一种基于AS安全联盟的域间路由系统拟态防护机制

苗 甫[1] 王振兴[1] 郭 毅[1,2] 张连成[1]
(中国人民解放军信息工程大学 郑州 450001)[1]
(清华大学网络科学与网络空间研究院 北京 100084)[2]

摘 要 针对域间路由系统的大规模低速率拒绝服务攻击(Low-rate DoS against BGP Session,BGP-LDoS)能够造成域间路由系统的整体瘫痪,而现有的检测方法和防护措施难以有效检测和防御此类攻击。BGP-LDoS攻击实施的前提是对域间路由系统的拓扑进行探测分析,获取关键链路的相关参数信息。网络拟态变换能够通过持续的动态变换来迷惑攻击者,增加攻击者对网络进行探测与分析的代价和复杂度,降低攻击成功的概率。借鉴拟态安全防御思想,提出了一种域间路由系统拓扑动态变换的防护方法,由系统中多个相邻自治系统(Autonomous System,AS)组成AS拟态联盟,在联盟内部进行拓扑等效变换。文中给出了实现的具体过程。对拓扑变换后的网络抗BGP-LDoS攻击的能力进行验证分析,实验结果表明,利用该方法可有效降低攻击者对网络拓扑分析的精确度,干扰其关键链路的选择过程,从而实现对BGP-LDoS攻击的防护。

关键词 拟态变换,AS安全联盟,网络安全,域间路由
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.09.029

AS Security Alliance Mechanism for Inter-domain Routing System Based on Mimicry Protection

MIAO Fu[1] WANG Zhen-xing[1] GUO Yi[1,2] ZHANG Lian-cheng[1]
(The PLA Information Engineering University,Zhengzhou 450001,China)[1]
(Network Science and Network Space Research Institute,Tsinghua University,Beijing 100084,China)[2]

Abstract Large-scale low rate denial of service attack against BGP sessions can cause paralysis of the inter-domain routing system as a whole. However,existing detection methods and protection measures are difficult to effectively detect and defense against such attacks. Detecting the topology of the inter-domain routing system and obtaining the key link parameters are fundamental steps to the BGP-LDoS attack. Network's mimic transformation can provide continuous dynamic transformation to puzzle the attacker,increase cost and complexity of the attacker's detection and analysis,reduce attack's success probability. From the view of mimic security defense,this paper presented an inter domain routing system security alliance mechanism. The method uses neighboring autonomous systems form as an ally,and makes equivalent topology transformation in the alliance. The realization of the specific process was given. The resilience of the BGP-LDoS attack after the mimicry transformation was checked and analyzed. Experimental results demonstrate that the method can effectively reduce the attacker's network topology analysis accuracy,and interference attacker's target link selection process. It can provide reliable protection for inter-domain system to against BGP-LDoS attack.

Keywords Mimic transformation,AS alliance,Network security,Inter domain routing

1 引言

基于BGP(Border Gateway Protocol)的域间路由系统位于互联网的控制层面,是不同自治域互连及交换网络可达信息的基本机制,是网络运营商实现策略控制的主要手段,也是互联网的关键基础设施。然而域间路由系统在设计之初缺乏安全性考虑,致使域间路由系统安全性问题日益突出,针对域间路由系统的攻击手段也越来越复杂,造成的危害性也远大于传统网络攻击[1-2],特别是最近提出的CXPST[3]和DNP[4]等攻击方式能够造成域间路由系统长时间整体瘫痪,且尚无有效的防范措施,本文将此类型攻击统称为BGP-LDoS攻击。

BGP-LDoS攻击一般具有很强的隐蔽性,其利用域间路由系统的自适应机制[5](如TCP拥塞控制机制、路由器的主动队列管理机制等)存在的安全漏洞,短时间内周期性地发送

到稿日期:2016-08-25 返修日期:2016-12-06 本文受国家自然科学基金(61402525,61402526,61472215,61502528),国家"863"高技术研究发展计划基金(2012AA012902)资助。

苗 甫(1981-),男,博士生,主要研究方向为信息安全、网络安全,E-mail:ufoaim@qq.com;王振兴(1959-)男,教授,博士生导师,主要研究方向为信息安全、网络安全;郭 毅(1984-),男,博士,讲师,主要研究方向为网络安全,E-mail:nongfu@live.cn(通信作者);张连成(1982-),男,博士,讲师,主要研究方向为网络安全。

大量的网络攻击包，致使系统中路由节点间的会话反复重建和断开，继而产生大量的路由更新报文，从而进一步耗尽路由节点的计算和存储资源，致使整个系统陷入彻底瘫痪的状态。BGP-LDoS 的攻击过程中，攻击流量和攻击引起的反应都是合法的，现有的检测和防护技术很难对 BGP-LDoS 进行有效探测和防护，这给互联网的安全运行带来了严重威胁。

分析 BGP-LDoS 的攻击过程，发现其能够成功攻击的关键环节在于获取域间路由系统精确的拓扑结构，分析其中的关键目标链路，然后对这些目标链路进行探测，获取其链路两端路由的节点信息和链路参数后才能实施攻击。

据此，若要防范 BGP-LDoS 攻击，首先则需阻止攻击者获取域间路由系统的精确拓扑结构信息。然而，由于域间路由系统功能的特殊性，为了沟通可达性信息，各路由节点需要了解系统的整体拓扑信息，域间路由系统本身具有的静态性和确定性难以阻止 BGP-LDoS 攻击的发生。

网络拟态变换可以通过构建不确定的、动态的环境，使得攻击者缺乏足够的时间对系统进行有效探测，降低攻击者在攻击之前所收集信息的有效性，使其收集的信息在攻击过程中成为过时的、无效的信息，提高攻击者信息收集和探测的代价和复杂性，降低系统被成功攻击的概率。

借鉴拟态防御的思想，提出一种拟态防御的域间路由系统安全防护方法。依据域间路由系统特性，由域间路由系统自治节点组成拟态联盟，在联盟内部进行网络拓扑等效变换。在不影响系统功能的前提下，使得联盟后的域间路由系统网络拓扑呈现出动态的多样性和不确定性，以阻止攻击者对系统网络拓扑结构进行精确探测，从而阻止 BGP-LDoS 攻击的实施。

2　相关工作

2.1　现有域间路由系统的安全增强机制

针对域间路由系统面临的安全威胁，现有的域间路由系统的安全增强机制主要分为协议扩展和安全监测两类。

协议扩展主要是对域间路由系统中运行的 BGP 协议进行修改，解决其安全性不足的问题。协议扩展主要采用认证技术，典型的有 S-BGP(Secure BGP)[6]，soBGP[7](secure origin BGP)，psBGP[8](pretty security BGP)和 Listen & Whisper[9]等。

域间路由系统安全监测不对协议进行改变，而是对域间路由系统各 AS 之间交换的路由信息进行检查、识别，从而发现异常路由信息。典型的安全监测技术有 PHAS[10]和 IRV[11]等。

然而，这些解决方案主要是解决 BGP 缺乏安全可信的路由认证机制的问题，以及确保路由信息传播过程中的真实性和完整性，防范前缀劫持、路由泄漏以及路径伪造等安全问题的发生，针对的仅是域间路由系统的控制平面。而 BGP-LDoS 攻击主要是针对域间路由系统数据平面的攻击，即通过大规模的链路拥塞，使得域间路由系统中节点间反复通联，进而产生巨量的路由更新消息，耗尽路由器的计算资源和存储资源，造成域间路由系统瘫痪。因此，现有的方法难以有效防范 BGP-LDoS 攻击。

2.2　网络拟态安全防御研究现状

网络拟态防御通过变换网络结构来改变网络拓扑，使得网络拓扑呈现出动态性、异构性、不确定性、非持续性，是一种防范网络攻击的有效可行的方法[12-14]。网络拟态防御主要是通过降低网络的确定性、静态性和同构性来增加攻击者的攻击难度，使得攻击者没有足够的时间对目标网络进行探测；同时降低其所搜集信息的有效性，使其在探测期间收集的信息在攻击期间变得无效，降低系统被成功攻击的概率，从而达到防护的目的。

当前网络拟态安全防御技术主要有变形网络、自适应计算机网络和开放流随机主机转换技术(OFRHM)等 3 种。变形网络主要研究网络管理人员如何对网络、主机以及应用程序进行随机调整和配置，使得整个网络呈现出动态性。攻击者难以探查网络的动态变化，从而使得攻击者攻击失败，典型的有美国雷声公司的 Morphinator 项目[15]、SAFE[16]等。自适应计算机网络主要研究网络本身如何通过自动改变拓扑结构和设置来防御网络攻击，典型的有 Fuzzbuster[17]和 ACD[18]等技术，目前已经开发了相应的分析模型，证明了方法的有效性。开放流随机主机转换技术主要是利用动态网络地址转换、地址空间随机化、网络地址跳变等技术使得网络对外地址呈现出动态性，从而使得攻击者找不到攻击目标，以此破坏攻击者的攻击链，典型的有 NSAR[19]，HSS[20]，MT6D[21]等技术。

虽然拟态防御在应对网络攻击方面具有较好的发展前景，但目前的研究还处于顶层设计阶段，缺乏应用到现实系统和环境的研究成果。由于域间路由系统中各节点属于不同的机构且高度自治，其利益和需求也不尽一致，因此难以集中进行管理和控制。

基于此，提出一种基于 AS 安全联盟的域间路由系统拟态防护机制，研究在不影响域间路由系统正常功能的前提下高效部署和应用拟态变换，提高域间路由系统防范 BGP-LDoS 攻击的能力。

3　域间路由系统拟态联盟

3.1　拟态联盟组建方法及变换流程

在域间路由系统中由相邻的 AS 节点自愿组成联盟。联盟后，联盟内节点首先推举 AC 节点。各联盟节点向 AC 报告本节点资源，包含处理转发能力、链路带宽及相关信息。AC 分析获取联盟外部节点经过联盟内部的实际路径，同时获取其经过联盟的 k 条最短路径。根据是否遭遇安全威胁，联盟决定是否采用拟态变换。当遭遇安全威胁时，AC 从 k 条路径中随机挑选一条作为实际路径，判断这条路径是否满足资源约束条件。当满足资源约束条件时便将该路径作为实际通信路径，若不满足则选取多条路径以满足通信需求。设置定时器，当路径使用时间到期之后，再根据系统安全威胁情况判断是否恢复原有路径，或继续进行动态变换。在进行动态变换时，联盟内部的实际路径发生了变化，而对外显示的路径不变，有效地隐藏了联盟内部的真实通信路径，从而能有效防范 BGP-LDoS 的攻击。其整体流程如图 1 所示。

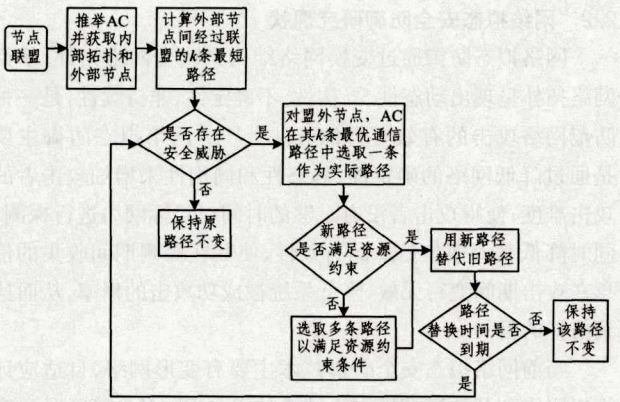

图 1 AS 拟态联盟组建及动态变换流程

以图 2 为例进行说明。AS1 和 AS10 自愿组建一个 AS 联盟 T。联盟后，各个节点根据自身处理能力和连接关系，推举 10 作为 AC，其他 AS 将自己的连接关系发送至 AC，AC 通过获取各节点之间的连接关系，确定了本联盟所连接的 4 个外部节点集合{A,B,C,D}。通过分析，AC 获取该节点集合时通过的联盟内部的实际路径为 A 1 4 3 7 9 B，C 1 4 3 D，B 9 7 3 D。根据联盟遭遇威胁的不同：当威胁较小时，AC 可以保持原来的实际路径不变；当威胁较大时，AC 计算所有外部节点经过联盟内部的 k 条最短路径，例如对于 C 和 D，计算得出另外 3 条最短路径分别是 C 1 2 5 8 D，C 1 4 5 8 D，C 1 2 10 8 D，随机采用其中一条路径作为新的通信路径。经过一段时间后，再次随机选择多个节点，随机从其 k 条最优路径选取一条作为新的通信路径。考虑资源约束问题，如果选取的路径 C 1 4 5 8 D 的最大承载量不能满足通信需求，由参与节点提出需求，AC 可以再随机指定一条路径，如 C 1 2 10 8 D，由这两条路径并行进行通信，确保满足承载量及业务需求。但所有这些路径的变换仅由联盟内部参与节点知悉，AC 所通告的路由信息不对盟外节点发布，因此对于联盟外部节点 A,B,C,D 而言，其路由表中存储的路径仍维持 A 1 4 3 7 9 B，C 1 4 3 D，B 9 7 3 D 不变。

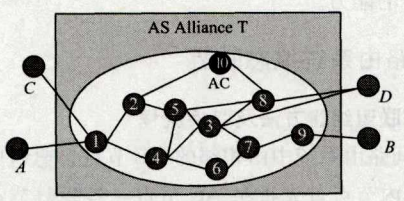

图 2 AS 拟态联盟示例

拟态联盟主要具备以下 3 方面的优势：

(1)有效干扰 BGP-LDoS 攻击前的拓扑关系和关键目标链路探测。联盟仅在内部对实际转发链路进行修改，而对外显示的路径并没有变化，攻击者无法探测出精确的路径消息，严重干扰了其攻击的实施。

(2)不影响域间路由系统的正常功能。利用路径变换，由 AC 控制联盟内部节点和链路的负载均衡，能够平衡各 AS 之间的利益关系，不影响各节点功能。

(3)不需要对现有的域间路由进行大的变动。充分利用现有的网络结构，不需要对现有的 BGP 协议和路由器进行变动，也不需要对拓扑关系进行修改，部署成本较低且扩展性较强，便于大规模部署。

拟态联盟需要解决的 3 个关键问题如下。

问题一：如何有效获取盟外节点对之间的 k 最短路径，降低计算复杂度；

问题二：如何变换盟外节点对之间的路径，使得攻击者无法探测真实通信路径，同时避免由于路径变换造成的实际通信路径增长，减少对系统通信效率的干扰；

问题三：由于各个节点均有自己的最大转发量，链路也有最大负载能力约束条件，在域间路由系统中，由于各时段的突发流量具有不确定性，如果在线路规划阶段进行资源规划，可能导致算法复杂度急剧增大，也难以保证满足资源的约束条件。因此如何有效解决资源约束问题也是拟态联盟变换的关键。

3.2 盟外节点对之间 k 最短路径的计算

定义 1(域间路由系统) 利用加权图 $G=(V,E)$ 表示域间路由系统。V 表示 AS 节点集合，v 表示一个 AS 节点，$\forall v\in V$，v_i 表示其编号。$\forall e\in E$，e_{ij} 表示连接两个节点 v_i 和 v_j 之间的一条直连链路。拟态联盟 $U(V_U,E_U)$ 是 G 的子集，V_U 和 E_U 分别是联盟 U 中的节点和链路的集合。

定义 2(节点属性集) 一个节点 v_i 某一时刻的最大处理能力为 $F(v_i)$，也称为节点的负载能力，当节点处理任务的能力大于负载能力时，节点工作失效，将引起系统不稳定。

定义 3(链路属性集) 一个链路 e_{ij} 的最大带宽为 $W(i,j)$，也称为链路的最大负载能力，当链路上的负载大于最大带宽时，链路拥堵，引起系统不稳定。

定义 4(节点邻接点集合) 对于 G 中的一个节点 v，其邻接点集合为 $\phi(v)=\{u|\langle u,v\rangle\in E\}$，与 v 直连的节点构成其邻接点集合。

定义 5 域间路由系统拟态联盟为 $U(v,e)$，盟外节点集合为 S，联盟中与 S 有直接连接关系的节点集合为 $\phi(S)$，对于 $\phi(S)$ 中的每一个节点对 (s,t)，其 k 条最短路径集合为 L_{st}^k。

由于遗传算法具有良好的全局搜索能力，可以快速搜索出空间中的全体解，因此采用遗传算法计算盟外节点 k 最短路径。算法流程为：

Step1 群体初始化，随机选择两个节点间的 n 条路径作为初始群体，对群体中的每个个体进行染色体编码；

Step2 对于群体中的每条染色体，分别计算适应度和选择概率；

Step3 按照 Step2 中计算的选择概率选择需要交叉操作的个体；

Step4 对需要交叉操作的个体根据交叉率进行交叉操作，根据变异率进行变异操作，产生世代更新；

Step5 按照评价标准对新产生的路径进行评价，决定是否接受；

Step6 根据染色体世代更新原则对子代群体进行操作；

Step7 判断是否选择出前 k 条最短路径，若选出，则算法终止，若达到终止条件，转 Step2。

根据算法流程，对其中的关键环节进行说明。

(1)染色体编码。利用节点编号对两点间的路径信息进行编号。以图 1 为例，节点 1 和节点 8 之间的一条路径可编

码为 1 2 5 3 8。由于不同的路径由不同的节点组成，因此将路径编码设置为变长形式。

(2)适应度函数。适应度函数主要用来描述染色体的适应度，在遗传算法的进化搜索中基本不利用外部信息，仅以适应度函数作为区分种群个体好坏的标准。适应度函数选择的好坏直接影响算法的优劣，好的适应度函数可以加快收敛速度，并能使算法跳出局部最优点。针对本问题的需要，引入路径适应度函数：

$$F=\frac{1}{\sum_{i=1}^{l} length(i)} \tag{1}$$

其中，l 表示经过的链路数，$length(i)$ 表示每条链路的权值，也即两个节点间的距离。从该函数可以看出，路径的权越小，距离越小，则其适应度越高。

每条路径的选择概率与适应度成比例，假设总的路径数目为 N，第 r 条路径的适应度为 f_r，则第 r 条路径被选中的概率为：

$$P_r=\frac{f_r}{\sum_{i=1}^{N} f_i} \tag{2}$$

这说明路径的适应度越大，则其被选中的概率越大。

(3)交叉操作。交叉操作即由一对父代染色体通过交换部分基因生成子代染色体。通过交叉操作，算法可以得到新一代个体(C)，这个新个体保留了部分父辈个体的特征。交叉操作可分为单点交叉、多点交叉和均匀交叉。本文采用单点交叉，交叉操作如下：例如染色体 $P_1=v_i,a_1,a_2,a_3,a_4,a_5,a_6,v_j$ 和染色体 $P_2=v_i,b_1,b_2,b_3,b_4,b_5,b_6,b_7,v_j$，进行交叉操作时，若选择的交叉位置在 P_1 的 a_3 处，则 P_1 的 a_3 以前的位置与 P_2 的 b_4 及其以后的基因组成新的染色体 C_1；同样，P_2 的 b_3 以前的位置与 P_1 的 a_4 及其以后的基因组成新的染色体 C_2。若 a_3 与 b_4 无连接，则依次向后搜索，若两者之间均没有连接基因，则这两条基因 P_1 和 P_2 交叉不成功，重新找两条染色体进行交叉。由于域间路由系统中不存在环路，因此交叉中出现的环路也应及时消除。本文采用覆盖法进行消除，直接将重复基因及其以后的全部基因整体向前移动到第一个重复位置，覆盖中间环路。例如，若发现染色体 $v_i,a_1,b_1,a_2,a_3,b_1,a_4,a_5,a_6,v_j$ 有环路，则利用覆盖法，覆盖后的染色体变为 $v_i,a_1,b_1,a_4,a_5,a_6,v_j$。

(4)变异操作。变异操作首先在群体中选择一个个体，对于选中的个体以变异概率随机改变染色体中某个基因块的值，改变成某一个或某一些等位基因块，形成新的染色体(M)。对于用路径表示的染色体，我们把连接节点组成的路径块视为基因块。以染色体 $P_1=v_i,a_1,a_2,a_3,a_4,a_5,a_6,v_j$ 为例，把 a_2,a_3,a_4,a_5 视为一个基因块，随机获取一条节点 a_2 到 a_5 的新路径 $a_2,b_1,\cdots,b_n,a_5$，实时变异操作后，染色体 P_1 变异为 $M_1=v_i,a_1,a_2,b_1,\cdots,b_n,a_5,a_6,v_j$。若在变异中出现环路问题，也可以采用覆盖法进行处理。

(5)交叉率 P_c 和变异率 P_m 的确定。交叉率和变异率对进化过程起着重要作用。P_c 确定新个体的产生速度，若取值过大则容易导致高适应度的个体被破坏，若取值过小则将导致搜索过程缓慢；P_m 决定新结构的产生的难易程度，若取值过大，则频繁产生新结构，算法变成随机搜索算法；若取值过小，将导致很难产生新结构。

本文采用以下算法对交叉率 P_c 和变异率 P_m 进行调整：

$$P_c=\begin{cases} P_{c1}-P_{c2}\dfrac{f_c-f_{avg}}{f_{\max}-f_{avg}}, & f_c\geqslant f_{avg} \\ P_{c1}, & f_c<f_{avg} \end{cases}$$
$$P_m=\begin{cases} P_{m1}-P_{m2}\dfrac{f_c-f_{avg}}{f_{\max}-f_{avg}}, & f_c\geqslant f_{avg} \\ P_{m1}, & f_c<f_{avg} \end{cases} \tag{3}$$

其中，$P_{c1}=0.85$，$P_{c2}=0.2$，$P_{m1}=0.01$，$P_{m2}=0.05$。P_c 为两个父代中适应度较大的一条路径；f_{avg} 表示每一代群体中的平均适应度值；$f_{\max}$ 标识每一代群体中适应度最大的一条路径。这种调整的好处在于当个体的适应度小于平均值时，采用较大的交叉率和变异率，以提高个体变优的概率；而当个体适应度较好时，采用较小的交叉率和变异率，便于保留优秀个体结构。

(6)新个体的接受准则。对于交叉和变异操作后出现的新个体，采用式(4)判断是否接受该新个体。

$$\xi=\begin{cases} 1, & f(i)\leqslant f(i_{new}) \\ \exp\{[(f(i)-f(i_{new}))*(1+\lambda)]/200\}, & f(i)>f(i_{new}) \end{cases} \tag{4}$$

其中，λ 表示迭代的次数。式(4)表明若子代新个体适应度变优，则安全地将其接收并作为新解；若子代新个体适应度变差，则以概率 ξ 接收。之所以以一定概率接收变差的子代新个体，主要是为了防止遗传算法容易早熟的问题。

(7)染色体的世代更新。遗传算法中，采用以下世代更新函数，$P'(t+1)=Rank(P(t),C(t),M(t))$，其中，$P(t)$ 为 t 时刻的种群染色体，$C(t)$ 为 t 时刻交叉操作后的染色体，$M(t)$ 为 t 时刻变异操作后的染色体，$P'(t+1)$ 为 $t+1$ 时刻经过排序优化选择后的新一代染色体。在世代更新时，若有相同的染色体，则进行排除。同时，如果产生的新一代群体中个体的最优适应度值小于父代，则利用父代的多个最优个体随机替代新一代群体中相应数量的适应度差的个体。

3.3　路径的随机化选取方法

定义 6　设 L_{ij} 为节点对$\langle v_i,v_j\rangle$之间的所有路径集合，其中 $v_i,v_j\in\phi(S)$，其中最短的 k 条路径的集合为 L_{ij}^k，在 L_{ij}^k 中按照从短到长的顺序对路径排序。

定义 7　在 AS 拟态联盟中，$\phi(S)$ 中任一节点对$\langle v_i,v_j\rangle$之间的一条实际路径 $l_{ij}\in L_{ij}^k$ 的最大有效期为 T_{expire}。

获取了 $\phi(S)$ 中节点间的 k 最短路径集合 L_k 后，路径随机化选取方法包括以下 3 个步骤：

Step1　从 $\phi(S)$ 中随机选取 n 个节点，形成 C_n^2 个节点对 $P_1,P_2,\cdots,P_{C_n^2}$。

Step2　对于每个节点对 $P_m=\langle v_i^m,v_j^m\rangle(1\leqslant m\leqslant C_n^2)$，利用随机数发生器 random(1,$k$)随机产生数字 $r(1\leqslant r\leqslant k)$，从 $L_{(ij)^m}^k$ 中选取第 r 条最短路径作为实际路径，形成 C_n^2 个节点之间的真实路径集合 $ReaLc_n^2$。$\phi(S)$ 中其他节点对之间选取最短路径。

Step3　$ReaLc_n^2$ 选取完毕后，计时器 T 从 0 开始计时，当 $T<T_{expire}$ 时，$ReaLc_n^2$ 保持有效；当 $T\geqslant T_{expire}$ 时，$ReaLc_n^2$ 全部

失效，返回 Step1，重新进行节点和路径的选取。

以图 2 为例，设 $n=k=3$，随机选取 1，8，9 之间最短的 3 条路径，如表 1 所列。在遇到安全威胁需要拓扑变换时，从每个节点对的最短的 3 条路径中随机选取一条作为通信路径；同时，设置定时器 $t=360$s，节点 1，8，9 的实际路径每隔 360s 就发生变化，让攻击者难以有效探测实际路径。

表 1 联盟边沿节点最短的 3 条路径

节点对	最短的 3 条路径
(1,8)	1 2 5 8
	1 4 3 8
	1 2 10 8
(1,9)	1 4 3 7 9
	1 4 6 7 9
	1 2 5 3 7 9
(8,9)	8 3 7 9
	8 5 4 6 7 9
	8 3 4 6 7 9

3.4 资源约束解决方法

定义 8 设在 t 时刻，路径 l_{ij} 上节点和链路的负载分别为 $Load_t(i)$，$Load_t(\rho_1)$，…，$Load_t(\rho_q)$，$Load_t(j)$ 和 $Load_t(i,\rho_1)$，$Load_t(\rho_1,\rho_2)$，…，$Load_t(\rho_q,j)$，其中 $\rho_1,\rho_2,\cdots,\rho_q$ 为实际路径 l_{ij} 上的顺序节点。

定义 9 $t+1$ 时刻，选取 l_{ij} 作为实际路径后，新加入 l_{ij} 的负载为 Δ。若同时满足：

$$\begin{cases} Load_t(i)+\Delta\leqslant F(i) \\ Load_t(\rho_1)+\Delta\leqslant F(\rho_1) \\ \cdots \\ Load_t(\rho_q)+\Delta\leqslant F(\rho_q) \\ Load_t(j)+\Delta\leqslant F(j) \end{cases} \& \begin{cases} Load_t(i,\rho_1)+\Delta\leqslant W(i,\rho_1) \\ Load_t(\rho_1,\rho_2)+\Delta\leqslant W(\rho_1,\rho_2) \\ \cdots \\ Load_t(\rho_q,j)+\Delta\leqslant W(\rho_q,j) \end{cases}$$

则说明选取 l_{ij} 作为实际路径不存在资源约束；若不能满足上述条件，则存在资源约束。

由于各个节点均有自身的最大转发量，链路也有最大负载能力约束条件，在域间路由系统中，各时段的突发流量也具有不确定性，如果在线路规划阶段进行资源规划，可能导致算法复杂度急剧增大，也难以满足资源的约束条件。因此在解决资源约束时，主要采用了请求-应答的方式：

请求：假设选取 l_{ij} 作为实际路径后存在资源约束，则 l_{ij} 上 $\exists v_\rho$ 或 $\exists e_{mn}$（$m\neq n$，且 m,n 均为路径 l_{ij} 上的相邻点），有 $F(\rho)<Load_{t+1}(\rho)$ 或 $W(m,n)<Load_{t+1}(m,n)$，这时由节点 ρ 或节点 m 向 AC 节点发出点减负请求 $Alleviate(l_{ij},\rho)$ 以及链路减负请求 $Alleviate(l_{ij},e_{mn})$。

应答：AC 收到 $Alleviate(l_{ij},\rho)$ 或 $Alleviate(l_{ij},e_{mn})$ 后，采取以下 3 个步骤进行应答：

Step1 对产生减负请求的这条 l_{ij} 的实际路径进行标记，然后从 $\overline{L_{ij}^k}=L_{ij}^k-\{l_{ij}\}$ 中再选取一条其他路径 l'_{ij} 作为真实路径。

Step2 若新路径再未收到新的减负请求，则使用新路径 l'_{ij}。若仍获取到新的减负请求且 $\overline{L_{ij}^k}\neq$null，则返回 Step1 继续选择符合资源约束条件的路径。

Step3 若 $\overline{L_{ij}^k}=$null，则说明单条路径已经无法满足资源约束，从 L_{ij}^k 选取两条路径 l'_{real1} 和 l'_{real2} 同时作为真实路径，继续监听是否存在资源约束的减负请求。若两条路径不能满足，则可以使用多条路径，直到满足条件为止。

以图 2 为例，当 AC 选择路径时，节点对(1,3)，(1,8)，(1,9)之间的通信流量均通过链路〈1,4〉，导致链路〈1,4〉拥塞，还可能导致节点 4 的转发负载超过其最大负载容量，这种情况下节点 4 可以向 AC 发送减负请求，AC 根据请求调整路径，如表 2 所列。若调整后导致链路〈1,2〉负载过大，AC 可以调整节点对(1,3)同时使用 1 4 3 和 1 2 5 3 两条路径通信。

表 2 资源约束调整

节点对	初始所用路径	调整后路径
(1,3)	1 4 3	1 2 5 3
(1,8)	1 4 3 8	1 2 5 8
(1,9)	1 4 3 7 9	1 4 3 7 9

4 实验验证及分析

为验证动态变换路径方法的有效性，采用了实际验证和模拟验证两种方式。实际验证利用已有的实验室网络，实际进行 BGP-LDoS 攻击以及路径变换，分析方法的有效性和对路由器产生的影响；模拟验证主要对互联网域间路由系统进行仿真实验，分析方法的抗攻击性。

4.1 联盟中单条链路抗 BGP-LDoS 攻击能力的验证

对于实际验证网络，利用 GNS3 搭建验证网络，网络环境如图 3 所示。共部署 11 个路由器，分别设置成不同的 AS 号。R_1-R_6 这 6 个路由器组成联盟，利用 R_6 作为联盟内部的 AC 节点。联盟设置为遭遇安全威胁的情况，最短路径数 $k=5$，即选择 5 条路径进行变换，变换定时器设置为 3 分钟。R_7-R_{10} 这 4 个路由器作为盟外节点，在联盟内部和盟外各设置若干个主机节点（Host）。各路由器之间的链路带宽的设置各不相同。各路由器的 KeepAlive 和 HoldTimer 也设置为非默认值，如表 3 所列。

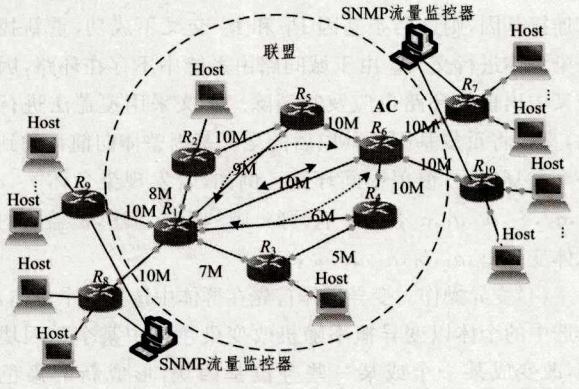

图 3 实验验证网络结构图

表 3 路由器参数设置

	MinRTO/ms	KeepAlive/s	HoldTimer/s
R_1	300	60	180
R_2	600	90	270
R_3	300	40	120
R_4	600	20	80
R_5	600	30	90
R_6	300	60	180

4.1.1 联盟内部无攻击节点条件下抗攻击能力分析

假设联盟内部无攻击节点，这时若对联盟内部的链路进

行攻击，则需要盟外攻击节点对联盟内部的目标链路信息进行分析。假设攻击者能够在盟外所有接口节点上部署监控设备，通过监控进出联盟的流量来分析链路和节点的参数信息。实验中在盟外的 4 个 AS 节点处均部署了 SNMP 流量监控器，模拟攻击者利用 SNMP MIB Browser 中的 tcpRtoMin 对象来探测链路〈R_1，R_6〉两端节点的 MinRTO，KeepAlive 和 HoldTimer 信息，使用 Iperf 工具模拟攻击者探测链路〈R_1，R_6〉带宽信息。每隔 5min 探测一次，共探测 10 次。结果如图 4－图 7 所示。

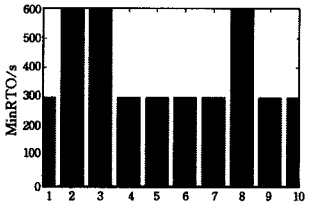

图 4　链路 MinRTO 参数探测结果

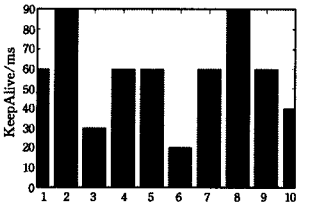

图 5　链路 KeepAlive 参数探测值

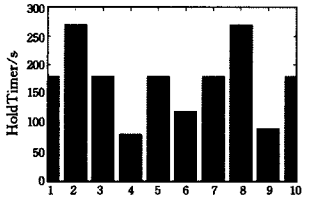

图 6　链路 HoldTimer 参数探测值

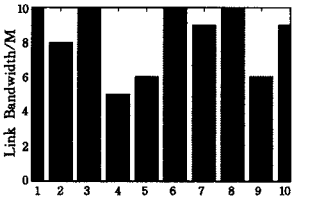

图 7　链路带宽探测值

可以看出，在联盟内无攻击节点的情况下，探测的结果与实际链路〈R_1，R_6〉的实际参数不一致，且多次探测的结果相差较大，这说明联盟干扰了攻击者对目标链路关键参数的探测。由于获取精确的链路参数是 BGP-LDoS 攻击成功的基础条件，因此节点联盟有效阻止了攻击的实施。

4.1.2　联盟内部有攻击节点条件下抗攻击能力分析

若联盟内部有攻击节点，假设攻击者获取了链路〈R_1，R_6〉带宽信息以及两端路由器的 MinRTO，KeepAlive 和 HoldTimer 信息，利用这些信息对链路进行攻击。实验中，攻击者攻击场景设置为 3 种：1）全部使用联盟内部攻击节点对联盟进行攻击；2）全部采用联盟外部攻击节点对联盟进行攻击；3）同时采用联盟外和联盟内攻击节点进行攻击。进行攻击时，脉冲强度 R 设置为 12M，攻击周期 T 设置为 300ms，脉冲长度 L 设置为 100ms，攻击带宽设置为 12M，每次攻击共持续 20min，共进行 10 次，记录攻击导致路由器 R_1 和 R_6 连接断开的次数，将联盟和未联盟时的结果进行对比，结果如图 8－图 10 所示。

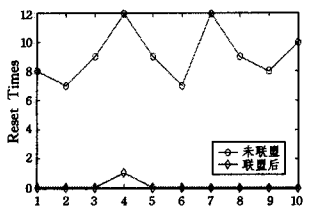

图 8　盟外节点攻击结果

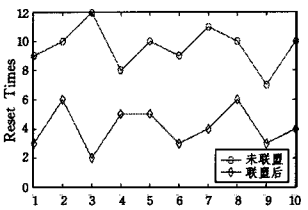

图 9　盟内节点攻击结果

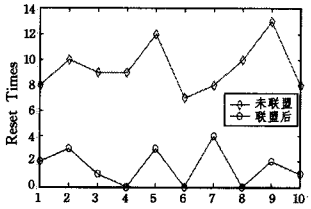

图 10　随机节点攻击结果

可以看出，攻击者即使获取了目标链路的信息，依然难以实施有效攻击。原因在于：对于盟外节点，由于实际路径不断变化其规划的途径链路〈R_1，R_6〉攻击流量并未实际经过链路〈R_1，R_6〉。同时，当链路〈R_1，R_6〉拥塞时，AC 通过 R_1 R_5 R_6 和 R_1 R_4 R_6 这两条次优路径进行分流，也减少了经过〈R_1，R_6〉的流量。对于盟内节点的攻击，AC 设置的随机路径同样可以分流，但 AC 主要计算了与盟外节点有连接关系的节点之间的最短 5 条路径，对其他节点之间的通信没有进行变换，因此防范盟内节点 BGP-LDoS 攻击的效果有待提高，但相比未结盟时，有效减少了攻击导致的连接断开次数。

4.2　多联盟中抗 BGP-LDoS 攻击分析

对于多联盟的抗 BGP-LDoS 攻击分析，我们选用实际互联网域间路由系统的数据进行模拟实验。实验设置 25000 个僵死节点作为攻击节点，采用 waledac[24] 建立分布模型。BGP-LDoS 攻击的流量和路径的规划与文献[4]相同。采用的域间路由系统数据是 CAIDA 2012 年 1 月提供的数据集[25]，其基本信息如表 4 所列。

表 4　数据集的基本信息

ASes	Links	Max degree	Min degree	Avg degree	Avg path length
27324	63268	3110	1	4.63	3.6

由于域间路由系统具有明显的社团性，社团内部节点的连接关系较为稠密，而不同社团之间的节点的连接关系稀疏，且同一社团的节点在地理位置上也较为接近，因此实验利用 Pajek 软件的 Louvain Method 方法将整个互联网系统划分为 52 个社团。每个社团作为一个联盟，在每个社团中选取度数最大的节点作为 AC 节点。在进行路径动态变换时分别设置 $k=3$，$k=5$，变换时间为 3min。每 5s 记录一次 AC 中的实际路径，为对比动态变换前和变换后对 BGP-LDoS 攻击的防护效果，实验采用与文献[3]相同的攻击方法进行对比验证。

4.2.1　平均路径长度变化

平均路径长度反映了拟态联盟在变换后传输效率的变化，由于实际路径会发生变化，在实验过程中每 3min 获取各个 AC 中的实际路径长度，以此分析未结盟时、$k=3$ 的结盟系统、$k=5$ 的结盟系统的实际平均路径的变换，进而分析这种结盟后的内部路径变换是否会导致传输效率降低。实验结果如图 11 所示。从图 11 中可以看出，在联盟之后，实际平均路径长度变化不大；$k=3$ 时，实际平均路径长度最大值为 3.75；$k=5$ 时，实际平均路径长度最大值为 4.18，与未结盟时的 3.6 相比，虽然有所增大，但增加并不明显。因此联盟内部的路径变换对域间路由系统的传输效率的影响不大。

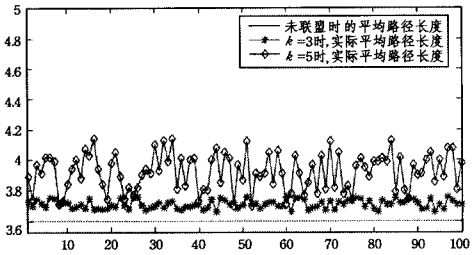

图 11 不同情况下平均路径长度的变化

4.2.2 各类链路与其他链路中断的比例

确保在攻击过程中使目标的链路会话中断,同时确保其他非目标链路畅通是 BGP-LDoS 攻击成功的重要保证。实验分析了未结盟时、$k=3$ 的结盟系统、$k=5$ 的结盟系统在遭遇攻击后各类链路失效的比例,如图 12 所示。

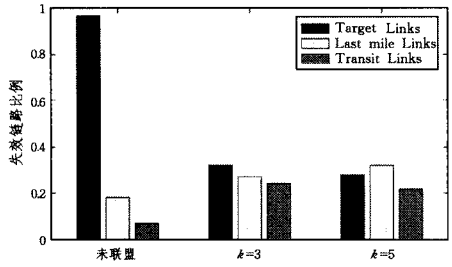

图 12 各类链路上 BGP 会话中断的比例

从图 12 可以看出由于实际通信路径发生变化,联盟能够有效干扰 BGP-LDoS 对目标链路的攻击,同时整个系统中链路失效的比例也将降低。部分目标链路仍然失效的主要原因是这部分目标链路位于联盟和联盟之间,BGP-LDoS 攻击主要利用了两个联盟内部的节点对目标链路进行攻击,因此导致其失效。

4.2.3 主要节点负载的比例

为进行对比分析,实验分析了域间路由系统中度数最大的、约占全部 AS 数量 10%的关键 AS 节点收到的路由更新报文的数量。结果如图 13—图 15 所示。

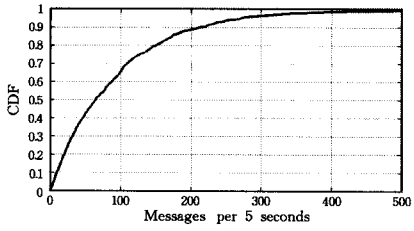

图 13 未受到 BGP-LDoS 攻击时的路由更新数量

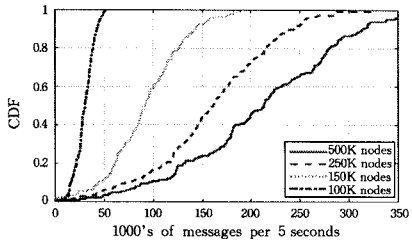

图 14 受到 BGP-LDoS 攻击时的路由更新数量(未进行拟态变换)

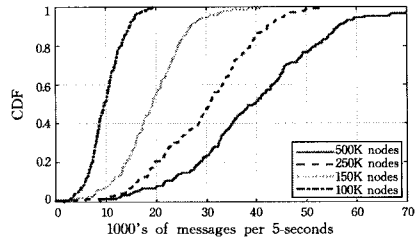

图 15 受到 BGP-LDoS 攻击时的路由更新数量(进行拟态变换后)

从图中可以看出,在未受到攻击时,这些关键 AS 节点中每 5s 收到的平均路由更新数量有 90%的概率在 200 条以下。当受到 BGP-LDoS 攻击后,节点未结盟时,关键节点收到的平均路由更新数量有了非常显著的增长,特别是使用 500K 攻击节点时,关键节点的平均路由更新数量有 90%的概率为 320 * 1000条,比未受到攻击时增长了 160000%。节点采用结盟策略后,即使在 500K 攻击节点攻击下,关键节点的平均路由更新数量有 90%的概率为 42 * 1000 条,比未受到攻击时仅增长了 2100%。这表明采用结盟防御的方法能够有效降低攻击的干扰,防止攻击效果的扩散。

4.2.4 几个关键 AS 的 bgp upadate 数据

度数较高的 AS 节点是域间路由系统的核心节点,实验对比分析了几个节点度数较高的 AS 关键节点 5s 内收到的路由更新数量,其中 AS 1299 的度数为 566,AS 4323 的度数为 587,AS 174 的度数为 1887,AS 3356 的度数为 2094。实验中,攻击节点的个数设置为 250K,$k=3$,分别获取 4 个节点在未联盟状态下和联盟状态下 5s 内的路由更新数量。结果如图 16—图 17 所示。

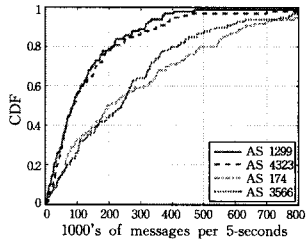

图 16 未联盟情况下关键 AS 受到 BGP-LDoS 攻击时的路由更新数量

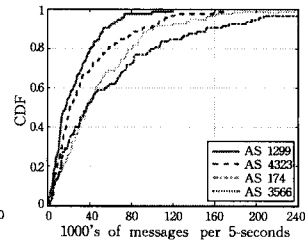

图 17 拟态变换后关键 AS 受到 BGP-LDoS 攻击时的路由更新数量

从图中可以看出,在联盟前后,这几个关键节点收到的路由更新数量有显著差异,联盟后的路由更新数量是联盟前的 10%,这充分说明了联盟能够有效降低 BGP-LDoS 攻击所产生的路由更新数量,从而使其攻击难以奏效。

结束语 随着互联网及信息安全技术的不断发展,域间路由系统面临日益严峻的安全威胁,尤其是近年出现的 BGP-LDoS 攻击,其技术的复杂度和可能造成的危害程度都要远大于传统网络攻击。已有的域间路由系统安全技术主要都是源于控制平面、基于异常路由的安全威胁而提出的,难以防御 BGP-LDoS 攻击这种源于数据平面、基于大规模流量的新型安全威胁。

为此,本文在分析 BGP-LDoS 攻击的基本原理和特点的基础上,针对 BGP-LDoS 攻击实施前需要精确的目标路径选取和规划这一前提条件,借鉴拟态安全防御思想,提出一种基于拟态联盟的拓扑变换方法。域间路由系统中的 AS 节点组

建安全联盟，联盟后内部推举 AC 作为控制节点，各联盟节点向 AC 通报并共享节点和链路的连接关系及转发能力和链路带宽等资源。AC 运用遗传算法获取盟外节点经过盟内的 k 条最优路径，而后根据安全威胁在联盟内部进行实际通信路径的随机变换。根据系统实施情况和盟内资源约束进行路径调整和分流。由于联盟对内显示实际路径改变，而对外显示路径保持不变，从而实现了对 BGP-LDoS 攻击的动态防御。实验结果表明，本文方法对 BGP-LDoS 攻击具有较强的防护能力，能够在不改变现有 BGP 协议的情况下实现对 BGP-LDoS 攻击的防护，且资源消耗较小，便于大规模部署。本文初步探讨了联盟拟态变换机制的可行性和有效性，未来将在此基础上进一步对实现的细节进行探讨和完善，对变换的成本和变换的同步问题进行深入研究。

参 考 文 献

[1] LI S, ZHUGE J W, LI X. Study on BGP security[J]. Chinese Journal of Software, 2013, 24(1): 121-138. (in Chinese)
黎松，诸葛建伟，李星. BGP 安全研究[J]. 软件学报，2013，24(1)：121-138.

[2] LI Q, ZHANG X, ZHANG X, et al. Invalidating idealized BGP security proposals and counter measures[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(3): 298-311.

[3] SCHUCHARD M, MOHAISEN A, FOO K D, et al. Losing control of the internet: using the data plane to attack the control plane[C]// Proceedings of the 17th ACM Conference on Computer and Communications Security. ACM, 2010: 726-728.

[4] LI H S, ZHU J H, QIU H, et al. The new threat to internet: DNP attack with the attacking flows strategizing technology [J]. International Journal of Communication Systems, 2015, 28(6): 1126-1139.

[5] ZHANG Y, MAO Z M, WANG J. Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing[C]// Proc of the Network and Distributed System Security Symposium (NDSS). 2007.

[6] KENT S, LYNN C, SEO K. Secure border gateway protocol (S-BGP)[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592.

[7] WHITE R. Securing BGP through secure origin BGP[J]. Internet Protocol Journal, 2003, 6(3): 15-22.

[8] OORSCHOT P C, WAN T, KRANAKIS E. On interdomain routing security and pretty secure BGP (psBGP)[J]. ACM Transactions on Information and System Security (TISSEC), 2007, 10(3): 11-25.

[9] SUBRAMANIAN L, ROTH V, STOICA I, et al. Listen and Whisper: Security Mechanisms for BGP[C]// Proceedings of 1th Symposium on Networked Systems Design and Implementation (NSDI'04). 2004: 127-140.

[10] LDA M, MASSEY D, PEI D, et al. PHAS: a prefix hijack alert system[C]// Proceedings of the 15th USENIX Security Symposium. Vancouver, Canada, 2006: 108-119.

[11] GOODELL G, AIELLO W, GRIFFIN T, et al. Working around BGP: An incremental approach to improving security and accuracy of inter-domain routing[C]// Proceedings of the ISOC NDSS. San Diego, US, 2003: 75-85.

[12] XU J, GUO, P, ZHAO M, et al. Comparing different moving target defense techniques[C]// Proceedings of the First ACM Workshop on Moving Target Defense. ACM, 2014: 97-107.

[13] CAI G L, WANG B S, WANG T Z, et al. Research and Development of Moving Target Defence Technology[J]. Journal of Computer Research and Development, 2016, 53(5): 968-987. (in Chinese)
蔡桂林，王宝生，王天佐，等. 移动目标防御技术研究进展[J]. 计算机研究与发展，2016，53(5)：968-987.

[14] WU J X. Meaning and Vision of Mimic Computing and Mimic Security Defence[J]. Telecommunication Science, 2014, 30(7): 2-7. (in Chinese)
邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学，2014，30(7)：2-7.

[15] MCCANEY K. Morphinator [EB/OL]. [2015-09-04]. http://gcn. com/articles/2012/08/03/army-mrohpinator-cyber-maneuver network defence. aspx.

[16] CHIRICESCU S, DEHON A, DEMANGE D, et al. SAFE: A clean-slate architecture for secure systems[C]// 2013 IEEE International Conference on Technologies for Homeland Security (HST). IEEE, 2013: 570-576.

[17] MUSLINER D J, RYE J M, THOMSEN D, et al. Fuzzbuster: Towards adaptive immunity from cyber threats[C]// 2011 Fifth IEEE Conference on Self-Adaptive and Self-Organizing Systems Workshops (SASOW). IEEE, 2011: 137-140.

[18] DARPA. Active cyber defense [EB/OL]. [2015-9-04]. http://www. darpa. mil/Our _ work/I2O/programs/Active-Cyber-Defence(ACD). aspx.

[19] ANTONATOS S, AKRITIDIS P, MARKATOS E P, et al. Defending against hitlist worms using network address space randomization[J]. Computer Networks, 2007, 51(12): 3471-3490.

[20] ZHAO X, TANG H B, WANG W B, et al. Moving target defense approach of HSS[J]. Computer Application Research, 2017, 34(1): 1-7. (in Chinese)
赵星，汤红波，王文博，等. 一种 HSS 移动目标防御方法[J]. 计算机应用研究. 2017，34(1)：1-7.

[21] DUNLOP M, GROAT S, URBANSKI W, et al. Mt6d: A moving target ipv6 defense[C]// Military Communications Conference (MILCOM 2011). IEEE, 2011: 1321-1326.

[22] MANADHATA P K, WING J M. A formal model for a system's attack surface[M]. Moving Target Defense. Springer New York, 2011: 1-28.

[23] ZHU Q, BAŞAR T. Game-theoretic approach to feedback-driven multi-stage moving target defense[C]// International Conference on Decision and Game Theory for Security. Springer International Publishing, 2013: 246-263.

[24] SINCLAIR G, NUNNERY C, KANG B B H. The waledac protocol: The how and why[C]// 2009 4th International Conference on Malicious and Unwanted Software (MALWARE). IEEE, 2009: 69-77.

[25] CAIDA. The IPv 4 Routed /24 AS Links Dataset [EB/OL]. [2015-9-04]. http://www. caida. org/data/active/ipv4_routed_topology_aslinks_dataset. xml.