复囚徒困境博弈模型,并引入奖罚分明策略,激励博弈过程中参与者采取合作策略为最优策略。

2) 针对协作网络中资源分配机制存在共谋行为问题,在资源分配机制中添加社会信誉值评估。

3) 仿真实验引入新的协作式防御策略,实验结果表明分组丢失率和资源分配率优于现有的基于 NFV 的协作式 DDoS 防御策略。

2 相关工作

目前,NFV 技术开始用于实现 DDoS 攻击防御,已经出现了一些相关的研究成果。

Fayaz 等^[7]提出了一种基于 SDN 和 NFV 的 DDoS 防御解决方案——Bohatei 方案。Bohatei 的 DDoS 缓解系统依赖于供应商提供的针对不同

攻击类型的有向无环图。系统对攻击流过滤采取将攻击类型与防御策略相匹配的方法,采取合适的防御策略对攻击流过滤。但此方案成本高,并容易引起隐私问题。

Guenane 等^[8]使用 NFV 技术和其他网络虚拟化功能设计了基于云的防火墙服务架构来防御 DDoS 攻击。该系统通过 NFV 作为动态实例化中间盒的手段,将属于合法连接的流量和潜在的攻击流量分开,来抵御 DDoS 攻击。

Rashidi 等^[9]提出一系列基于 NFV 技术解决 DDoS 攻击策略——VGuard、CoFence^[5]和基于桶转发机制的灵活 DDoS 缓解系统^[10]。VGuard 是一种使用 NFV 技术实现基于优先级划分的动态流量工程。将外部区域的流量按优先级指向不同的隧道,通过静态和动态两种方法为 DDoS 攻击下的可信流量提供满意的服务。但这种方法不适用于所有 DDoS 攻击;基于桶转发机制的灵活 DDoS 缓解系统是通过批处理转发提高调度程序的可伸缩性,使合法流量引入最小性能降级实现缓解 SYN 洪泛攻击;CoFence 是一种使用 NFV 的“域帮助域”协作域网络,其特点为通过资源共享缓解过量流量,但缓解流量过程中,内部存在着恶意行为问题,影响缓解 DDoS 攻击能力。

Jakaria 等^[11]提出的 VFence 是一种使用 NFV 技术区分攻击数据分组和合法数据的 DDoS 防御机制。系统使用网络代理在系统可能受到攻击时拦截数据分组,验证其真实性,并丢弃非法数据分组保护服务器安全。

综上所述,通过 NFV 技术实现 DDoS 攻击防御中,现有方案和成果虽然可以解决一些问题,但未考虑在防御过程中节点出现自私行为的问题。自私行为的出现,破坏了协作网络过滤 DDoS 攻击的能力。针对上述不足,本文构建奖罚分明的重复囚徒困境博弈模型,并引入基于社会信誉值的动态资源分配机制,有效遏制自私行为的产

生, 更好地抵御 DDoS 攻击。

3 预备知识

3.1 重复囚徒困境博弈模型

囚徒困境博弈是博弈论的非零和博弈中最具代表性的例子, 它反映了个人的最佳选择并非整体的最佳选择^[12]。

在原始的囚徒困境博弈中, 每个人都有两种选择合作 (C) 与背叛 (D)^[13]。如果双方合作或背叛, 玩家将获得奖励 R 或惩罚 P , 如果一方合作另一方背叛时, 合作方获得收益 S 而背叛方获得收益 T , 其收益矩阵 M 为^[14]

$$M = \begin{matrix} & \begin{matrix} C & D \end{matrix} \\ \begin{matrix} C \\ D \end{matrix} & \begin{bmatrix} R & S \\ T & P \end{bmatrix} \end{matrix} \quad (1)$$

式(1)中最左侧一列代表自己的决策; 最上面一行代表邻域的决策; 收益满足排名 $T > R > P > S$ 。对于每个节点来说, 最优的策略是不合作策略, 但若博弈双方均不合作, 则双方的总收益 $2P$ 小于双方采取合作的总收益 $2R$, 这是囚徒困境博弈的困境所在。为了促进协作网络中参与者相互合作, 本文工作选择重复的 PD 博弈, 即重复囚徒困境 (IPD, iterated prisoner's dilemma) 博弈问题。

因此, 本工作构建 IPD 博弈模型, 博弈过程用 $\varsigma = \Gamma(N, (S_n(i))_{n \in N}, (u_n)_{n \in N})$ 的三元组表示^[14]。其中, 集合 N 用来表示所有参与者的集合; $S_n(i)$ 表示参与者 n 在第 i 轮博弈选择的策略空间, 而 $(S_n(i))_{n \in N} = S_1(i) \times S_2(i) \times \cdots \times S_n(i)$ 表示所有参与者在第 i 轮博弈形成的策略空间组合, $S_n(i) = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ 。其中, $S_n(i) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ 表示参与者 n 在第 i 轮博弈采取合作行为, $S_n(i) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ 表示参与者 n 在第 i 轮博弈采取背叛行为^[15]; 映射

$u_n(s)$ 表示参与者 n 博弈 s 轮的平均效用函数, $u_n: (S_n(i))_{n \in N} \rightarrow R$, R 为实数集

$$u_n(s) = \frac{\sum_{i=1}^s \varphi_n(i) \cdot P_n(i) \cdot R_n^*(i)}{s} \quad (2)$$

其中, $\varphi_n(i)$ 为第 i 轮博弈的奖励系数, $P_n(i)$ 为参与者 n 的第 i 轮的效用, $R_n^*(i)$ 为参与者 n 直到第 i 轮的社会信誉值, s 为博弈总次数。

3.2 网络功能虚拟化

网络功能虚拟化是指使用软硬件解耦以及功能抽象代替专用的设备, 使网络管理者可以在网络功能虚拟化设备上配置网络功能及网络服务, 实现了资源充分灵活使用^[16]。

通过网络功能虚拟化技术, 使加入协作网络的节点共享虚拟 IPS。共享同一个虚拟 IPS 的所有节点统称为域。虚拟 IPS 的目的是检测和过滤 DDoS 攻击。因为 NFV 的灵活性, 可以在需要时创建虚拟 IPS, 并可动态配置其容量。为了方便研究, 本文阐述了基于 NFV 的协作式 DDoS 防御系统拓扑, 如图 2 所示。

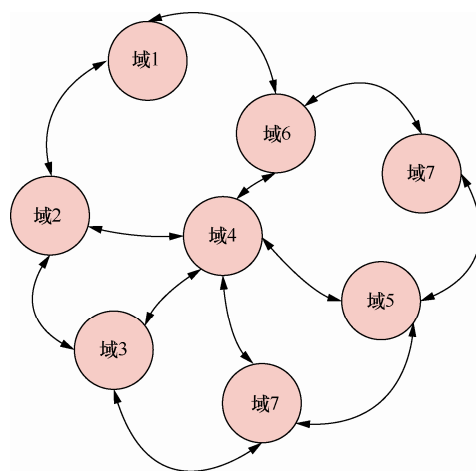


图2 协作网络拓扑

4 新的协作式 DDoS 防御策略

为了协作网络能有效避免自私行为对缓解 DDoS 攻击能力的影响, 本文针对自私行为中的

不合作行为和共谋行为进行改进。首先,在 IPD 博弈模型中添加奖罚分明策略,通过奖励手段和惩罚手段,IPD 博弈参与者选择合作策略作为最佳策略,博弈的结果也间接影响了社会信誉值;其次,提出了由所有邻居参与者参与评估的社会信誉值评估方式,避免了协作网络进行资源分配过程中存在勾结行为,并由此提出基于社会信誉值的资源分配方式;最后,描述了能有效遏制自私行为,促进协作网络缓解 DDoS 攻击能力的协作式防御策略具体方案。

4.1 奖罚分明的 IPD 博弈模型

为了激励博弈参与者选择合作策略作为自己的最佳策略,本文工作在博弈中添加奖罚分明策略。奖罚分明策略具体描述为:博弈过程中若一方犯错,则此次博弈两方同时受到惩罚,收益减少;若一方连续 K 轮博弈中都没有犯错,则在第 $K+1$ 次博弈获得收益奖励。

为了简化收益矩阵 M 中参数的数量,这里采取 Nowak 和 May 使用的收益矩阵 (其中 $1 < b < 2$)。

$$M = \begin{bmatrix} 1 & 0 \\ b & 0 \end{bmatrix} \quad (3)$$

奖罚分明的 IPD 博弈模型的详细描述如下。

1) 初始化协作网络,其度分布服从泊松分布。

2) 初始化每个域的策略,即为每个参与者随机设定一个初始策略。

3) 初始化每个域的收益矩阵, $M = \begin{bmatrix} 1 & 0 \\ b & 0 \end{bmatrix}$,

其中 $1 < b < 2$,初始化 $\varphi_n(1)$ 为 1.0,初始化 $P_n(1)$ 为 0,初始化 R_n^* 为 0;

4) 依次取网络中的每个域 j 与自己的邻居域 i 重复博弈,判断每次博弈后域 j 的单次效用 $P_j(i)$ 。

$$P_j(i) = \sum_{l \in \Omega_j} [s_j^T M s_l - \beta(1 - s_j^T s_l)] \quad (4)$$

其中, s_j 为域 j 采取的策略, s_l 为域 l 采取的策略, β 为惩罚因子, $0 < \beta < 1$, $P_j(i)$ 为所有邻域 j 对域 i 采取的措施的收益。由 $P_j(i)$ 可知,当 s_j 和 s_l 同时采取合作策略,本次博弈效用才能增加,否则受到惩罚。

5) 记录域 j 采取合作策略的次数。

① 若连续 K 次博弈都采取合作策略,则第 $K+1$ 次的奖励系数为

$$\varphi_j(k+1) = (1+\alpha)\varphi_j(k) = (1+\alpha)\varphi_j(1) = 1+\alpha \quad (5)$$

其中, α 为奖励因子, $0 < \alpha < 1$,但在 $K+2$ 次博弈,恢复初始值,并重新记录合作次数。

② 若没有达到连续 K 次博弈都采取合作策略,则奖励系数一直为初始值 $\varphi_n(1) = 1.0$ 。

6) 重复步骤 4) 和步骤 5),直至所有域与邻域博弈结束。

7) 奖罚分明策略流程如图 3 所示。

该模型充分考虑了博弈的演化过程中个体的自主性,在重复博弈过程中通过奖罚分明,激励博弈参与者选择合作策略作为自己最佳策略。

定理 1 添加奖罚分明策略后,IPD 博弈模型中的参与者为了获得更高收益而选择采取合作作为最佳策略。

证明 假设 $u_n(s+1) \geq u_n(s)$ 时,代入式(2)可得

$$\frac{\varphi_n(s+1) \cdot P_n(s+1) \cdot R_n^*(s+1)}{s+1} \geq 0 \quad (6)$$

由于奖励系数 $\varphi_n(s+1) \geq 0$ 恒成立,且社会信誉值 $R_n^*(s+1) \geq 0$ 也恒成立,则只须判断 $P_n(s+1) \geq 0$ 是否成立。

由式(4)知

$$P_n(s+1) = \sum_{l \in \Omega_n} [s_n^T M s_l - \beta(1 - s_n^T s_l)] \quad (7)$$

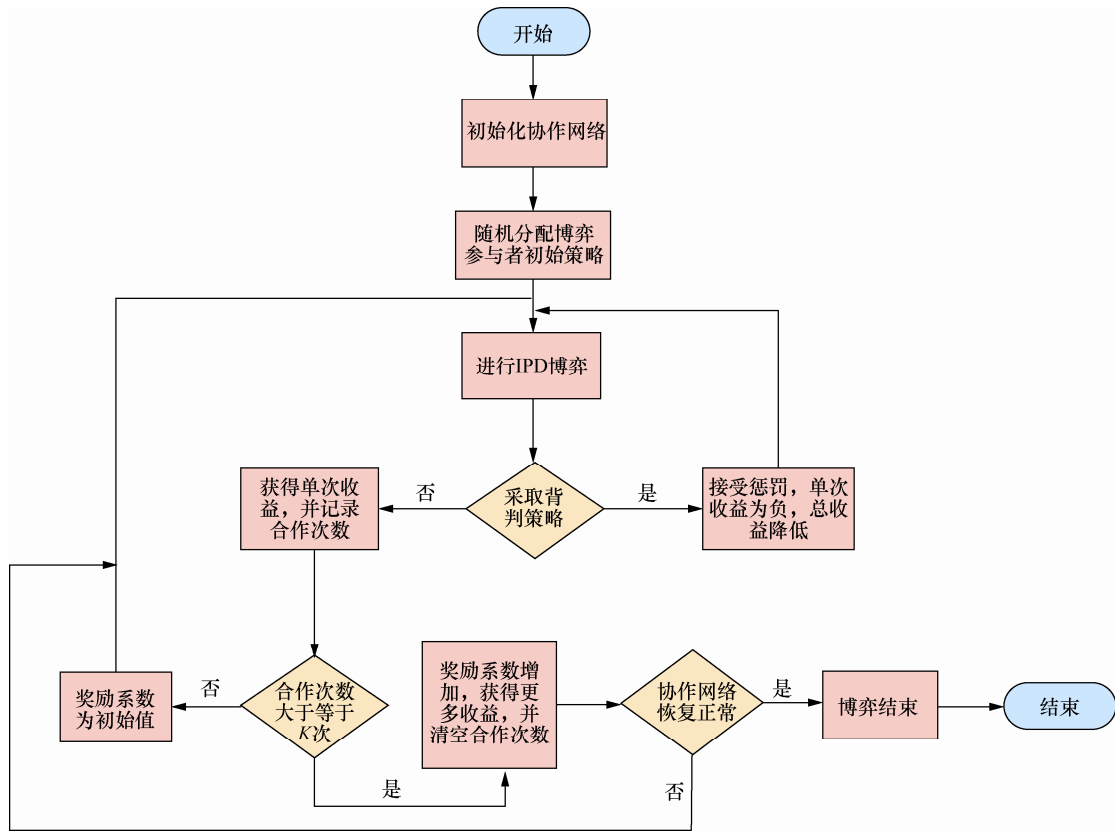


图3 奖励分明策略的IPD博弈流程

即当域 n 的多个邻域中, 采取合作行为的域的数量大于采取不合作行为的域的数量时, $P_n(s+1) > 0$ 成立, 此时博弈模型获得更多的收益, 且合作行为的域的数量越多, 收益越多, 证明成立。

4.2 基于社会信誉值的资源分配方式

协作网络有效缓解DDoS攻击主要通过动态资源分配机制实现^[14]。现有的方案通过在协作网络中构建多领导多跟随的Stackelberg博弈并基于历史信誉值进行资源分配, 但这种机制无法解决共谋行为, 即域和邻域存在“勾结”行为, 两个采取自私行为的域通过相互抬高对方信誉来欺骗其他域。

本文提出了一种新的通过社会信誉值决定资源分配的策略, 通过所有邻域对该域综合评估确定该域的社会信誉值可以有效遏制共谋行为。协作网络参与者分配给所有邻居参与者资源量的多

少, 按邻居参与者社会信誉值决定, 且一旦社会信誉值低于阈值, 协作网络将此参与者判定具有自私行为, 从协作网络中移除。

本文的社会信誉值由直接信誉值和间接信誉值构成。下面介绍资源分配方式中社会信誉值的相关定义。

直接信誉值: 若域 m 与域 n 互相帮助分担流量, 域 m 帮助域 n 分担资源为 α_{mn} , 域 n 帮助域 m 分担资源为 β_{mn} , 则域 m 在域 n 处的直接信誉值为

$$R_{mn} = \frac{\alpha_{mn}}{\alpha_{mn} + \beta_{mn}} \quad (8)$$

间接信誉值: 域 n 不仅考虑本处对域 m 的直接信誉值, 域 n 还将其他邻域 k 处对域 m 的信誉值与域 m 在博弈过程中采取的行为作为参考。即间接信誉值为

$$I_{mn}^k = R_{mk} \cdot \gamma \quad (9)$$

其中, γ 为奖惩因子, $\gamma = \begin{cases} 1+\alpha, & \text{域采取合作策略} \\ 1, & \text{初始值} \\ 1-\beta, & \text{域采取拒绝策略} \end{cases}$ 。

社会信誉值由所有邻居参与者的间接信誉值加和平均与该参与者的直接信誉值构成。

$$R_{mn}^* = \frac{\sum_{k \in S} I_{mn}^*}{S} \cdot \lambda + R_{mn} (1 - \lambda) \quad (10)$$

其中, $0 \leq R_{mn}^* < 1$, λ 为比例系数, λ 决定直接信誉值与间接信誉值在社会信誉值所占比例。

由于社会信誉值评估方法是通过所有邻居参与者的综合评估, 所以参与者之间采取勾结行为, 也无法迅速地获得更多的收益。

定理 2 协作网络中的参与者帮助具有更高社会信誉值的参与者, 所得到的回报更多。

证明 假设域 m 与域 n 互相帮助分担流量, 域 m 在域 n 处的社会信誉值为

$$R_{mn}^* = \frac{\alpha}{\beta} \quad (11)$$

其中, $\alpha < \beta$ 。

域 m 在与一个域合作后, 其综合信誉值为

$$R_{mn}^* = \frac{\alpha + \mu}{\beta + \mu} \quad (12)$$

设与信誉值较低的域合作后得到 μ_1 , 与信誉值较高的域合作后得到 μ_2 。即要证明当 $\mu_1 < \mu_2$ 时, $R_{mn1}^* < R_{mn2}^*$ 。

假设 $R_{mn1}^* < R_{mn2}^*$, 则有

$$\frac{\alpha + \mu_1}{\beta + \mu_1} < \frac{\alpha + \mu_2}{\beta + \mu_2} \quad (13)$$

化简为

$$\alpha(\mu_2 - \mu_1) < \beta(\mu_2 - \mu_1)$$

由于 $\alpha < \beta$, 则 $\mu_1 < \mu_2$ 。反证成立, 即可证明当 $\mu_1 < \mu_2$ 时, $R_{mn1}^* < R_{mn2}^*$ 成立。由此可知任何一个域与信誉值高的域互相帮助, 能得到更高的信誉值, 也就会获得更多的回报。

基于社会信誉值的动态资源分配算法如下。

算法 协作网络中的域资源分配算法

输入邻域数量 k ; 社会信誉值 R ; 邻域 i 需要缓解自身安全的资源 S_i ; 协作网络用于资源分配的总资源 M

过程

- 1) 收集所有邻域最新的社会信誉值;
- 2) 循环 (对域与其每个邻居域)
- 3) 如果存在初始域, 即刚加入协作网络的域
- 4) 则初始域所获得资源分配 C_0 为

$$C_0 = \frac{M}{2k}$$

- 5) 否则按社会信誉值分配资源量
- 6) 判断终止条件, 结束循环
- 7) 根据域间博弈结果计算 R_j^* , R_m^* (即 R_j^* 是域 j 的社会信誉值, R_m^* 是域 m 的社会信誉值)
- 8) 计算每个域所能得到的资源 C_i

$$C_i = \frac{R_i}{\sum_{j=1}^j R_j} \cdot M$$

- 9) 当 $C_i - S_i > 0$ 时, $C_i \leftarrow S_i$
- 10) 否则输出 C_i

输出域分配到的资源量集合 C ; 社会信誉值集合 R

4.3 新的协作式 DDoS 攻击防御策略

本文在基于 NFV 的协作式防御架构的基础上, 构建具有激励机制的 IPD 博弈模型, 并引入基于社会信誉值得资源分配方式, 本文提出新的协作式 DDoS 攻击防御策略具体步骤 (如图 4 所示) 如下。

- 1) 节点发现自身流量过多, 超过自身存储能力。
- 2) 加入协作网络, 并分配自己能负担的最大资源。
- 3) 加入协作网络的域进行信誉值更新。
- ① 获得初始信誉值, 并进行重复囚徒困境博弈。

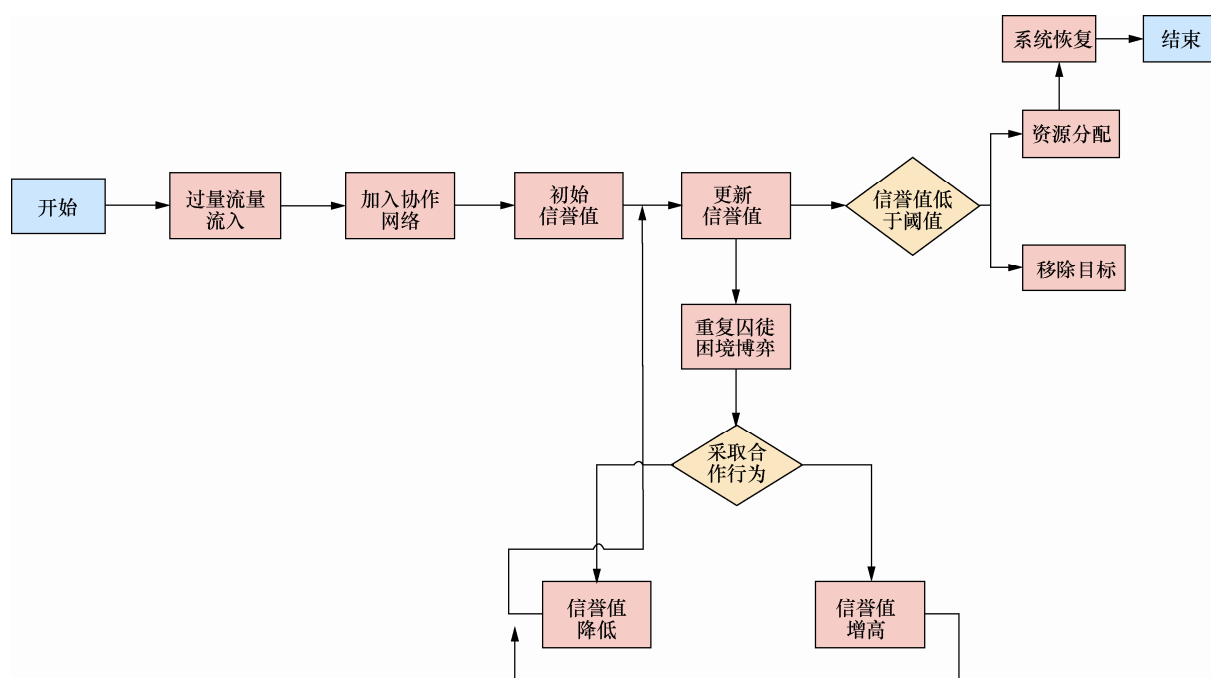


图4 新的防御DDoS攻击流程

② 判断域和邻域博弈时，是否采取合作行为。

a. 如果是，则域信誉值增加，效用增多，更新信誉值并进行下一步。

b. 如果不是，则信誉值降低，效用减小，更新信誉值并进行下一步。

4) 判断域的信誉值低于系统设置的阈值。

① 如果是，则判定域为自私域，从协作网络中删除。

② 如果不是，域可与邻域进行资源分配，使系统正常工作。

5) 直到协作网络内所有域完成博弈，并将过量流量过滤完毕，结束。

5 仿真结果和分析

本文通过搭建 Rashidi 等的 CoFence 协作网络中的仿真案例并与其进行对比，通过对比采取新的协作式 DDoS 攻击防御策略前后的运行结果，验证新的策略在分组丢失率、合作性和资源分配量上是否有更好效果，验证是否有效

遏制自私行为，并提高协作式网络缓解 DDoS 攻击有效性。

5.1 仿真模型

本文模拟原协作网络 CoFence^[5]中的域共享其虚拟 IPS 来实现 DDoS 数据过滤功能。网络中定义两种不同类别的流量：合法流量和攻击流量。合法流量为域在正常情况下接收到的流量，攻击流量为域在受到攻击时接收到的流量。合法流量的速率为 1 000 分组/秒，攻击流量的速率为 6 000 分组/秒，每个虚拟 IPS 的最大分组处理速率为 2 000 分组/秒。本文模拟 10~20 s 时间段为 DDoS 攻击时间。

如图 5 所示，域 i 内的流量为合法流量，域 j 在 10~20 s 之间存在攻击流量。在域 j 内存在大量攻击流量时，需要采取缓解措施并加入协作式网络。

域加入协作式网络的分组到达速率如图 6 所示。当加入协作式网络后，域 j 的分组到达速率下降为 5 000 分组/秒左右。这是由于域 i 帮助域 j 分担过量流量。

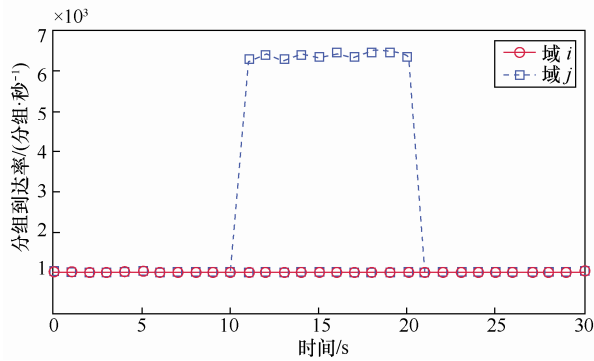


图 5 域的原始速率

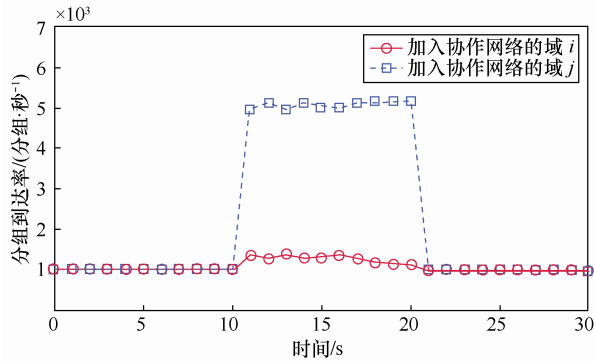


图 6 加入协同网络后域的速率

通过图 5 与图 6 对比可知，加入协作式网络的域可以有效缓解大量攻击流量的威胁。

5.2 分组丢失率

分组丢失率是指在一定时间内节点丢弃流量占总传输流量的比例。分组丢失率是判断缓解 DDoS 攻击能力的主要指标。

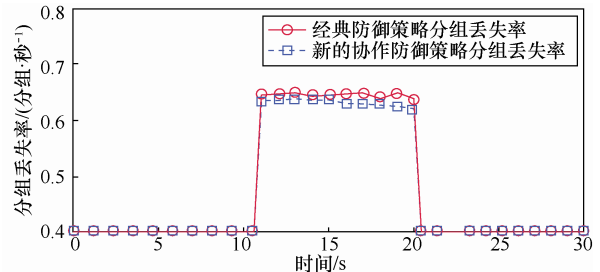
如图 7 所示，相对于经典的缓解 DDoS 攻击策略，新的协作防御策略的域具有较低的分组丢失率。而与采取原有策略时相比分组丢失率没有明显降低，新的协作防御策略在性能上没有明显提升，但该策略构成的协作式网络具有更好的安全性。

5.3 信誉值

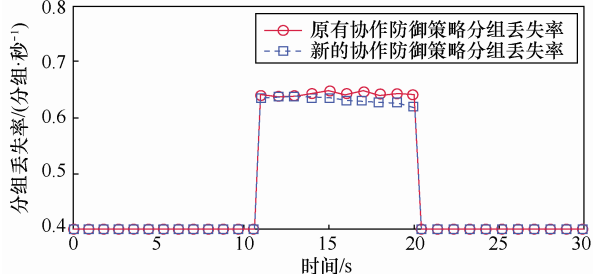
信誉值是本文提出的策略能有效解决协作式防御网络中自私行为的重要指标。

如图 8 所示，采取自私行为的域在经过一段次数的博弈后，域的信誉值低于系统设定的阈值，使采取自私行为的域剔除协作网络；而一直采取合作行为的域，在经过不断博弈中，

获得越来越高的信誉值，即证明在新的策略中采取合作行为可以获得更好的效益，提高了协作式网络的合作性。



(a) 加入经典防御策略



(b) 加入原有协作防御策略

图 7 新的协作防御策略与经典防御策略和原有协作防御策略的分组丢失率的对比

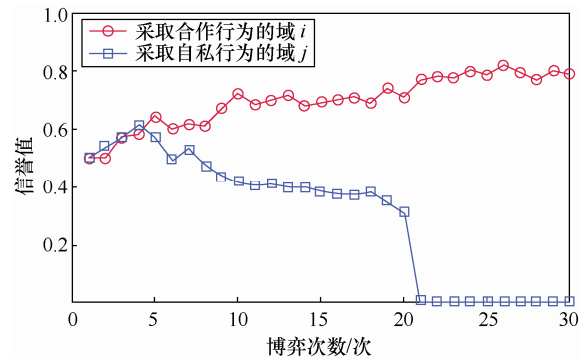


图 8 信誉值对比

5.4 资源分配量

在协作式网络中，域能公平、激励相容地得到应有资源量帮助恢复自身稳定，很大程度上影响着协作式网络缓解 DDoS 攻击的效果。所以，每个域的资源分配量也是判定协作式网络能有效缓解 DDoS 攻击的重要指标。

如图 9 所示，当邻域数量较少时，采用新的防御策略的域获得的帮助低于原有策略和经典策略的域，这是由于采取奖罚分明策略使域与邻域间较

容易受到惩罚。但随着邻域的增多,由于这种激励机制的存在,协作式网络间合作性大大增强,系统中的域乐意互相帮助来得到更多的收益,促进缓解 DDoS 能力增强。所以,该实验表明在邻域数量相对较多时,采取新的防御策略有助于域获得更多帮助。

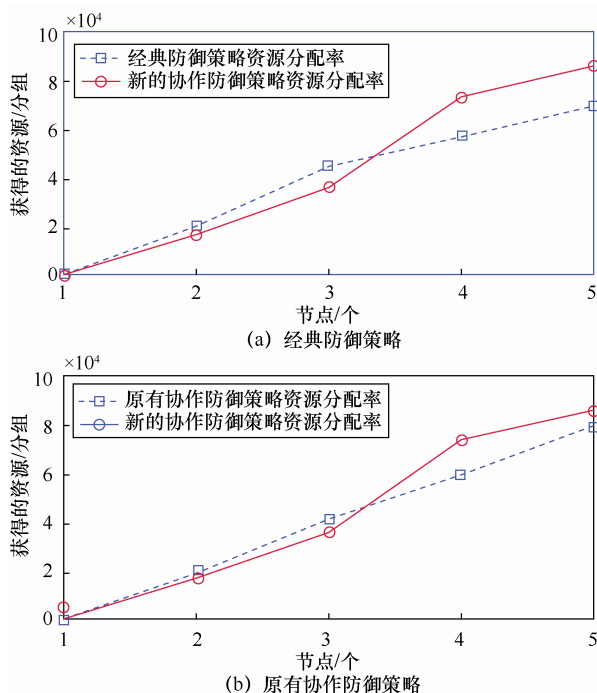


图9 新的协作防御策略与经典防御策略和原有协作防御策略的资源分配率对比

5.5 传输延迟

如图 10 所示,采取新的防御策略的域相对以往的 DDoS 防御技术多 0.3 ms 左右的延迟。这种延迟是新的防御策略使域间资源分配时,额外增加囚徒困境博弈过程,但这种延迟不影响 DDoS 防御功能。

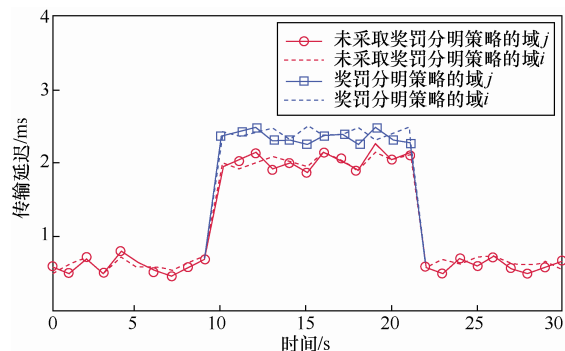


图10 传输延迟对比

6 结束语

本文针对 DDoS 防御系统中出现自私行为的问题,提出了新的协作式 DDoS 防御技术。通过使用 NFV 技术构建协作网络,在协作网络中构建重复囚徒困境博弈模型,采取奖罚分明策略激励合作并达到纳什均衡,并添加基于社会信誉值的资源分配方式,有效遏制了协作式网络中自私行为的产生。实验证明,与之前的协作式网络进行比较,该技术使协作式网络具有更好的合作性,且分组丢失率、资源分配量都有相较提升,使协作式网络更加高效地缓解 DDoS 攻击。在未来工作中将研究使用区块链中的工作量证明算法区分攻击者,更好地抵御 DDoS 攻击。

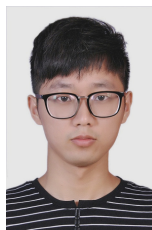
参考文献:

- [1] YAN Q, YU F R, GONG Q, et al. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 602-622.
- [2] MIRKOVIC, REIHER P. A taxonomy of DDoS attack and DDoS defense mechanisms[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(2): 39-53.
- [3] CHANG R K C. Defending against flooding-based distributed denial-of-service attacks: a tutorial[J]. Communications Magazine IEEE, 2002, 40(10): 42-51.
- [4] HERRERA J G, BOTERO J F. Resource allocation in NFV: a comprehensive survey[M]. IEEE Press, 2016.
- [5] RASHIDI B, FUNG C, BERTINO E. A collaborative DDoS defence framework using network function virtualization[C]//2016 12th International Conference on Network and Service Management (CNSM). 2016.
- [6] FENG L, YANG Q, KIM K, et al. Dynamic rate allocation and forwarding strategy adaption for wireless networks[J]. IEEE Signal Processing Letters, 2018, 25(7): 1034-1038.
- [7] FAYAZ S K, TOBIOKA Y, SEKAR V, et al. Bohatei: flexible and elastic DDoS defense[C]// Usenix Conference on Security Symposium. 2015: 817-832.
- [8] GUENANE F, NOGUEIRA M, SERHROUCHNI A. DDoS mitigation cloud-based service[C]//IEEE Trustcom/Bigdata/ISPA. 2015:

1363-1368.

- [9] FUNG C J, MCCORMICK B. VGuard: a distributed denial of service attack mitigation method using network function virtualization[C]//International Conference on Network and Service Management. 2015: 64-70.
- [10] RASHIDI B, FUNG C, RAHMAN M. A scalable and flexible DDoS mitigation system using network function virtualization[C]//IEEE/IFIP Network Operations and Management Symposium. 2018: 1-6.
- [11] JAKARIA A H M, YANG W, RASHIDI B, et al. VFence: a defense against distributed denial of service attacks using network function virtualization[C]//Computer Software and Applications Conference. 2016: 431-436.
- [12] LUO C, ZHANG X, LIU H, et al. Cooperation in memory-based prisoner's dilemma game on interdependent networks[J]. Physica A Statistical Mechanics & Its Applications, 2016, 450:560-569
- [13] PERC M, SZOLNOKI A. Social diversity and promotion of cooperation in the spatial prisoner's dilemma[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2008, 77(1 Pt 1): 011904
- [14] ASHLOCK D, KIM E Y, ASHLOCK W. A fingerprint comparison of different prisoner's dilemma payoff matrices[J]. IEEE Transactions on Biological Science, 2010(6): 219-226.
- [15] YANG H X, WU Z X, RONG Z, et al. Peer pressure: enhancement of cooperation through mutual punishment[J]. Phys Rev E Stat Nonlin Soft Matter Phys, 2015, 91(2):022121.
- [16] XU Z, LIANG W, GALIS A, et al. Throughput optimization for admitting NFV-enabled requests in cloud networks[J]. Computer Networks, 2018.

[作者简介]



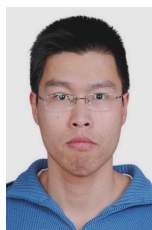
许传丰(1994-), 男, 江苏宿迁人, 福建师范大学硕士生, 主要研究方向为网络安全、博弈论。



林晖(1977-), 男, 福建福州人, 博士, 福建师范大学副教授、硕士生导师, 主要研究方向为信任管理、无线网络信息安全、移动云计算。



郭烜成(1995-), 女, 福建龙岩人, 福建师范大学硕士生, 主要研究方向为网络安全、机器学习。



汪晓丁(1982-), 男, 福建福州人, 福建师范大学讲师, 主要研究方向为网络优化与无线通信网络。