doi:10.11959/j.issn.1000-436x.2017056

基于最优路径跳变的网络移动目标防御技术

雷程[1,2,3]，马多贺[2]，张红旗[1,3]，韩琦[4]，杨英杰[1,3]

(1. 解放军信息工程大学密码工程学院，河南 郑州 450001；2. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100093；
3. 河南省信息安全重点实验室，河南 郑州 450001；4. 哈尔滨工业大学信息对抗技术研究所，黑龙江 哈尔滨 150001)

摘 要：移动目标防御（MTD, moving target defense）是一种改变网络攻防对抗格局的技术，路径跳变则是该领域的研究热点之一。针对现有路径跳变技术，由于路径选取存在盲目性，跳变实施缺乏约束性，难以在保证网络性能的同时最大化防御收益等问题，提出基于最优路径跳变的网络移动目标防御技术。通过可满足性模理论形式化规约路径跳变所需满足的约束，以防止路径跳变引起的瞬态问题；通过基于安全容量矩阵的最优路径跳变生成方法选取最优跳变路径和跳变周期组合，以实现防御收益的最大化。理论与实验分析了该技术抵御被动监听攻击的成本和收益，证明其在保证网络性能的同时实现了跳变收益的最大化。

关键词：移动目标防御；路径跳变；可满足性模理论；瞬态问题；安全容量矩阵；防御收益最大化

中图分类号：TP393 **文献标识码**：A

Network moving target defense technique based on optimal forwarding path migration

LEI Cheng[1,2,3], MA Duo-he[2], ZHANG Hong-qi[1,3], HAN Qi[4], YANG Ying-jie[1,3]

(1. Cryptography Engineering Institute, PLA Information Engineering University, Zhengzhou 450001, China;
2. State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China;
3. Henan Key Laboratory of Information Security, Zhengzhou 450001, China;
4. Institute of Information Countermeasure Techniques, Harbin Institute of Technology, Harbin 150001, China)

Abstract: Moving target defense is a revolutionary technology which changes the situation of attack and defense. How to effectively achieve forwarding path mutation is one of the hotspot in this field. Since existing mechanisms are blindness and lack of constraints in the process of mutation, it is hard to maximize mutation defense benefit under the condition of good network quality of services. A novel of network moving target defense technique based on optimal forwarding path migration was proposed. Satisfiability modulo theory was adopted to formally describe the mutation constraints, so as to prevent transient problem. Optimization combination between routing path and mutation period was chosen by using optimal routing path generation method based on security capacity matrix so as to maximum defense benefit. Theoretical and experimental analysis show the defense cost and benefit in resisting passive sniffing attacks. The capability of achieving maximum defense benefit under the condition of ensuring network quality of service is proved.

Key words: moving target defense, forwarding path migration, satisfiability modulo theory, transient problem, security capacity matrix, defense benefit maximization

---

收稿日期：2016-10-31；**修回日期**：2017-02-05

通信作者：马多贺，maduohe@iie.ac.cn

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（No.2011CB311801）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2012AA012704, No.2015AA016106）；郑州市科技领军人才基金资助项目（No.131PLKRC644）；中国科学院先导专项基金资助项目（No.XDA06010701）；中国科学院信息工程研究所“青年之星”计划基金资助项目（No.118800808）；中国科学院重点部署专项基金资助项目（No.Y6X0061105）

Foundation Items: The National Basic Research Program of China (973 Program) (No.2011CB311801), The National High Technology Research and Development Program of China (863 Program) (No.2012AA012704, No.2015AA016106), Zhengzhou Science and Technology Talents Program (No.131PLKRC644), Strategic Priority Research Program of the Chinese Academy of Sciences (No.XDA06010701), Young Scientist Program of Institute of Information Engineering CAS (No.118800808), CAS Key Deployment Project (No.Y6X0061105)

1 引言

随着信息技术的飞速发展，网络安全愈加受到重视。然而，诸如 AS (autonomous system)前缀劫持、SWIFT 银行系统风波、2.7 亿 Gmail 和 Hotmail 账号遭泄露等互联网安全事件的频繁曝光，新型网络攻击方法不断涌现，网络安全面临严峻挑战。研究表明[1,2]，现有网络安全态势具有“易攻难守”的特点。首先，网络系统体系结构上存在固有安全缺陷，工程的安全性难以证明，设计的缺陷在所难免。攻击方可以利用网络系统漏洞的普遍存在性，不断发展新的攻击手段以增加已知威胁的破坏力、发掘新的漏洞以创造更具影响的未知威胁。防御方认知的局限性使基于先验知识的检测机制难以枚举可能的攻击手段、发掘目标网络中所有的漏洞。所以，攻防双方具有信息不对称的特性。其次，网络组成的确定性和结构的静态性为网络杀伤链的执行提供了所需的依存环境。攻击方可通过长期侦测和收集目标网络的配置信息和漏洞，进而安插后门实施控制；网络使用时间越长，挖掘网络漏洞的时间越多，后门更易于安插。防御方采用的封堵方法大多基于威胁特征或网络自身安全缺陷，而攻击方却变换利用已知威胁并创造性地利用未知威胁来实现攻防，这就造成防御方法永远滞后于攻击手段。所以，攻防双方具有时间不对称特性。此外，网络空间要素的单一性加剧了攻防态势的不平衡。攻击方只需要找到一个缺陷，就可以通过安装后门威胁整个网络系统。与此同时，利用相同的脆弱性可对不同网络节点发起多次攻击，从而以较低的成本获得较高的攻击收益。防御方则需要综合应用或部署防火墙、安全网关等设备实现杀毒灭马、封门堵漏，通过防御所有可能被利用的资源脆弱性，以提高系统的安全性。所以，攻防双方具有成本不对称的特性。综上所述，网络信息系统静态、确定、同构的体系结构和基于先验知识的安全防护体系在网络攻击趋向自动化、智能化的态势下，难以有效应对愈加复杂和智能的渗透式网络入侵，更加剧了网络攻防“易攻难守”的不对称困境。

为了缩小网络攻防的不对称差距，网络移动目标防御(network moving target defense)[3,4]应运而生。它以提供运行环境的随机、动态、异构为目标，通过多要素的主动变迁以破坏攻击链[5]对运行环境确定、静态、同构的依存要求，以阻断网络攻击的发生。由于转发路径作为网络攻击方面的有机组成部分和网络扫描的主要对象，成为了亟需被防护的重要网络属性，因此，路径跳变技术[6]就是其中关键技术之一。它通过动态改变通信双方的传输路径，以规避和防御攻击方的恶意监听，从而增加攻击探测的难度和成本，提高防御的效果和收益。

分析现有路径跳变技术研究主要存在以下问题。

1) 由于跳变路径的选取并未综合考虑路由节点和转发链路的性能约束，导致路径跳变过程出现瞬态问题[7]，降低了路径跳变的可用性。

2) 由于跳变路由节点和跳变周期选取的不合理，导致路径跳变的实施难以充分发挥其防御能力。

针对以上问题，本文提出了基于最优路径跳变的网络移动目标防御技术(OFPM, network moving target defense technique based on optimal forwarding path migration)。采用基于 SMT 的跳变约束，通过形式化描述转发路径要满足的约束，选取符合要求的路由节点和转发链路，防止跳变过程中产生瞬态问题，以提高路径跳变的可用性；提出基于安全容量矩阵的最优跳变路径生成方法，选取跳变路径和跳变周期的最优组合，以实现防御收益的最大化。

2 背景知识与相关工作

2.1 移动目标防御基本原理

移动目标的思想最早起源于古希腊的“隐豆戏法”[3]，它将豆子隐藏在 3 个杯子中的一个，通过不断变换杯子的位置，增加游戏参与者猜中豆子位置的难度。美国白宫国防安全委员会在 2010 年的研究进展报告[4]中明确指出：移动目标是通过在多个维度上移动以降低攻击方优势、增加防御弹性的系统。

移动目标防御是由移动目标的思想发展而来。2011 年，美国总统行政办公室国家科学与技术委员会发布的《可信网络空间：联邦网络空间安全研究与发展项目战略计划》[5]报告中将移动目标防御定义为一种通过创建、分析、评估和部署多样化、随时间持续变换的机制或策略，增加攻击方实施攻击的复杂度和成本，限制和降低系统脆弱性曝光程度和被攻击概率，提高系统弹性的防御手段。

移动目标防御的基本架构如图 1 所示，其基本工作原理如下。

1) 依据设定的安全目标制定网络系统的安全

策略和功能任务，并对网络资源进行初始化。

2) 依据安全策略选取跳变元素和跳变周期，通过跳变配置管理实现对网络系统的动态配置。

3) 下发跳变配置方案，将其部署到目标网络系统的相应节点中，以实施跳变。

4) 分析引擎，通过感知和分析当前网络系统的安全状态，将结果反馈给跳变触发机制。

5) 跳变触发机制通过分析当前网络安全状态与跳变实施效能，判断下一阶段的跳变策略。

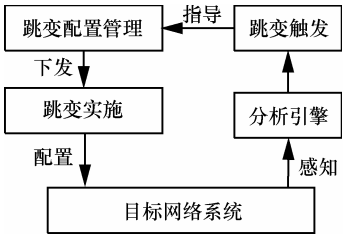

图 1　移动目标防御的基本架构

移动目标防御是通过提高系统的不确定性阻止网络威胁的主动防御技术。它通过增加网络组成的不确定性降低攻击扫描侦测的有效性，以缩小攻防双方的信息不对称；通过增加网络结构的动态性压缩攻击时限，以缩小攻防双方的时间不对称；通过增加网络要素的多样性提高攻击实施的成本，以缩小攻防双方成本的不对称。

2.2　路径跳变相关工作

现有路径跳变技术研究主要包含确定性多路径随机选择[6~9]和路由随机跳变[10~12]这 2 类。

1) 确定性多路径随机选择是预先获得尽可能多的路由节点不相交路径，从而在每次跳变时随机选取不同的转发路径以实现跳变的技术。Jafarian 等[6]提出了一种随机路由跳变方法(RRM, random route mutation)，通过可满足性模理论[13] (SMT, satisfiability modulo theory)形式化规约转发路径所需满足的限制条件，从而计算可选取的转发路径。该方法相较于静态网络中单路径转发可抵御约 90%的链路监听；文献[8]则在此基础上通过完全信息静态博弈对跳变周期进行最优选择，从而保证了跳变防御的持续有效；Dolev 等[9]则提出了基于 n–k 门限的多路径跳变方案，通过将一次会话中的数据流分为 n 份，仅允许少于 k 份的数据用相同路径转发，以防止数据传输过程中的被动监听。

2) 路由随机跳变则是通过预先获取所有符合要求的路由节点，从中随机选取下一跳路由节点进行数据流转发以实现跳变的技术。Shu 等[10]通过设计随机路由选取算法，实现无线网络中的数据安全传输；文献[11]则基于 2 种博弈模型计算从某一源节点到目的节点的多转发路径，并在此基础上随机选取跳变路由实现安全传输；Gillan 等[12]通过虚拟移动路由增加攻击方侦测难度，以抵御 DDoS 攻击。

3　路径跳变与最优路径跳变算法

路径跳变架构如图 2 所示，它通过多样、动态地改变路由部署与转发策略实现转发路径的动态切换，从而增加攻击方的攻击难度和代价，以提高抵御被动监听的能力。由于被动监听具有不可感知性，因此现有路径跳变机制主要采用自主式随机跳变的方法[6,12]。然而，由于自主式随机路径跳变在选取下一跳变周期的转发路径时仅依据事先设定的选取算法，而未能针对网络安全状态进行实时调整，从而难以在保证网络系统服务质量的同时完全发挥路径跳变的优势，在跳变防御有效性和跳变实施可用性上存在一定局限性。

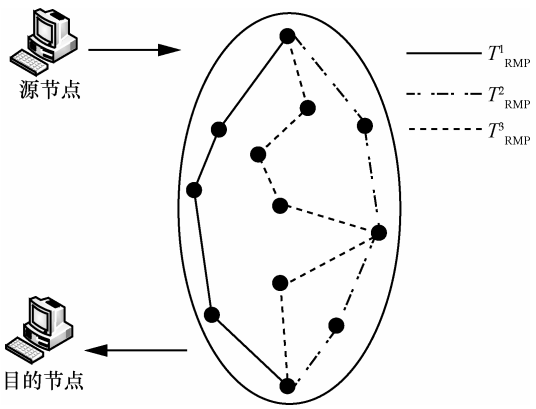

图 2　路径跳变架构

最优路径跳变算法在随机路径跳变的基础上依据软件定义网络(SDN, software defined network)的全局视图[14]和基于 SMT 的跳变约束对转发路径中路由节点和转发链路所需满足的性能约束进行形式化规约，以防止路径跳变过程中出现瞬态问题；与此同时，通过借鉴最大流—最小割[15]的思想，提出基于安全容量矩阵的最优跳变路径生成方法，选取跳变路径和跳变周期的最优组合，提高抵御被动监听的能力，以实现防御收益的最大化。OFPM 中所用符号具体含义如表 1 和表 2 所示。

表 1 OFPM 中的符号（变量）

符号	含义
T_{RMP}	OFPM 跳变周期
$b_v^{T_{\mathrm{RMP}}}(k)$	布尔变量，表示路由节点 v 在跳变周期 T_{RMP} 内是否转发第 k 条数据流
ML_e	跳变转发链路 e
MR_v	跳变路由节点 v
$C_v(k)$	路由节点承载数据流 k 时的边际成本
$C_e(k)$	转发链路承载数据流 k 时的边际成本
$\chi(MR_v)$	转发路径中去除源地址和目的地址所属路由后剩余的转发路由节点集合
d_{v-D}^k	当前路由节点 MR_v 到目标节点的距离
$sc_{S,D}$	从 S 到 D 实现安全转发的路由节点和转发链路的资源容量大小
$c_{S,D}$	S 到 D 间的最大剩余容量
$\omega^s{}_{S,D}$	安全系数
$\boldsymbol{Q}[sc_{S,D}]_{n\times n}$	从 S 到 D 的安全容量矩阵
σ	调整参数

表 2 OFPM 中的符号（常量）

符号	含义
C_v^{th}	路由节点需要保留的最小数据量
$C_v^{\max}$	路由节点可承载的累计边际成本最大值
C_e^{th}	转发链路需要保留的最小数据量
$C_e^{\max}$	转发链路可承载的累计边际成本最大值
$L_{\max}$	设定的最大转发路径长度

3.1 基于 SMT 的跳变约束

瞬态问题[16,17]是跳变过程中网络性能急速下降的现象，它会导致分组乱序和分组丢失概率的增加。其中，分组乱序的产生是由于跳变路径迁移造成的转发数据分组序列错乱；分组丢失则是由于转发节点和链路容量不足、转发路径不可达，以及流表更新不一致引起。此外，由于分组乱序和分组丢失会进而触发 TCP 重传机制，在实施路径跳变的网络中会造成 TCP 性能的恶化，导致路径跳变的可用性降低。为了保证网络服务质量，提高跳变实施的可用性，OFPM 采用基于 SMT 的跳变约束，从转发路径容量、传输时延和可达性 3 个方面形式化规约跳变路径所需满足的约束条件；结合“逆序添加，顺序删除”的流表更新方法，以防止由于跳变路径切换引发的瞬态问题。

路径跳变中网络资源容量[16]是指网络系统中路由节点和转发链路的剩余可用资源量。其中，路由节点的剩余可用资源量主要取决于剩余可用的流表项，这是因为路由节点的 CPU 消耗、存储剩余量等与流表项大小正相关[17]；转发链路的剩余可用资源量则主要取决于剩余的可用带宽。由于实际网络环境具有多流交汇的特点，因此路由节点和转发链路的开销是指某一时刻所有经过该路由或链路的数据流所需成本的累加和。布尔变量 $b_v^{T_{\mathrm{RMP}}}(k)$ 表示路由节点 v 在跳变周期 T_{RMP} 内是否转发第 k 条数据流，若转发，则 $b_v^{T_{\mathrm{RMP}}}(k)=1$；否则，$b_v^{T_{\mathrm{RMP}}}(k)=0$。类似地，$b_e^{T_{\mathrm{RMP}}}(k)$ 表示转发链路 e 在跳变周期 T_{RMP} 内是否传输第 k 条数据流，若数据流经该链路，则 $b_e^{T_{\mathrm{RMP}}}(k)=1$；否则，$b_e^{T_{\mathrm{RMP}}}(k)=0$。跳变路径所需满足的约束具体如下。

1) 转发路径容量约束。该约束通过选取可承载累计流表大小的路由节点和可承载累计转发数据流量的转发链路，以防止由于数据溢出造成的丢失分组问题，具体如式(1)~式(4)所示。

$$c_v(k)=C_v(\sigma^{1-\frac{C_v(k)}{C_v}}-1) \tag{1}$$

$\forall MR_i$，若 $C_v^{\max}-\sum_{i=1}^{k}b_v^{T_{\mathrm{RMP}}}(i)c_v(i)\geqslant C_v^{\mathrm{th}}$，则

$$b_v^{T_{\mathrm{RMP}}}(i)=1 \tag{2}$$

$$c_e(k)=C_e(\sigma^{1-\frac{C_e(k)}{C_e}}-1) \tag{3}$$

$\forall ML_e$，$C_e^{\max}-\sum_{i=1}^{k}b_e^{T_{\mathrm{RMP}}}(i)c_e(i)\geqslant C_e^{\mathrm{th}}$，则

$$b_e^{T_{\mathrm{RMP}}}(i)=1 \tag{4}$$

基于边际成本的指数函数被广泛用于量化不同条件下网络资源性能消耗的指标，如单播或多播时路由节点及转发路径的性能消耗等[18,19]，因此 OFPM 采用基于边际成本的指数函数量化路由节点和转发链路的资源开销。式(1)表示添加一条新的流表项所需的边际成本函数 $c_v(k)$。其中，C_v 表示流表中剩余流表项数量，σ 为调整参数，经过理论[20]分析设定参数值为 $\sigma=2n$，n 为网络路由节点数量；$1-\frac{c_v(k)}{C_v}$ 表示当第 k 条数据流的转发信息添加到路由节点 v 后流表的利用率。式(2)说明流表累计增加的边际成本必须在所选路由节点可承载范围 $C_v^{\max}$ 之内，且剩余的流表长度不小于 C_v^{th} 从而不会出现数据溢出等问题。类似于式(1)、式(3)表示转发一条

数据流所需的边际成本。其中 $1-\frac{c_e(k)}{C_e}$ 表示当第 k 条数据流经转发路径 e 后带宽的利用率。式(4)说明累计带宽消耗的边际成本必须在所选转发链路可承载的范围 $C_e^{\max}$ 之内，且剩余的带宽不小于 C_e^{th} 使转发链路具有剩余能力处理由于负载均衡和网络抖动等引起的数据波动。其中，C_e^{th} 表示转发链路 ML_e 需要保留的最小数据量。

2) 转发路径时延约束。该约束通过选取总传输时延符合条件，且跳变路径时延差小于分组间时延(inter-packet delay) 的转发路径，以防止跳变过程中产生的分组乱序问题，具体如式(5)和式(6)所示。

$$\sum b_v^{T_{\text{RMP}}}(k) \leqslant L_{\max},\quad MR_v \in \{MR_S, MR_1, \cdots, MR_D\} \tag{5}$$

若 $\{L_{T_{\text{RMP}}+1} | (t(i+1,k)-t(i,k)) > \max[D(L_{T_{\text{RMP}}})] - \min[D(L_{T_{\text{RMP}}+1})]\}$，则 $b_L^{T_{\text{RMP}}+1}(k)=1$ (6)

式(5)表示每条数据流的转发路径长度不能超过设定的最大值 $L_{\max}$。由于传输时延与转发路径中路由节点个数正相关[21]，因此通过限定转发路径长度防止传输时延过大导致的网络服务质量下降。与此同时，在转发路径迁移之前，OFPM 通过环回时间[22](round trip time)度量备选的下一跳变周期转发路径 $L_{T_{\text{RMP}}+1}$ 中最小传输时延与现有转发路径 $L_{T_{\text{RMP}}}$ 中的最大传输时延，并利用式(6)判断 $L_{T_{\text{RMP}}+1}$ 中最小传输时延与 $L_{T_{\text{RMP}}}$ 中的最大传输时延之差是否小于平均分组间时延，从而防止路径迁移过程中由于转发路径时延差过大造成的额外分组乱序问题，具体证明见第 3.2 节。OFPM 通过转发路径时延约束保证相邻跳变周期内转发路径迁移时不会额外产生分组乱序问题。

3) 转发路径可达性约束。该约束通过限制对转发路由节点的选取，以防止转发回路的出现，以及由此引发的分组丢失问题，具体如式(7)~式(9)所示。

$$b_S^{T_{\text{RMP}}}(k)=1,\quad b_D^{T_{\text{RMP}}}(k)=1,\quad \sum_{i\in I} b_i^k = \sum_{o\in O} b_o^k \tag{7}$$

若 $b_v^{T_{\text{RMP}}}(k)=1$，则 $\forall MR_v \in \chi(MR_v)$，$\sum b_v^{T_{\text{RMP}}}(k)=2$ (8)

若 $\forall MR_v \in \{MR | MR_{v-1}\text{的下一跳}\}$，则 $d_{v-D}^k \leqslant d_{(v-1)-D}^k$ (9)

式(7)表示在该条转发路径上，所有路由节点的入度和出度是相同的。式(8)表示路径中的每个转发路由节点都与其上一跳和下一跳路由节点是物理邻接的。其中，$\chi(MR_v)$ 表示转发路径中去除源地址和目的地址所属路由后剩余的转发路由节点集合。然而，将数据流从一个节点转发到其相邻的下一跳节点并不能保证数据的可达。因此，式(9)对转发节点与目标路由节点间的距离进行了约束。它表示下一跳路由节点到目标节点的距离不大于现有转发节点到目标路由节点的距离，其中，d_{v-D}^k 表示 MR_v 到目标节点的距离。式(9)保证了数据流在到达目标路由节点后将不会再被转发。

尽管可满足性解问题现在依然是 N-P 问题，但是现有如 Z3[13]等 SMT 求解器的规模已经达到百万数量级以上，可有效用于求解满足条件的跳变路径集合。

3.2　基于安全容量矩阵的最优跳变路径生成

最优跳变路径生成方法依据最大流—最小割理论，选取最优跳变路径和跳变周期组合，以提高抵御被动监听的能力，实现跳变防御收益的最大化。由于攻击方会对路由节点和转发链路进行恶意监听，而现有网络资源容量未将安全性考虑在内。因此，即使路由节点和转发链路满足 3.1 节中的跳变约束，其可用性会随着安全风险的增加而降低。OFPM 基于网络资源容量矩阵[16,17]的概念，定义了网络安全容量矩阵；在此基础上利用最大流—最小割理论选取最优跳变路径和跳变周期组合，以实现路径跳变的收益最大化。

实际网络可用有向图 $G(N, L)$ 表示，其中，N 是节点集合，它表示软件定义网络中的跳变路由节点集合 $\{MR_v\}$；L 是有向边集合，表示转发链路集合 $\{ML_v\}$。若对图 $G(N, L)$ 中任意的源节点 S 和目的节点 D，有 $\{MR_S, ML_1, \cdots, MR_i, ML_i, \cdots, MR_D\}$，则记为图 G 中从 S 到 D 的一条转发路径 $L_{T_{\text{RMP}}}$。

定义 1　给定一个网络 $G(N, L)$，它可以表示为加权有向图 $\vec{G}(N, L, W)$。其中，$W=\{C, B\}$，C 表示路由节点的安全容量，B 表示转发链路的安全带宽。

网络安全容量矩阵是基于 $\vec{G}(N, L, W)$ 生成的 $\boldsymbol{Q}[sc_{S,D}]_{n\times n}$，其中，$n=|N|$ 表示网络转发路由节点数量；$sc_{S,D}$ 表示任意地从源节点 $S\in N$ 到目的节点 $D\in N$ 可实现安全转发的路由节点和转发链路的资源容量大小。如式(10)所示，它由 *S-D* 间的最大剩余容量 $c_{S,D}$ [16]与安全系数 $\omega^s{}_{S,D}$ 共同组成。$c_{S,D}$ 可通过实时在线获取的网络状态信息基础上计算得到。$\omega^s{}_{S,D}$ 如式(11)所示，它是由攻击方采取的监听

策略和防御方采取的跳变策略共同决定的：攻击方通过采用不同监听策略 $a\in A$ 以实现攻击收益的最大化，即最小化 $\omega^s{}_{S,D}$；防御方则通过选取不同的跳变策略 $d\in D$ 以最大化跳变防御的收益，即实现 $\omega^s{}_{S,D}$ 的最大化。因此，$\omega^s{}_{S,D}$ 与时间 T 内攻击方的监听次数为 $R_A=\dfrac{T}{r_A}$、跳变的次数为 $R_D=\dfrac{T}{T_{\mathrm{RMP}}}$、攻击方监听第 j 条链路的概率 P_j^a 和数据分组经过第 j 条链路的概率 $P_{j\cdot}$ 有关。

$$sc_{S,D}=c_{S,D}\omega^s{}_{S,D} \tag{10}$$

$$\omega^s{}_{S,D}=1-\min_{d\in D}\max_{a\in A}\sum_{l_j\in L_+} f\left(\frac{R_A}{R_D}P_j^aP_{j\cdot}\right) \tag{11}$$

OFPM 在安全容量矩阵的基础上通过计算跳变路径和跳变周期的最优组合以实现 $sc_{S,D}$ 的最大化。具体流程如算法 1 所示。

算法 1 最优路径迁移和跳变周期组合生成算法

1) 初始化最优转发路径和跳变周期组合队列 Q;

2) 构建无向图 G 的广度优先搜索树; //以源节点所属的 MR_S 为根节点；以 MR_i 到 MR_S 的距离为依据进行降序排列，并将到 MR_S 距离的放在同一级

3) 对 MR_i、ML_i 进行观测和排序，其中，$i\in[1,n]$；

4) 利用可满足性模理论求解器选择符合约束条件的 MR 和 ML 集合; //依据式(1)~式(4)

5) 计算最小割树; //获得 $c_{S,D}$ 的最大流

6) 将无向图 G 转换为加权有向图 $\vec{G}$；

7) 获得 $f^s{}_{S,D}$ 的最大流；

8) 将 $f^s{}_{S,D}$ 转化为 $\omega^s{}_{S,D}$ // 依据定理 1

9) 构建安全容量矩阵 $\boldsymbol{Q}[sc_{S,D}]_{n\times n}$；

10) for each $MR_i\in\{MR_i\}$ do

11) if $i=1$ then

12) 选取 MR_S；

13) else

14) 选取与 $MR_{i\text{-}1}$ 物理邻接的转发路由节点集合 $\{MR_i\}'$; //依据式(7)~式(9)

15) end if

16) end for;

17) 选取满足转发路径时延约束的转发路径; //式(5)和式(6)

18) 将符合约束条件的备选转发路径和跳变周期组合加入到队列 Q 中；

19) 对 $sc_{S,D}$ 中备选转发路径和跳变周期组合进行降序排序；

20) 将排名最高的作为下一周期的迁移路径；

21) return 最优迁移路径和跳变周期；

基于安全容量矩阵的最优跳变路径生成方法首先利用广度优先搜索算法(BFS, breadth-first searching)对跳变路由节点进行遍历，并选取满足转发路径容量约束条件的路由节点与转发链路集合步骤 2)~步骤 4)；其次，利用 Hao-Orlin 等[23]算法得到从 S 到 D 上 $c_{S,D}$ 的最大流问题(步骤 5))；计算 $f^s{}_{S,D}$ 的最大流，并依据定理 1 进行转换为 $\omega^s{}_{S,D}$ (步骤 6)~步骤 8))；在此基础上，构建由 S 到 D 的安全资源容量矩阵(步骤 9))；利用转发路径时延约束和可达性约束对安全资源容量矩阵中可能的转发路径进行过滤(步骤 10)~步骤 18))；最后，对满足约束的跳变路径和跳变周期组合进行排序(步骤 19)和步骤 20))，并返回最优跳变路径和跳变周期组合(步骤 21))，从而保证跳变防御收益的最大化。

此外，假设网络中顶点数量为 n，链路数量为 m。在最优路径选取算法中，构建广度优先搜索树的计算复杂度为 $O[\mathrm{lb}(n)]$；Z3 SMT 求解器由于使用了 congruence-closure 算法，其计算复杂度为 $O[(n+m)\mathrm{lb}(n+m)]$；文献[24]算法的计算复杂度为 $O\left[nm\mathrm{lb}\left(\dfrac{n^2}{m}\right)\right]$。因此，OFPM 的计算复杂度为 $O\left[nm\mathrm{lb}\left(\dfrac{n^2}{m}\right)\right]$。

定理 1 给定一个加权有向图 $\vec{G}(N,L,W)$，$1-\omega^s{}_{S,D}$ 的值等于 $\vec{G}$ 中任意 $l_j\in L_+$ 在约束条件为 $W(l_j)=\dfrac{1}{P_j^a}$ 下 S-D 最大流的倒数。

证明 由式(11)可知，在跳变周期和跳变路径确定的情况下，即 $d\in D$ 确定，$1-\omega^s{}_{S,D}$ 与被动监听方法 a 的选取线性相关。因此，$1-\omega^s{}_{S,D}$ 可表示为 $\min\limits_{a\in A,\,d}\sum\limits_{l_j\in L_+}\lambda$，其中 $\lambda\geqslant P_j^aP_{j\cdot}$。

令 $\overline{\lambda}=\dfrac{1}{\lambda}$，则 $f^s{}_{S,D}=\dfrac{1}{1-\omega^s{}_{S,D}}$，且 $f^s{}_{S,D}=\max\overline{\lambda}$，则 $\dfrac{1}{1-\omega^s{}_{S,D}}$ 如式(12)所示。它表示 $\vec{G}$ 中任意 $l_j\in L_+$ 在 $\overline{\lambda}_{P_{j\cdot}}\leqslant\dfrac{1}{P_j^a}$ 约束条件下 S-D 的最大流问题。

$$\frac{1}{1-\omega^{s}_{S,D}}=\max_{\substack{a\in A,d\\ \bar{\lambda}P_{j\cdot}\leqslant\frac{1}{P_j^a}}}\bar{\lambda} \tag{12}$$

由此可知，对$1-\omega^{s}_{S,D}$的求解可以转化为在约束条件为$W(l_j)=\frac{1}{P_j^a}$下的*S-D*最大流问题，证毕。

4　基于 SDN 的 OFPM 架构设计与实施

4.1　基于 SDN 的 OFPM 架构设计

由于 SDN 架构[24]具有控制平面与数据平面相分离的特性，且控制平面可对网络设备集中管理，精确定义底层设备对数据分组的转发；数据平面则具有可编程特点，实现了对底层设备网络行为变化的灵活控制。因此，OFPM 依托 SDN 全网视图和集中控制的特性，进行路径跳变决策和部署。整体架构如图 3 所示，它通过跳变路由(MR, mutation router)和跳变控制器(RC, randomization controller)实施协同跳变。RC 主要由跳变路由管理、路径跳变决策和跳变路径实施 3 部分组成。跳变路由管理通过南向接口，利用如 OpenFlow 协议等监测和控制整个网络。它通过收集的网络路由节点状态以及网络拓扑等信息，依据路由节点和转发路径要满足的约束构建符合约束条件的跳变路由集合。路径跳变决策的主要作用是利用基于安全容量矩阵的最优跳变路径生成方法选取最优跳变路径和跳变周期组合。跳变路由实施则依据选取的跳变路径进行流表部署下发，以更新选取的跳变路由配置。管理员可以通过定义静态流表项的优先级以实现路由选择和路径迁移。MR 的主要作用是依据流表对通信数据流进行修改和转发，将不能匹配流表的数据分组以及 ARP、ICMP、DNS、DHCP 等协议的数据分组转发到 RC 中处理；收集和过滤网络拓扑和路由节点状态等信息并定期上报给 RC。

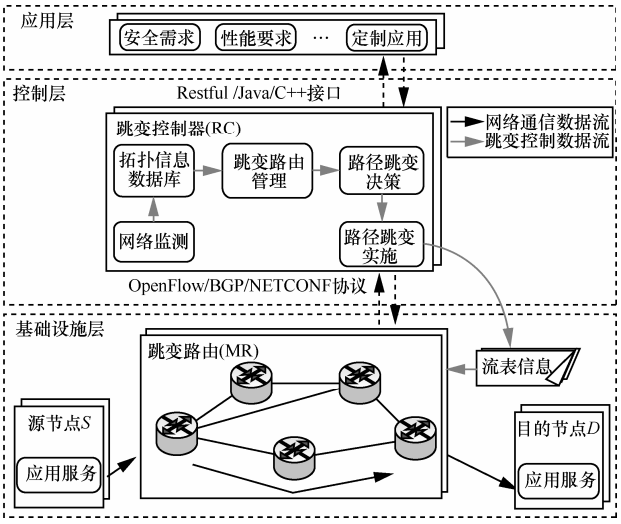

图 3　基于 SDN 的 OFPM 整体架构

4.2　OFPM 的工作流程

OFPM 架构基本工作流程如下。

1) RC 首先使用链路层发现协议(LLDP, link layer discovery protocol)获取全局网络拓扑；在此基础上通过端口状态请求消息(PSQ, port state request message)定时获取网络中跳变路由的状态信息。

2) MR 在收到 PSQ 消息后反馈端口状态回复消息(PSR, port state reply message)，以将其状态信息上报给 RC。

3) RC 中的跳变路由管理模块基于 SMT 形式化规约跳变路由要满足的条件，并依据网络拓扑和路由状态等信息构建符合约束条件的跳变路由集合。

4) RC 中的路径跳变决策模块采用基于安全容量矩阵的最优跳变路径生成方法选取最优的跳变路径和跳变周期组合。

5) RC 中的路径跳变实施模块依据路径跳变决策的结果通过流表的 *Modify-State* 消息配置跳变路由，并依据跳变周期设定 *idle_time* 值。

此外，由于路径跳变更新需要将新的流表信息下发并配置到多个 MR 上，流表更新过程易产生流表配置不一致的问题。因此，OFPM 路径跳变更新过程采用逆序添加、顺序删除的更新方式。

5　理论分析

5.1　跳变效果分析

假设在一段时间T内传输的数据流为 f，则每个跳变周期内传输的数据流为$\frac{f}{R_D}$；攻击方监听的网络节点集合V_R中监听数量为r，$r<n$；源节点S和目标节点D间的转发节点集合V_T中有s个节点；攻击方成功监听某条数据流的概率是独立分布，成功率$x=P_j^aP_{j\cdot}$。

1) 在$R_A\leqslant R_D$时，攻击方被动监听的成功率服从伯努利分布$B(R_A,x)$。成功监听的数据流为$fx\frac{R_A}{R_D}$。

2) 当 $R_A > R_D$ 时，攻击方恶意监听的成功率服从伯努利分布 $B(R_A, x)$，但是由于在 $R_A > R_D$ 条件下攻击方的监听频率更快，因此在每个跳变周期内，攻击方可进行 $z = \left\lceil \frac{R_A}{R_D} \right\rceil$ 次的监听，它服从几何分布 $G(x)$，即攻击方在某一次攻击中成功监听某个路由节点，那么在该跳变周期内的剩余几次监听中，攻击方都可以成功监听该路由节点中的数据流。由此可知，攻击方成功监听的数据流为 $f\sum_{k=1}^{z}\frac{x(1-x)^{k-1}[z-(k-1)]}{z}$。

在静态网络中，由于没有路由跳变，因此可认为 $z = R_A$。攻击方成功监听 S 到 D 间数据流的概率为 $f\sum_{k=1}^{R_A}\frac{x(1-x)^{k-1}[R_A-(k-1)]}{R_A}$，其中，攻击方成功监听第 j 条链路的概率为 $P_j^a = \frac{(\mathrm{C}_n^r - \mathrm{C}_{n-s}^r)}{\mathrm{C}_n^r}$。

在 RRM[6]网络中，当 $MR_S \in V_R$ 或者 $MR_D \in V_R$ 时，攻击方可监听从 S 到 D 的传输路径，则有 $\mathrm{C}_2^1\mathrm{C}_{n-2}^{r-1} + \mathrm{C}_2^2\mathrm{C}_{n-2}^{r-2}$；当 $MR_S \notin V_R$ 且 $MR_D \notin V_R$ 时，当且仅当 G 中 S 到 D 的路由节点可被割集 V_C 分割在 x 个相互连接的子图 $G_1, G_2, \cdots, G_x$ 中时，即 $V_C \subseteq V_R$，攻击方可监听从 S 到 D 的传输路径。若符合要求的 V_R 数量为 n_{V_R}，则 $P_j^a = \frac{(\mathrm{C}_2^1\mathrm{C}_{n-2}^{r-1} + \mathrm{C}_2^2\mathrm{C}_{n-2}^{r-2} + n_{V_R})}{\mathrm{C}_n^r}$。由于 RRM 采用了固定的跳变周期，因此，攻击方成功监听数据流的概率可表示为 $\min(R_A, R_D)p_{\min(R_A,R_D)} \cdot f\sum_{k=1}^{z}\frac{x(1-x)^{k-1}[z-(k-1)]}{zR_D}$，其中，$p_{\min(R_A,R_D)}$ 表示 $R_A \leqslant R_D$ 或 $R_A > R_D$ 发生的概率。

类似地，在 OFPM 网络中，攻击方成功监听从 S 到 D 传输路径的概率为 $P_j^a = \frac{(\mathrm{C}_2^1\mathrm{C}_{n-2}^{r-1} + \mathrm{C}_2^2\mathrm{C}_{n-2}^{r-2} + n_{V_R})}{\mathrm{C}_n^r}$。由于 OFPM 基于安全容量矩阵获得最优跳变路径和跳变周期组合，因此可依据攻击方扫描频率的改变而调整跳变周期，攻击方监听数据流的成功率为 $fx\frac{R_A}{R_D}$。

综上所述，相较于静态网络和 RRM 网络，OFPM 有效降低了被动监听的成功率。

5.2 性能分析

由 3.1 节可知，跳变路径迁移引发的分组乱序是产生性能消耗的原因[25]，它降低了路径跳变的可用性。因此，定理 2 证明了 OFPM 通过增加转发路径时延约束，可有效防止由于跳变路径迁移而引起的分组乱序。

定理 2 $\{L_{T_{\mathrm{RMP}}+1} | (t(i+1,k) - t(i,k)) > \max[D(L_{T_{\mathrm{RMP}}})] - \min[D(L_{T_{\mathrm{RMP}}+1})]\}$ 保证了 OFPM 跳变过程中不发生分组乱序。

证明 从源节点 S 到目的节点 D 的传输路径中，假设第 t 个跳变周期内的传输路径路由为 $L_{T_{\mathrm{RMP}}}$；第 t+1 个跳变周期内的传输路径路由为 $L_{T_{\mathrm{RMP}}+1}$。由于选择的下一周期的跳变路径满足 $\{L_{T_{\mathrm{RMP}}+1} | (t(i+1,\ k) - t(i,k)) > \max[D(L_{T_{\mathrm{RMP}}})] - \min[D(L_{T_{\mathrm{RMP}}+1})]\}$，则对于任意的数据流 f_k，必然有 $D(f_k^{T_{\mathrm{RMP}}}) \geqslant \min[D(L_{T_{\mathrm{RMP}}})]$ 成立。

假设数据流 f_k 的数据分组 x_i 从传输路径 $L_{T_{\mathrm{RMP}}}$ 上转发；数据分组 x_{i+1} 从路径 $L_{T_{\mathrm{RMP}}+1}$ 上转发，且 $\Delta t = t(i+1,k) - t(i,k)$。

1) 当 $\max[D(L_{T_{\mathrm{RMP}}})] = D(f_k^{T_{\mathrm{RMP}}})$ 时，数据分组 x_i 在传输路径 $L_{T_{\mathrm{RMP}}}$ 的最大时延满足 $\max[D(f_k^{T_{\mathrm{RMP}}})] < \min[D(L_{T_{\mathrm{RMP}}+1})] + \Delta t$；

2) 当 $\max[D(L_{T_{\mathrm{RMP}}})] > D(f_k^{T_{\mathrm{RMP}}})$ 时，数据分组 x_i 在传输路径 $L_{T_{\mathrm{RMP}}}$ 的最大时延依然满足 $\max[D(f_k^{T_{\mathrm{RMP}}})] < \min[D(L_{T_{\mathrm{RMP}}+1})] + \Delta t$。

已知 $\min[D(L_{T_{\mathrm{RMP}}+1})] \leqslant D(f_k^{T_{\mathrm{RMP}}+1})$ 成立，且由 1)和 2)可知，条件 $\max[D(f_k^{T_{\mathrm{RMP}}})] < D(f_k^{T_{\mathrm{RMP}}+1}) + \Delta t$ 成立。因此，在路径跳变过程中，任意的数据流都不会额外产生分组乱序，证毕。

与此同时，由于流表更新过程易造成流表配置不一致，导致部分转发数据分组出现错误而被丢弃。OFPM 通过采用“逆序添加，顺序删除”更新方式降低流表更新过程中出现的分组丢失问题。“逆序添加”是指跳变控制器按照从目的节点到源节点的逆序方向对跳变路径上的路由节点安装流表信息；“顺序删除”则是指跳变控制器按照从源节点到目的节点的顺序方向删除旧的流表规则。定理 3 将所有转发节点进行了分类，证明了该流表更新方式可有效保证流表更新过程中的一致性，从而提高了路径跳变的可用性。

定理 3 “逆序添加，顺序删除”的更新方式保证了路径跳变更新过程中数据分组的可达性。

证明 假设“逆序添加，顺序删除”的更新方

式无法保证数据流传输过程中的可达性。这说明更新过程中存在跳变路由 MR_i 无法将数据分组发送到某些节点。所有跳变路由可分为 4 类。

1) $MR_i \notin MR_{\text{new}} \wedge MR_i \notin MR_{\text{old}}$：它表示该跳变路由既不属于本次跳变周期内的转发路由，也不属于下一周期内的转发路由集合。因此，这类跳变路由不会接收到任何数据分组。

2) $MR_i \in MR_{\text{new}} \wedge MR_i \notin MR_{\text{old}}$：它表示跳变路由只属于下一跳变周期内的转发路由集合。因此，这类跳变路由不会接收到本次跳变周期内的数据分组，且只会依据更新的路由表转发下一周期的数据分组。

3) $MR_i \in MR_{\text{new}} \wedge MR_i \in MR_{\text{old}}$：它表示跳变路由既属于本次跳变周期内的转发路由，又属于下一周期内的转发路由集合。因此，这类跳变路由会依据相应的路由表项进行转发。

4) $MR_i \notin MR_{\text{new}} \wedge MR_i \in MR_{\text{old}}$：它表示跳变路由只属于本次跳变周期内的转发路由集合。因此，这类跳变路由只会接收到本次跳变内的数据分组，且依据原有路由表进行转发。此外，当经过 RTT(round trip time)时间后，跳变路由未收到数据分组，则证明本次跳变周期内数据分组已全部转发，且不会收到下一周期内的数据分组[6]。

由此可知，在路径跳变更新过程中被转发的数据分组依然可达，与假设相矛盾，证毕。

6　实验与分析

为了验证 OFPM 的可行性和有效性，利用 Mininet[26]构建仿真网络拓扑，采用 Waxman 模型进行随机网络拓扑生成，其中，α=0.3，β=0.2。利用支持 Openflow1.3 的 OpenVSwitch(OVS)[27]作为 MS，OpenDaylight[28]作为 RC。OpenDaylight 和 OVS 上通过部署最优路径跳变算法实现传输路径的迁移；同时利用 Z3 作为 SMT 求解器。实验所用的数据量为 9×10^5；速率为 1.56×10^3 packet/s；攻击方监听任意一条链路的概率 $P_{\cdot}^{a}$ 服从 [0.3, 0.95] 上的随机均匀分布[12]。

6.1　抵御被动监听实验

在 5.1 节分析的基础上，通过对比分析不同最大转发路径长度、不同被监听链路的数量以及被动监听频率条件下静态网络、RRM 和 OFPM 网络中被动监听的成功率检验其抵御被动监听的能力。

当 R_A=R_D，且攻击方可同时被动监听 250 个路由节点时，通过改变网络规模分析静态网络、RRM 和 OFPM 抵御被动侦测的能力。如图 4 所示，由于静态网络中不存在路径跳变的情况，因此，在攻击方攻击能力一定的情况下，其被动监听的成功率随着网络规模的增加而降低；与此同时，若网络规模相同，攻击方监听某条转发链路的成功率随着转发路径的长度增加而增加；在相同网络规模和转发路径长度的条件下，由于 OFPM 采用了基于安全矩阵容量的最优路径选取方法，可针对当前网络状态选取最优的跳变路径和跳变周期组合。所以，OFPM 较 RRM 抵御被动监听的能力更高，当转发路径长度 $L_T=5$ 时，OFPM 可抵御约 94%的被动监听。

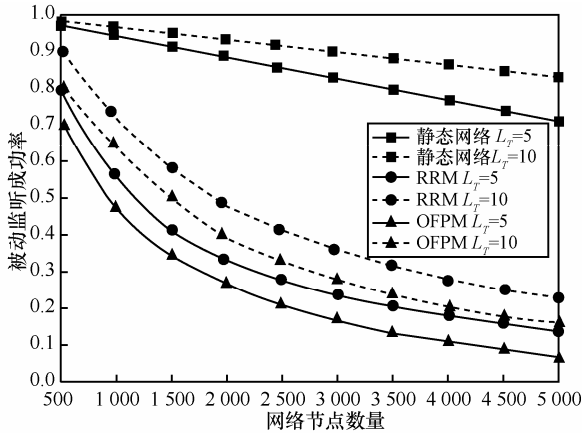

图 4　监听成功率与网络规模的关系

当 R_A=R_D，且路由节点为 n=2 000 时，通过改变攻击方同时被动监听节点的能力分析静态网络、RRM 和 OFPM 抵御被动监听的能力。如图 5 所示，若转发路径长度相同时，攻击方被动监听的成功率随其攻击能力的增加而升高。当攻击方可同时监听

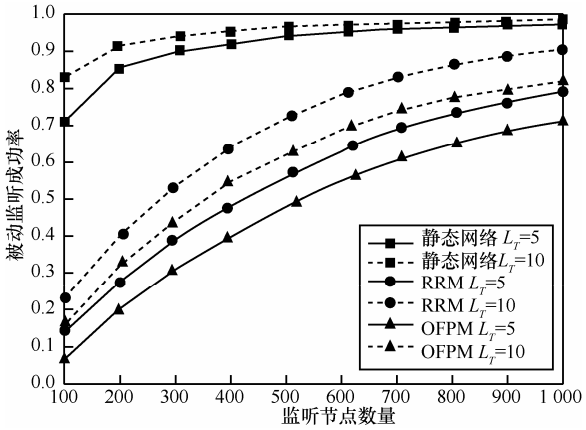

图 5　监听成功率与监听节点数量的关系

的路由节点数量少于路由节点总数的$\frac{1}{2}$时，由于OFPM针对当前网络状态选取最优的跳变路径和跳变周期组合，有效发挥了路径跳变的防御能力，因此，相较RRM和静态网络可有效抵御攻击方的被动监听。

当路由节点n为2 000，且攻击方可同时监听的路由节点数量为200个路由节点时，通过改变攻击方监听频率分析静态网络、RRM和OFPM抵御被动监听的能力。如图6所示，由于RRM采用固定跳变周期，随着攻击方监听频率的增加，当$R_A>R_D$时，RRM抵御被动监听的能力等同静态网络；由于OFPM采用基于安全容量矩阵的最优跳变路径生成，因此即使攻击方提高监听频率，但OFPM随后通过调整跳变频率，使$R_A \leqslant R_D$。

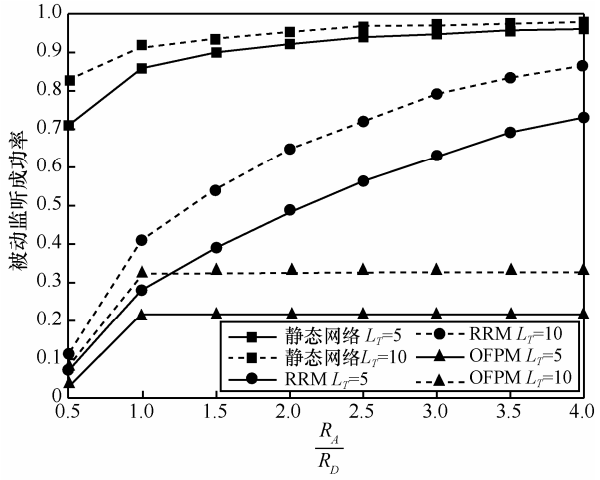

图6 监听成功率与监听频率的关系

6.2 性能实验

在5.2节分析的基础上，本节主要对OFPM跳变过程中分组序列的情况进行实验。

如图7所示，由于RRM随机选取符合要求的下一跳转发路径，因此，随着跳变频率的增加，下一跳变周期的转发路径中最小传输时延与现有转发路径$L_{T_{\mathrm{RMP}}}$中的最大传输时延之差大于转发数据流中最小分组间时延的比例也随之增加，进而导致分组乱序比例逐渐增加；OFPM采用了转发路径时延约束，因此，在转发路径跳变过程中，分组乱序概率与静态网络几乎相同，不会产生额外的分组乱序问题。

7 结束语

本文针对现有路径跳变技术难以在保证网络服务质量的基础上最大化防御收益的问题，提出了基于最优路径跳变的网络移动目标防御技术。利用SMT形式化规约跳变路径所需满足的约束条件，以防止路径跳变过程中出现的瞬态问题，及由此造成的分组丢失和分组乱序；提出基于安全容量矩阵的最优跳变路径生成方法，依据最大流—最小割理论求解最优跳变路径和跳变周期组合，以最大化跳变防御能力。理论分析和仿真实验比较了OFPM与静态网络和RRM抵御不同被动监听的能力。实验表明OFPM在$L_T=5$，攻击方同时监听$\frac{1}{20}$路由节点的条件下，可有效抵御约94%的被动监听攻击。此外，在跳变路径迁移和流表更新过程中，OFPM中产生的分组乱序概率与静态网络几乎相同。由此可知，OFPM在保证系统服务质量的同时实现了跳变防御收益的最大化。

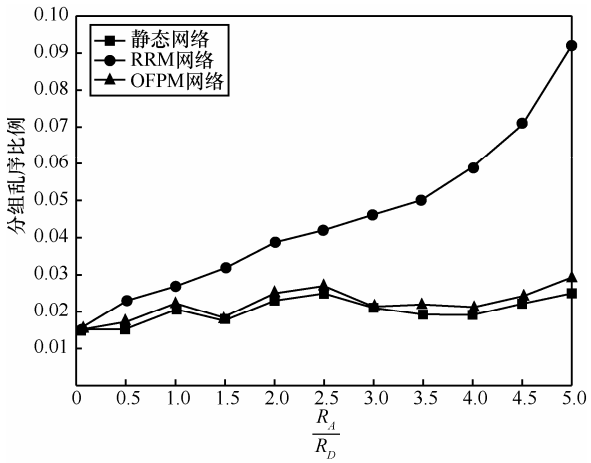

图7 分组乱序实验

参考文献：

[1] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense: creating asymmetric uncertainty for cyber threats[M]. Springer Science & Business Media, 2011.

[2] LEI C, MA D H, ZHANG H Q. Optimal strategy selection for moving target defense based on Markov game[J]. IEEE Access, 2017.

[3] SUN K, JAJODIA S. Protecting enterprise networks through attack surface expansion[C]//The 2014 Workshop on Cyber Security Analytics, Intelligence and Automation. 2014: 29-32.

[4] LEI C, MA D, ZHANG H, et al. Moving target network defense effectiveness evaluation based on change-point detection[J]. Mathematical Problems in Engineering, 2016: 20166-391502.

[5] YADAV T, RAO A M. Technical aspects of cyber kill chain[C]// International Symposium on Security in Computing and Communication. Springer International Publishing. 2015: 438-452.

[6] DUAN Q, AL-SHAER E, JAFARIAN H. Efficient random route

mutation considering flow and network constraints[C]//IEEE Conference on Communications and Network Security (CNS). 2013:260-268.
[7] NELAKUDITI S, LEE S, YU Y, et al. Fast local rerouting for handling transient link failures[J]. IEEE/ACM Transactions on Networking (ToN), 2007, 15(2): 359-372.
[8] JAFARIAN J H, AL-SHAER E, DUAN Q. Formal approach for route agility against persistent attackers[C]//European Symposium on Research in Computer Security. 2013: 237-254.
[9] DOLEV S, DAVID S T. SDN-Based Private Interconnection[C]// 2014 IEEE 13th International Symposium on Network Computing and Applications (NCA). 2014: 129-136.
[10] SHU T, KRUNZ M, LIU S. Secure data collection in wireless sensor networks using randomized dispersive routes[J]. IEEE Transactions on Mobile Computing, 2010, 9(7): 941-954.
[11] BOHACEK S, HESPANHA J P, LEE J, et al. Game theoretic stochastic routing for fault tolerance and security in computer networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(9): 1227-1240.
[12] GILLANI F, AL-SHAER E, LO S, et al. Agile virtualized infrastructure to proactively defend against cyber-attacks[C]//2015 IEEE Conference on Computer Communications (INFOCOM). 2015:729-737.
[13] BJØRNER N, DE MOURA L. Z310: applications, enablers, challenges and directions[C]//Sixth International Workshop on Constraints in Formal Verification. 2009.
[14] QAZI Z A, LEE J, JIN T, et al. Application-awareness in SDN[J]. ACM SIGCOMM Computer Communication Review, 2013, 43(4): 487-488.
[15] HAN S, PENG Z, WANG S. The maximum flow problem of uncertain network[J]. Information Sciences, 2014, 265: 167-175.
[16] YU M, YI Y, REXFORD J, et al. Rethinking virtual network embedding: substrate support for path splitting and migration[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 17-29.
[17] COHEN R, LEWIN-EYTAN L, NAOR J S, et al. On the effect of forwarding table size on SDN network utilization[C]//IEEE INFOCOM 2014-IEEE Conference on Computer Communications. 2014: 1734-1742.
[18] KAR K, KODIALAM M, LAKSHMAN T V, et al. Routing for network capacity maximization in energy-constrained ad hoc networks[C]//INFOCOM. 2003.
[19] LIANG W, GUO X. On-line multicasting for network capacity maximization in energy-constrained ad hoc networks[J]. IEEE Transactions Mobile Computing, 2006, 5:1215-1227.
[20] HUANG M, LIANG W, XU Z, et al. Dynamic routing for network throughput maximization in software-defined networks[C]//IEEE INFOCOM The 35th Annual IEEE International Conference on Computer Communications. 2016:978-986.
[21] PENG B, KEMP A H, BOUSSAKTA S. QoS routing with bandwidth and hop-count consideration: a performance perspective[J]. Journal of Communications, 2006, 1(2): 1-11.
[22] JACOBSON V. Congestion avoidance and control[J]. ACM SIGCOMM Computer Communication Review, 1988, 18(4): 314-329
[23] HAO J, ORLIN J. A faster algorithm for finding the minimum cut in a directed graph[J]. Journal of Algorithms, 1994,17(3): 424-446.
[24] KIRKPATRICK K. Software-defined networking[J]. Communications of the ACM, 2013, 56(9):16-19.
[25] LEUNG K C, LI V O K, YANG D. An overview of packet reordering in transmission control protocol(TCP): problems, solutions, and challenges[J]. IEEE Transactions on Parallel & Distributed Systems, 2007, 18: 522-535.
[26] LANTZ B, HELLER B, MCKEOWN N. A network in a laptop: rapid prototyping for software-defined networks[C]//The 9th ACM SIGCOMM Workshop on Hot Topics in Networks. 2010.
[27] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: enabling innovation in campus networks[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2):69-74.
[28] MEDVED J, VARGA R, TKACIK A, et al. Opendaylight: towards a model-driven SDN controller architecture[C]//2014 IEEE 15th International Symposium on a World of Wireless, Mobile and Multimedia Networks. 2014: 1-6.

作者简介：

雷程（1989-），男，北京人，解放军信息工程大学博士生，主要研究方向为网络信息安全、移动目标防御、数据安全交换和网络流指纹等。

马多贺（1982-），男，安徽六安人，博士，中国科学院信息工程研究所助理研究员，主要研究方向为应用安全、移动目标防御、云安全、网络与系统安全等。

张红旗（1962-），男，河北遵化人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为网络安全、移动目标防御、等级保护和信息安全管理等。

韩琦（1981-），男，河南平顶山人，博士，哈尔滨工业大学副教授，主要研究方向为信息隐藏、信息对抗、量子密码和多媒体安全等。

杨英杰（1971-），男，河南郑州人，博士，解放军信息工程大学教授、硕士生导师，主要研究方向为数据挖掘、态势感知和信息安全管理等。