计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20160461
54(12):2761-2771, 2017

基于路径与端址跳变的SDN网络主动防御技术

张连成[1] 魏 强[1] 唐秀存[2] 房家保[1]
[1](数学工程与先进计算国家重点实验室 郑州 450002)
[2](江南计算技术研究所 江苏无锡 214083)
(liancheng17@gmail.com)

Path and Port Address Hopping Based SDN Proactive Defense Technology

Zhang Liancheng[1], Wei Qiang[1], Tang Xiucun[2], and Fang Jiabao[1]
[1](*State Key Laboratory of Mathematical Engineering and Advanced Computing*, *Zhengzhou* 450002)
[2](*Jiangnan Institute of Computing Technology*, *Wuxi*, *Jiangsu* 214083)

Abstract Existing path hopping technologies are not so efficient for defending global network interception and analysis attackers, and existing port and address hopping technologies spend too much effect on hopping synchronization and are difficult to be deployed. In order to mitigate these problems, a path and port address hopping based SDN proactive defense (PPAH-SPD) scheme, making full use of SDN network characteristics (such as control plane and data plane separation, logically centralized control) and introducing of multi-path routing, is proposed. PPAH-SPD scheme models the path hopping problem as a constraint solving problem, and utilizes satisfiability modulo theory solver to obtain multiple available paths, which satisfy overlap and capacity constraints. According to path hopping strategy and specific hopping interval, SDN controller installs corresponding flow entries into all OpenFlow switches along every specific path, and these switches can then use these flow entries to properly forward the corresponding network flows, and simultaneously change their address and port information. Theoretical analysis and experimental results show that PPAH-SPD scheme can not only achieve transmission path hopping and port and address random hopping along every single transmission path with comparatively small communication time delay and computation overhead, and but also improve proactive defense capability of SDN network to resist global network interception and analysis attack, denial of service attack and insider threat.

Key words software defined network (SDN); moving target defense; path hopping; port and address hopping; proactive defense

摘 要 为解决已有路径跳变技术难以抵御全局截获分析攻击及已有端址跳变技术跳变同步难、部署难度大等问题,提出基于路径与端址跳变的SDN网络主动防御技术.首先,将路径跳变问题建模为约束求解问题,使用可满足性模理论求解器求解获得满足重复约束和容量约束的多条路径,然后,依据特定跳变时隙向所选跳变路径上的所有OpenFlow交换机下发对应的端址跳变流表项,使这些交换机对数据流进行正确转发的同时,更改其端口与地址信息.理论分析与实验结果表明:所提技术可以以较小的

收稿日期:2016-06-15;**修回日期**:2016-08-31
基金项目:国家自然科学基金项目(61402526,61402525,61502528)
This work was supported by the National Natural Science Foundation of China (61402526, 61402525, 61502528).

通信时延开销与计算开销实现通信双方传输路径与传输路径上端口与地址的随机跳变,且可提升 SDN 网络对于全局截获分析攻击、拒绝服务攻击与内部威胁的主动防御能力.

关键词 软件定义网络;移动目标防御;路径跳变;端址跳变;主动防御

中图法分类号 TP393.08

随着软件定义网络(software defined network, SDN)标准与产品的日益成熟、部署与应用的逐步广泛[1-2],针对 SDN 网络的探测扫描[3]、拒绝服务(denial of service, DoS)攻击[4]等逐步出现[5-6],SDN 网络安全问题日益突出.

当前,SDN 网络安全防护技术和手段大多采取防火墙[7]、入侵检测与防御[8]、DoS 攻击检测与防护[9-10]、安全策略增强[11-12]等被动式防护思想,安全防御者与网络攻击者之间所花费的时间与代价极其不对等,安全防御者处于非常被动的局面,通常要为整个网络添加层层安全防护措施,而网络攻击者则较为主动,有时只需利用系统中的某一脆弱点即可攻破网络.

为改变传统安全防护极其被动的局面,移动目标防御(moving target defense, MTD)[13-15]技术是近年来出现的网络安全领域的革命性技术,摒弃以构建无缺陷防御系统的方式维护网络安全性,而代之以构建、评价、部署开发出一种多样或持续随时间无规律变化的机制来提升网络攻击的复杂度和花费,从而降低攻击的成功率.

路径跳变(path hopping)和端址跳变(port and address hopping)是典型的网络 MTD 技术[13-15].为解决已有路径跳变技术难以抵御全局截获分析攻击及已有端址跳变技术跳变同步难、部署难度大等问题,充分利用 SDN 网络的控制与转发分离、网络可编程等新特性,提出基于路径与端址跳变的 SDN 网络主动防御(path and port address hopping based SDN proactive defense, PPAH-SPD)技术,可以用较小的代价和开销,提高 SDN 网络的主动防御能力.

1 研究现状分析

本节主要对路径跳变及与路径跳变相关的多路径路由(multipath routing)与端址跳变方面的研究现状进行总结与分析.

1.1 多路径路由

为实现负载均衡,学术界早在 20 世纪 70 年代就已提出在计算机网络中使用多路径路由,诸如拆分多路由(split multiple routing, SMR)[16],AOMDV(ad hoc on-demand multipath distance vector)[17]和 AODVM(ad hoc on-demand distance vector multipath)[18]等,试图在路由中寻找不相交路径(disjoint path)[18].通过多路径路由来提高安全性的协议有 SPREAD(security protocol for reliable data delivery)[19],SRP(secure routing protocol)[20-21],SecMR(secure multipath routing)[22],然而这些协议中路由选择是确定的,如果攻击者知道算法,那么路由就能被预测到.Shu 等人[23]提出的基于随机走(random walk)的多路径算法能在无线传感器网络中生成随机、高分散、更节能的多路径路由.然而,由于拓扑和服务质量(quality of service, QoS)的诸多限制,该算法并不适用于有线网络.

1.2 路径跳变

在传统网络协议中,转发路由通常是静态的,而静态路由为攻击者进行窃听、收集网络信息、开展 DoS 攻击等提供了便利条件.为解决该问题,路径跳变借鉴多路径路由思想,使得通信双方的通信路径在通信过程中按照一定算法进行随机跳变,使攻击者失去对路径上特定节点或链路进行有效监听或 DoS 攻击的能力,进而提高网络与系统的安全性.

Talipov 等人[24]提出基于 R-ADOV(reverse AODV)的路径跳变方法.通过 R-AODV,源节点可建立到目的节点的多条路径,在数据传输自适应跳转到可用路径上,可保护数据不受恶意节点的入侵.该方法适应于自组织网络,在有线网络中难以直接实现.

Duan 等人[25]提出一种主动随机路由跳变(random route mutation, RRM)技术,能同时随机改变网络中多条数据流的路由来抵御探测、窃听和 DoS 攻击,并且满足端对端 QoS 特性.为主动抵御 DoS 攻击,Jafarian 等人[26]提出一个灵活的多路径路由方法,结合博弈论(game theory)和约束满足优化(constraint satisfaction optimization)来确定攻击威慑(attack deterrence)的最佳策略,同时满足网络的安全、性能和 QoS 要求.上述路径跳变技术[25-26]侧重于多路径随机传输,目的是减少被攻击者截获分析的可能性,对于只能截获部分网络链路与节点

的局部攻击者而言具有非常好的防范效果,但对于全局攻击者,因攻击者可以捕获网络中全部通信流量,进而可有效关联分析得到真实的通信流量及顺序,已有路径跳变技术对于该类攻击者的防范效果不够好.

1.3 端址跳变

端址跳变通过在通信时对通信一方或双方的地址和端口进行随机跳变以实现主动安全防护,是地址跳变与端口跳变的结合.

Shi 等人[27]提出一种基于端址跳变的 DoS 主动防御策略,并提出一种适合远程网络应用的时间戳同步方法,基于 Java 移动代理技术设计并实现了一个端址跳变原型系统,验证了端址跳变策略抗 DoS 攻击的良好性能. 丰伟[28]提出一种改进的地址端口动态跳变技术,对网络时间同步矫正方案进行了改进,并且验证了所提技术可提高音视频通信系统的抗攻击能力. Luo 等人[29]提出一种随机端口地址跳变(random port and address hopping,RPAH)机制,基于源身份和服务身份,不可预测、持续高速地改变 IP(Internet protocol)地址和通信端口,可有效抵御网络探测、SYN(synchronize)洪泛攻击和蠕虫扫描.

端址跳变技术对通信双方之间的跳变同步要求较高,通信双方必须清楚跳变形式和规律及当前跳变时隙所使用的跳变信息,从而保证通信的正常进行. 常见的跳变同步方式主要有严格时间同步[30]、ACK(acknowledge)同步[31]和时间戳同步[27]. 严格时间同步方式受网络延迟、数据包拥堵等的影响较大;ACK 同步方式将同步信息放置于 ACK 报文中,易被截获分析;时间戳同步方式和分布式时间戳同步方式[32]不需要严格时间同步,但部署难度大、实现相对复杂. 此外,现有端址跳变技术在跳变时与通信双方的关联度较高,部署难度较大.

为提升 SDN 网络的主动防御能力,针对已有路径跳变技术难以有效防御全局截获分析攻击者的问题与已有端址跳变技术跳变同步难、开销大与部署难度大的问题,充分利用 SDN 网络的控制与转发分离、逻辑集中控制和网络可编程等新特性,提出基于路径与端址跳变的 SDN 网络主动防御技术.

2 基于路径与端址跳变的 SDN 主动防御技术

本节首先分析 SDN 网络在实现路径与端址跳变时的技术优势,然后再对所提 PPAH-SPD 技术的架构及核心环节进行阐述.

2.1 SDN 网络优势特性分析

由于 SDN 网络架构具有鲜明的逻辑集中控制与网络可编程特性[1-2],在实现路径与端址跳变时具有 3 点优势:

1) SDN 网络由 SDN 控制器进行逻辑集中控制,跳变功能可以从具体的网络代理(如路由器、中继节点等)中抽取出来,统一放在 SDN 控制器处实现,使得跳变功能与通信双方无关,进而无需改变通信节点的配置信息,不但实现方便、部署容易,且调试与修改也非常便利;

2) 在 SDN 网络架构下,可对网络通信数据流在转发的同时进行数据包特定字段(如 IP 地址与端口等)的修改,不仅可避免通信会话中断,还可实现通信数据流特定字段信息在网络传输过程中的随机变化,可有效应对全局攻击者的截获与分析,极大增加全局攻击者的分析难度;

3) 可实现基于 SDN 控制器的透明跳变同步. 借助 SDN 网络的逻辑集中控制特性,SDN 控制器具备天然的集中与同步特性,只需要向发送者与接收者所接入的 OpenFlow 交换机(即通信网关)分别发送特定流表项即可实现透明跳变同步,省却同步开销,不但不需要严格的时间同步和发送额外的事件同步报文,且可保证跳变信息的安全.

2.2 PPAH-SPD 技术系统架构与基本处理流程

PPAH-SPD 技术架构如图 1 所示,路径跳变模块依据通信双方协商的共享信息进行当前跳变时隙所需路径信息的生成与选择,并指示端址跳变模块生成随机地址与端口信息;端址跳变模块主要依据路径跳变模块的指示与当前时隙生成所需的随机地址端口表,并指示流表维护模块进行流表项下发;流表维护模块负责根据当前跳变时隙对当前跳变路径上的所有交换机进行对应流表项的下发,并及时删除过期跳变路径上对应交换机的过期流表项.

在 PPAH-SPD 中,SDN 控制器负责具体的决策,是 PPAH-SPD 技术的核心,主要功能是路径跳变的触发与具体决策、传输路径上端址跳变功能实现等;OpenFlow 交换机接收 SDN 控制器的具体决策,安装特定流表项,通过不同的流表项来实现具体的路径跳变与端址跳变;为提高 PPAH-SPD 技术的适用范围,减少对通信双方的依赖,整个跳变通信过程与通信双方无关,通信双方在通信时,SDN 控制器会将其接入的 OpenFlow 交换机作为通信网关

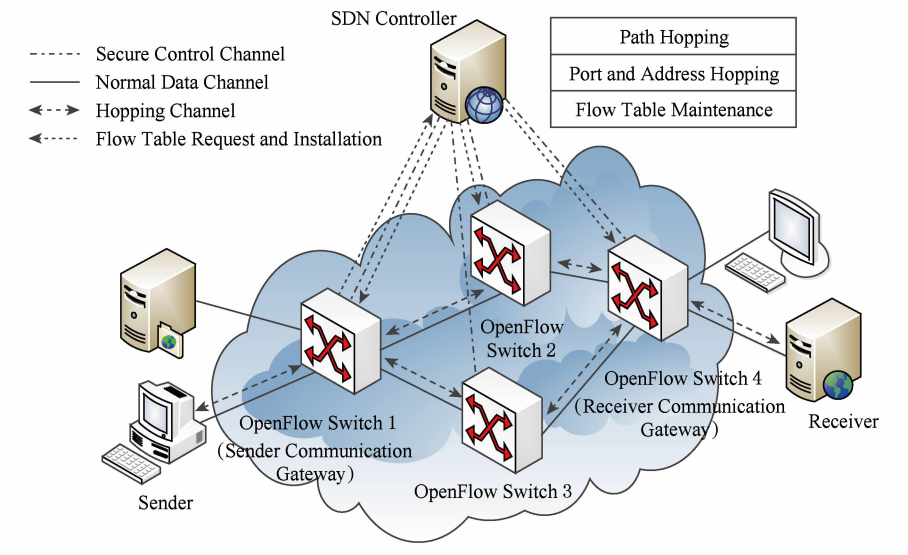

Fig. 1 PPAH-SPD framework

图 1 PPAH-SPD 系统架构

(如图 1 中的发送者通信网关与接收者通信网关),部署与实施更加方便与灵活.

下面主要阐述多路径的约束求解、单路径上的端址跳变及传输路径上 OpenFlow 交换机处理流程核心环节.

2.3 多路径的约束求解

路径跳变需要随机改变通信双方之间的通信路径与路由,同时在选择路径时还需要考虑:1)重复约束. 为了增加不可预测性和更好的负载均衡,新路径应该避免使用最近使用过的中间节点,路径跳变中的重复节点及链路越少,不可预测性越大. 2)容量约束. 新的路径不应该包含已经超负荷或者不满足流量带宽要求的节点或链路.

本文将路径跳变问题建模为约束求解问题,使用可满足性模理论(satisfiability modulo theory, SMT)求解器求解获得满足重复约束和容量约束的多条路径. SMT 是被众多领域使用的强大约束满足求解器,能处理任何能被建模成布尔或算数格式的约束,而且便于添加新的约束.

1) 路径跳变建模与基本约束

将网络建模为有向图 $G=(V,E)$,其中 V 是主机集合、E 是链路集合. 假设 1 条源节点为 S、目的节点为 D 的流($S,D\in V$),流的持续期可被划分为多个时间间隔,即跳变时隙 λ(单位为 s). 路径跳变需要为每个时隙在 S 和 D 之间找 1 条满足容量与重复约束的路径.

2) 攻击者能力假设

对于截获分析攻击者,假设攻击者不干扰网络的正常功能,不生成或篡改流量,只是监听链路或节点. 假设攻击者为全局攻击者,能监听整个网络,也能截获网络中所有节点间的通信数据流并进行分析.

对于 DoS 攻击者,假设攻击者能在一段时间内破坏有限的链路或节点,因为攻击者的预算和能力是有限的,且攻击太多链路或节点也将增加暴露概率.

3) 基于 SMT 的约束求解

本节对路径跳变进行 SMT 形式化. 假设网络中共包含 a 个节点 $v_1,v_2,\cdots,v_a$ 和 b 条链路 $e_1,e_2,\cdots,e_b$. 流入节点 $v_j(1\leqslant j\leqslant a)$的链路集合表示为 I_j,流出节点 v_j 的链路集合记为 O_j.

源节点 S 到目的节点 D 的有效路径可形式化为

$$\sum_{e_i\in O_j}u_i=\sum_{e_i\in I_j}u_i,\ v_j\neq S,\ v_j\neq D, \tag{1}$$

$$\sum_{e_i\in O_S}u_i=1, \tag{2}$$

$$\sum_{e_i\in I_D}u_i=1, \tag{3}$$

$$u_i\in\{0,1\},\ \forall i, \tag{4}$$

其中,变量 u_i 表示链路 e_i 是否出现在路径中,如果 $u_i=1$,则链路 e_i 被该路径所使用,否则就没被使用;式(1)保证了其他节点(除源节点和目的节点外)在流入与流出方面的平衡;式(2)和式(3)保证数据流的源节点和目的节点必须是 S 和 D;式(4)指定 u_i 的取值为 0 或 1.

为保证之前用过的包含 $e_{i1},e_{i2},\cdots,e_{ig}$ 的路径不被当前路径再次使用,添加重复约束:

$$\neg((u_{i1}=1)\wedge(u_{i2}=1)\wedge\cdots\wedge(u_{ig}=1)). \tag{5}$$

对于容量约束,将其形式化为

$$\sum_{k=1}^{L} u_{ik} \leqslant R_i,\ 1 \leqslant i \leqslant b, \tag{6}$$

其中,变量 u_{ik} 表示链路 e_i 是否被路径 r_k 所使用,L 表示路径的个数,R_i 表示允许包含链路 e_i 的路径最大数量.

4) 路径跳变算法

路径跳变算法如算法 1 所示,由 SDN 控制器来实现和操作,在每个跳变时隙 λ 结束后,使用函数 $ModifyPath$ 来安装使用新路由 r_{k+1}、撤销旧路由 r_k. 另外,对于每条路径,还要安装反向路由才行实现通信路径的双向跳变(路由 r_k 的逆向路由表示为 r_k^{-1}).

算法 1. 从 S 到 D 数据流路径跳变算法.

使用 SMT 求解器确定满足条件的路径;

当第 k 个跳变时隙结束时

$$ModifyPath(r_k \rightarrow r_{k+1});$$

$$ModifyPath(r_k^{-1} \rightarrow r_{k+1}^{-1}).$$

函数 $ModifyPath$(如算法 2 所示)用于保证在数据流传输期间的端到端可达性,使得数据流被完全地传输. 为达到此目标,必须要保证任何从旧路由 r_k 跳变到新路由 r_{k+1}的跳变不会造成不可达.

算法 2. 路径修改算法.

函数 $ModifyPath(r_k \rightarrow r_{k+1})$:

向满足 $sw \in r_{k+1} \wedge sw \notin r_k$ 的所有交换机 sw 添加路由条目;

向满足 $sw \in r_{k+1} \wedge sw \in r_k$ 的所有交换机 sw 修改路由条目;

等待 1 个往返时延;

向满足 $sw \notin r_{k+1} \wedge sw \in r_k$ 的所有交换机 sw 删除路由条目.

定理 1. 算法 2 保证了可靠、无损的数据流传输.

证明. 假设算法 2 不能保证无损的数据流传输,意味着存在交换机 sw 在某时刻不能转发数据包. 基于是否包含于旧路由 r_k 与新路由 r_{k+1},所有 OpenFlow 交换机可分为 4 种:

① $sw \notin r_{k+1} \wedge sw \notin r_k$. 这种交换机不会收到任何数据流的数据包,因为没有交换机有向这种交换机转发数据包的规则.

② $sw \in r_{k+1} \wedge sw \notin r_k$. 这种交换机在路由 r_{k+1} 条目添加之前不会收到任何数据包,因为在路由 r_k 上没有交换机会转发数据包给这种交换机. 过后,这种交换机将可靠地转发数据包.

③ $sw \in r_{k+1} \wedge sw \in r_k$. 该种交换机将基于路由 r_k 或路由 r_{k+1}条目可靠地转发数据包.

④ $sw \notin r_{k+1} \wedge sw \in r_k$. 在路由 r_{k+1}被激活后,交换机 sw 可能会收到 1 个数据包,最迟收到该数据包的时间比源与目的节点间数据包往返时延要短. 在这之前,sw 将可靠地转发数据包,之后,该交换机将不会收到任何数据流的数据包.

因此,没有交换机不能转发数据流的数据包,存在矛盾,假设不成立,证明定理 1 是正确的. 证毕

2.4 单路径上的端址跳变

本文所提 PPAH-SPD 技术不但采取多条路径进行数据流传输,为进一步提高攻击者难度,防范全局截获分析攻击者,还在每条路径上实现网络通信数据流中所携带的源及目的 IP 地址与端口在转发过程中随机跳变功能,且该过程对源、目的节点透明.

1) 端址跳变过程

与传统跳变技术相比,PPAH-SPD 技术将随机跳变功能从网络节点处转移到通信数据传输的路径上,通信数据流所经过的每一跳 OpenFlow 交换机都会对数据包中的源和目的 IP 地址与源和目的端口进行随机修改,而传统跳变技术中的跳变只发生在传输路径的第 1 跳和/或最后 1 跳. 与传统跳变技术相比,本文所提技术可使得通信数据流中源和目的地址与端口的跳变更频繁、更加难以预测,可有效提升攻击者的攻击复杂度、时间及精力花费,进而可降低网络被攻击的风险.

单路径上的端址跳变过程为:对于需要转发的数据包,在保证数据包按照既定路径到达目的节点的同时,每一跳 OpenFlow 交换机将会根据匹配的流表项对数据包中的源及目的 IP 地址与源及目的端口进行随机更改,如图 2 所示,其中 rIP_a,rIP_b 为实际 IP 地址,vIP_1,vIP_2 为虚拟 IP 地址;$rPORT_a$,$rPORT_b$ 为实际端口,$vPORT_1$,$vPORT_2$ 为虚拟端口.

2) 随机地址端口生成算法

SDN 控制器生成的随机地址端口表若固定不变,那么攻击者可以通过多次测试监听,从而获得完整的随机地址端口表,进而对通信数据流进行截获重组分析,难以达到保护网络通信数据安全的目的.

本文随机 IP 地址生成算法为

$$IP = \mathrm{Hash}(Timestamp)_{16} \,|\, \mathrm{Hash}(Nonce)_{16}, \tag{7}$$

其中,$Timestamp$ 是时间戳,$Nonce$ 是随机数,$\mathrm{Hash}(Timestamp)_{16}$表示取时间戳经过 Hash 之后的前 16 b,$\mathrm{Hash}(Nonce)_{16}$表示取随机数经过 Hash 之后的后 16 b,由 2 者组成随机的 IP 地址.

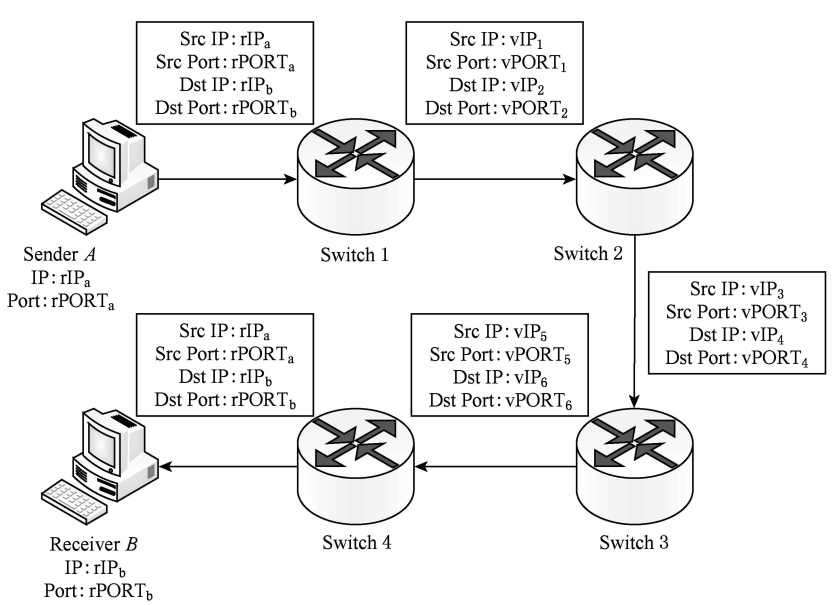

Fig. 2 Port and address hopping along a specific path

图 2 单路径上的端址跳变

随机端口生成算法为

$$PORT=\mathrm{Hash}(Timestamp\,|\,Nonce)_{16},\quad(8)$$

其中，$\mathrm{Hash}(Timestamp\,|\,Nonce)_{16}$表示取时间戳和随机数经过 Hash 之后的前 16 b，作为随机端口.

时间戳 *Timestamp* 和随机数 *Nonce* 由 SDN 控制器随机生成，每当生成新的随机地址端口表，控制器就依据该表对跳变路径上所有交换机的流表项进行维护，以此提高攻击者的监听与分析难度.

2.5 传输路径上 OpenFlow 交换机处理流程

OpenFlow 交换机通过流表中用户定义或预设的规则(流表项)按照优先级匹配和处理数据包. 当数据包成功匹配 1 条流表项后将首先更新该流表项对应的统计数据(如成功匹配数据包总数目和总字节数等)，然后根据流表项中的指令进行相应操作，如转发至某一端口、修改数据包某一字段等.

PPAH-SPD 技术主要利用 SDN 网络中的控制器为特定传输路径上的所有 OpenFlow 交换机下发不同匹配项、不同执行动作的流表项来实现端址跳变功能，该过程的处理流程如图 3 所示.

当 OpenFlow 交换机收到数据流之后，首先判断有无相匹配的流表项，如果有，则按照流表项中的动作执行处理，如果没有(表明 SDN 控制器尚未下发相应的流表项)，则需向 SDN 控制器发送数据包请求下发相应的流表项. 当 SDN 控制器收到该数据包之后，则会根据该数据包进行流表项下发. 在下发流表项时，SDN 控制器根据式(7)和式(8)生成随机地址端口表，包括随机源 IP 地址子表、随机目的 IP 地址子表、随机源端口子表和随机目的端口子表，

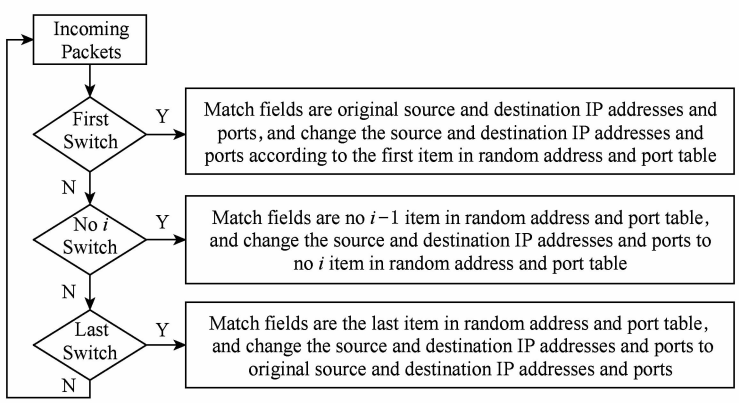

Fig. 3 Port and address hopping process on different switches along a specific path

图 3 单路径上端址跳变数据流处理流程

4 张子表大小均为 $l-1$(l 为路径上 OpenFlow 交换机的个数),SDN 控制器针对传输路径上的 OpenFlow 交换机下发往返方向的流表项.

3 安全性分析

从影响网络安全性的全局截获分析攻击、拒绝服务攻击与内部威胁 3 个方面来分析 PPAH-SPD 技术的安全防御能力.

3.1 抗全局截获分析攻击能力分析

假设真实所传输的数据包序列为$\{p_1,p_2,\cdots,p_n\}$,攻击者截获得到的数据包序列为$\{c_1,c_2,\cdots,c_m\}$(假设 $m>n$). 截获分析攻击的目的就是从截获得到的所有 m 个数据包中分析得到真实的 n 个数据包,并且分析得出 n 个数据包的真实顺序并重组.

假设攻击者能力较强,可将发送者与接收者之间通信时间内该网络中产生的所有数据包都截获到(包含网络中所有通信的交互数据包),假设 S_c 为攻击者捕获数据包的开销,S_e 为比对过滤所花费的开销(因单条传输路径上 PPAH-SPD 技术还进行了端址跳变,因此攻击者还需要对多个数据包序列进行比对过滤),S_f 为攻击者从比对过滤后数据包中分析重组得到真实序列的数据包的开销,则攻击者的总开销为

$$S_{all}=S_c+S_e+S_f. \tag{9}$$

假设攻击者比对过滤后的数据包里包含全部通信双方的数据包,且顺序完全正确,这种情况下攻击者的重组开销最小,其重组开销为

$$S_{f_{min}}=\sum_{i=1}^{n}S_{analysis_i}=nS_{analysis}=O(n), \tag{10}$$

其中,$S_{analysis_i}$ 为第 i 个数据包的分析开销,$S_{analysis}$ 为单个数据包的分析开销.

假设攻击者比对过滤后的数据包里包含全部通信双方的数据包,但顺序完全逆序,这种情况下攻击者的重组开销最大,其重组开销为

$$S_{f_{max}}=\sum_{i=m-n+1}^{n}iS_{analysis_i}=O(n^2). \tag{11}$$

综合式(9)~(11)可知,攻击者总体开销为:$S_c+S_e+O(n)\leqslant S_{all}\leqslant S_c+S_e+O(n^2)$. 一般而言,攻击者在数据包截获方面的开销相对固定,则截获分析攻击者所需的总体开销为 $\Omega(n)\leqslant S_{all}\leqslant O(n^2)$.

上述分析过程并未包含因数据包加密而给攻击者可能带来的解密与分析开销,如果通信双方在通信过程中再使用加密算法将通信数据流进行加密处理,则攻击者的总体开销将会更大;另外,如果攻击者所部署的数据包捕获工具一旦出现漏抓的情况,则很有可能漏掉部分数据包,进而会直接到影响攻击者的分析与重组工作.

综上,PPAH-SPD 技术对于数据流截获分析攻击有较好防范作用,即使攻击者可截获通信双方通信过程中的全部数据包,也难以分析得出正常的顺序而还原出原始传输数据信息.

3.2 抗拒绝服务攻击能力分析

假设中间路径上的 DoS 攻击者知道 PPAH-SPD 技术的存在,并从可用路径、地址与端口总数中随机挑选路径、地址与端口进行攻击.

假设 T_0 为未使用 PPAH-SPD 技术时攻击者击中目标所耗费的时间,N_r 是可用路径的总数,N_a 是可用地址的总数,N_p 是可用端口的总数,可知引入 PPAH-SPD 技术后,攻击者成功击中目标的时间为

$$T'=T_0\left(1+\sum_{i=1}^{N_rN_aN_p-1}i\frac{C_{N_rN_aN_p-1}^{i}}{C_{N_rN_aN_p}^{i}C_{N_rN_aN_p-1}^{1}}\right). \tag{12}$$

由式(12)可知,由于采用路径与端址跳变,PPAH-SPD 技术增加了攻击者的时间代价.

假设 N_d 是 DoS 攻击者的数量,z 是攻击者产生数据包的速率,λ 是跳变时隙,x 代表包含正确路径、地址和端口的恶意数据包(即命中数据包),x 的均值为

$$E(x)=\frac{N_dz\lambda}{N_rN_aN_p}. \tag{13}$$

由式(13)可知,PPAH-SPD 技术抗 DoS 攻击性能除了与攻击者数量 N_d、攻击数据包产生速率 z 有关,还与跳变时隙 λ、可用路径总数 N_r、可用地址总数 N_a 和可用端口总数 N_p 有关. λ 越小,则跳变速度就越快,攻击者猜中路径、地址与端口号的概率越低,连续时间内遭受攻击的概率就越低;可用路径总数 N_r、可用地址总数 N_a 和可用端口总数 N_p 越大,攻击者猜中路径、地址与端口号的概率越低,网络的安全性就越高.

因此,在应用 PPAH-SPD 技术时,应尽可能减小跳变时隙. 另外,还可想办法增加可用路径、地址与端口总数. 如:扩大可用网络的规模和数量,在更大的网络范围内使用路径与端址跳变技术;在网络层同时启动 IPv4(Internet protocol version 4)协议和 IPv6(Internet protocol version 6)协议进行通信(充分利用 IPv6 网络地址空间巨大的特点)、采用多穴跳变通信方式等;在传输层同时采用用户数据报协议(user datagram protocol, UDP)、传输控制协

议(transmission control protocol, TCP)和其他传输层协议进行通信.

3.3 抗内部威胁能力分析

在PPAH-SPD技术中,虽然发送者和接收者的真实地址和端口并未发生变化(为了实现对通信双方的透明,减少通信双方配置复杂度与部署难度),面临被攻击者开展针对性攻击的风险,但仍然能有效抵御来自SDN网络内部的安全威胁.这是因为:1)即使攻击者处于与发送者或接收者同样的内部网络之中,由于SDN网络的逻辑集中控制和控制与转发分离特性,攻击者的截获分析能力并未比3.1节假设的能力更强;2)攻击者可截获的链路与节点越多,虽然截获能力越强,但对攻击者的能力和资源要求越高,被发现的概率也越高;3)因攻击者不是授权用户,其在访问目的主机(发送者或接收者)时,同样也要经过SDN控制器的检查与过滤.

4 实验结果及分析

为测试PPAH-SPD技术的有效性和性能,使用Mininet网络模拟软件[33]、Open vSwitch(OVS)虚拟交换机[34]模拟并搭建SDN测试网络,采用NOX[35]作为SDN控制器负责路径与端址跳变功能,Mininet模拟器、OVS交换机、SDN控制器、发送者、接收者及攻击者(单个攻击节点可运行多个攻击程序)均部署在不同的节点上,这些节点构建于若干台配置均为Intel i7-4790 4核3.6 GHz CPU,4 GB内存的机器上.搭建的测试环境拓扑结构与图1类似,不再赘述.

4.1 跳变开销测试

本节主要从路径选择时SMT求解开销、路径跳变时路径更新开销、控制器CPU处理开销和数据流平均传输时延4个方面来测试路径与端址跳变带来的各项开销.

1) 路径选择时SMT求解开销

重复约束条件下路径选择时的SMT求解时间如图4所示,其中w是新路径不能重复的跳变时隙数量.从图4可知,当网络规模增加时,特别是当网络中交换机数量达到300后,SMT求解时间也随之增加.这是因为随着网络规模的增加,可能的路径数量以指数级增加.

2) 路径跳变时路径更新开销

假设新路径与旧路径间的重复节点很少,则路径跳变过程的路径更新开销可以通过每个跳变时隙

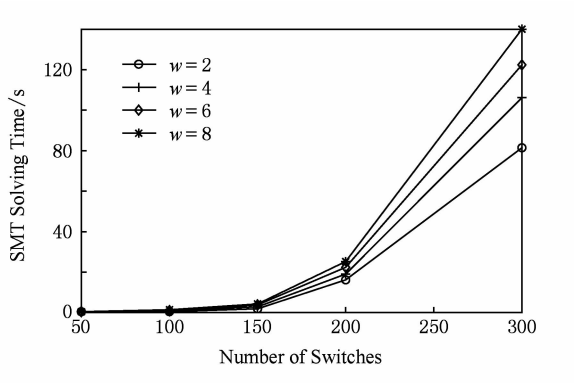

Fig. 4 SMT solving time under overlap constraint

图4 重复约束条件下SMT求解时间

中路径的平均长度来估算.对不同规模和长度上限的Waxman随机网络进行SMT求解获得的平均路由长度如图5所示.从图5可知,随着网络规模(即图5中的N)的增加,路径跳变算法的平均路由长度收敛于某值.

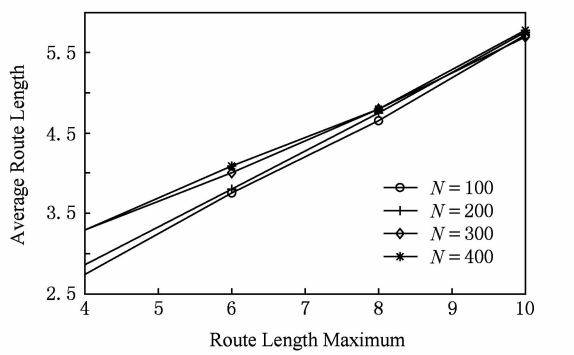

Fig. 5 Average route length of path hopping algorithm

图5 路径跳变算法平均路由长度

3) 控制器CPU处理开销

为测试PPAH-SPD技术对SDN控制器(因跳变功能主要由SDN控制器配合交换机来完成,而交换机的开销主要体现在流表项的查询与转发修改上,属于其基本功能)所带来的额外处理开销,分别使用不同长度的数据包进行通信,测试其对控制器CPU处理开销的影响,测试结果如图6所示.测试结果表明,PPAH-SPD技术对通信双方的通信过程进行端址跳变保护时,对SDN控制器所带来的额外开销并不大,在3.7%~6.5%之间,属于可接受的安全开销范围.

4) 数据流平均传输时延

对不同路径跳数情况下通信数据流的平均传输时延进行了测试,同时测试不采取端址跳变(未跳变)情况下的平均传输时延,2种情况下的对比结果如图7所示.从图7可知,在路径跳数相同的情况

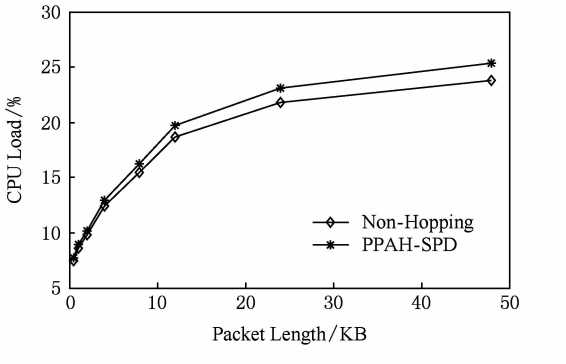

Fig. 6 Controller CPU load influenced by PPAH-SPD

图 6 控制器 CPU 负载影响

下,数据流在端址跳变情况下时延较高,而在未跳变情况下时延较低,但是端址跳变所增加的时延数量级为微秒.为保证通信的安全,端址跳变所增加的处理时延处于可接受的范围之内.

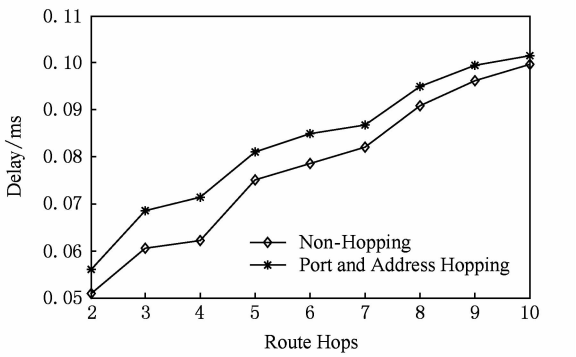

Fig. 7 Transmission delay difference between port and address hopping and non-hopping

图 7 端址跳变与未跳变下的传输时延比较

4.2 抗全局截获分析攻击能力测试

为测试 PPAH-SPD 技术保护下通信双方地址与端口的变化情况(以单路径上的端址跳变为例),对通信双方的流量进行分析,并与未跳变和端口跳变技术进行对比.

假设 PPAH-SPD 技术下通信节点所使用的地址范围为 192.168.1.0/24 与 192.168.2.0/24,通信双方使用的地址随机分配在 2 个地址空间里,远程攻击者很难分析得出通信双方当前通信与全程通信中所使用的地址与端口信息,进而难以有效还原重组出正确的数据流及顺序.

假设截获分析攻击者位于通信双方附近,可以将通信双方之间的全部通信数据包都截获下来,未跳变、地址跳变与端址跳变(只选取了部分地址对)3 种不同情况下的通信地址对情况如图 8 所示:

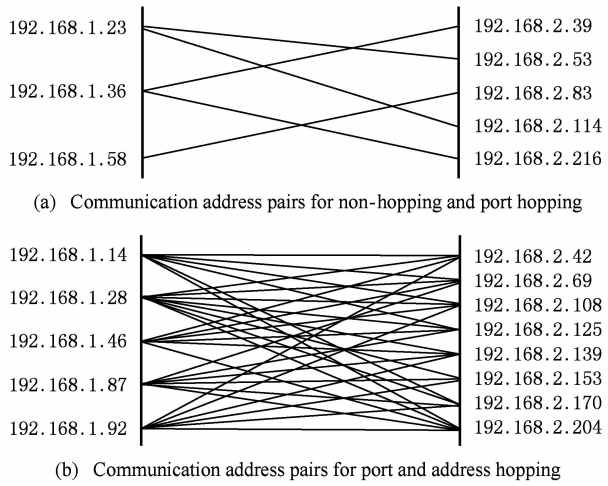

Fig. 8 Communication address pairs for non-hopping, port hopping and port and address hopping

图 8 未跳变、端口跳变与端址跳变下的通信地址对

实验结果表明:未跳变与端口跳变技术均难以有效分散网络流量,抗全局截获分析攻击能力较差;而端址跳变技术则可有效分散网络流量,使得通信双方的通信流量分散于多个网络连接中,攻击者即便是截获到完整的数据流,其分析重组出通信数据流的复杂度和难度也极大.

4.3 抗拒绝服务攻击能力测试

为测试 PPAH-SPD 技术的抗 DoS 攻击能力,使用 hping3 开源软件[36]构建典型 SYN 洪泛 DoS 攻击工具,攻击者逐个攻击受保护通信双方可用的路径、地址与端口.

测试受保护节点在不同 DoS 攻击速率下的响应时间,以测试 PPAH-SPD 技术的处理性能和开销大小,并与未跳变时的响应时间进行对比,如图 9 所示:

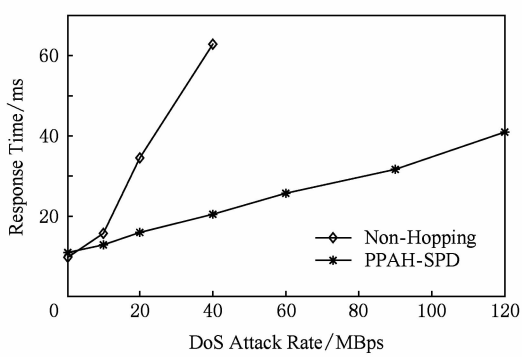

Fig. 9 Node response time comparison

图 9 节点响应时间测试

从图 9 可以看到,随着攻击强度的不断增大,未跳变情况下的固定路径与地址端口的通信方式,在

DoS 攻击面前,节点的响应时间很容易受到影响,而在 PPAH-SPD 技术保护下,节点则可承受更多攻击流量的攻击,因此 PPAH-SPD 技术可有效提高节点间通信的抗 DoS 攻击能力.

5 结束语

为提升 SDN 网络主动防御能力,充分利用 SDN 网络的控制与转发分离、逻辑集中控制等特性,引入移动目标防御与多路径路由思想,提出基于路径与端址跳变的 SDN 网络主动防御技术,不但可实现通信过程的多路径随机跳变,且可有效隐藏通信双方的原始地址和端口信息,对于全局截获分析攻击、DoS 攻击与内部威胁有较好的主动防御能力.

本文所实现的路径跳变为主动式,跳变规则、信息与策略等都是事先设置或临时配置的,较为依赖防护者的防护水平和配置能力,下一步拟引入博弈论进行跳变策略的优化选择,并实现反应式(reactive)跳变,将攻击者行为与网络实时状况纳入防御体系中,进一步提高 SDN 网络的主动防御能力.另外,为提高 PPAH-SPD 系统的可扩展能力,可将其扩展为多个控制器同时协调进行跳变处理,每个控制器管理一部分网络,缓解单个控制器情况下的性能瓶颈.

参 考 文 献

[1] Xia Wenfeng, Wen Yonggang, Foh C H, et al. A survey on software-defined networking [J]. IEEE Communications Surveys & Tutorials, 2015, 17(1): 27-51

[2] Farhady H, Lee H, Nakao A. Software-defined networking: A survey [J]. Computer Networks, 2015, 81: 79-95

[3] Shin S, Gu Guofei. Attacking software-defined networks: A first feasibility study [C] //Proc of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. New York: ACM, 2013: 165-166

[4] Antikainen M, Aura T, Sarela M. Spook in your network: Attacking an SDN with a compromised OpenFlow switch [G] //LNCS 8788: Proc of the 19th Nordic Conf. Berlin: Springer, 2014: 229-244

[5] Akhunzada A, Ahmed E, Gani A, et al. Securing software defined networks: Taxonomy, requirements, and open issues [J]. IEEE Communications Magazine, 2015, 53(4): 36-44

[6] Alsmadi I, Xu Dianxiang. Security of software defined networks: A survey [J]. Computers & Security, 2015, 53: 79-108

[7] Hu Hongxin, Han W, Ahn G, et al. FlowGuard: Building robust firewalls for software-defined networks [C] //Proc of the 3rd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. New York: ACM, 2014: 97-102

[8] Giotis K, Argyropoulos C, Androulidakis G, et al. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments [J]. Computer Networks, 2014, 62: 122-136

[9] Wang Bing, Zheng Yao, Lou Wenjing, et al. DDoS attack protection in the era of cloud computing and software-defined networking [J]. Computer Networks, 2015, 81: 308-319

[10] Wang Haopei, Xu Lei, Gu Guofei. FloodGuard: A DoS attack prevention extension in software-defined networks [C] //Proc of the 45th Annual IEEE/IFIP Int Conf on Dependable Systems and Networks. Piscataway, NJ: IEEE, 2015: 239-250

[11] Shin S, Yegneswaranz V, Porrasz P, et al. AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks [C] //Proc of the 20th ACM Conf on Computer and Communications Security. New York: ACM, 2013: 413-424

[12] Kreutz D, Ramos F M V, Verissimo P. Towards secure and dependable software-defined networks [C] //Proc of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. New York: ACM, 2013: 55-60

[13] Carvalho M, Richard F. Moving-target defenses for computer networks [J]. IEEE Security & Privacy, 2014, 12(2): 73-76

[14] Xu Jun, Guo Pinyao, Zhao Mingyi, et al. Comparing different moving target defense techniques [C] //Proc of the 1st ACM Workshop on Moving Target Defense. New York: ACM, 2014: 97-107

[15] Cai Guilin, Wang Baosheng, Wang Tianzuo, et al. Research and development of moving target defense 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)

[16] Lee S, Gerla M. Split multipath routing with maximally disjoint paths in ad hoc networks [C] //Proc of the 11th IEEE Int Conf on Communications. Piscataway, NJ: IEEE, 2001: 3201-3205

[17] Marina M K, Das S R. On-demand multipath distance vector routing in ad hoc networks [C] //Proc of the 9th IEEE Int Conf on Network Protocols. Piscataway, NJ: IEEE, 2001: 14-23

[18] Ye Zhenqiang, Krishnamurthy S V, Tripathi S K. A framework for reliable routing in mobile ad hoc networks [C] //Proc of the 22nd Annual Joint Conf of the IEEE Computer and Communications Societies, Volume 1. Piscataway, NJ: IEEE, 2003: 270-280

[19] Lou Wenjing, Liu Wei, Fang Yuguang. Spread: Enhancing data confidentiality in mobile ad hoc networks [C] //Proc of the 23rd Annual Joint Conf of the IEEE Computer and Communications Societies, Volume 4. Los Alamitos, CA: IEEE Computer Society, 2004: 2404-2413

[20] Papadimitratos P, Haas Z J. Secure routing for mobile ad hoc networks [C] //Proc of SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. Piscataway, NJ: IEEE, 2002: 193-204

[21] Argyroudis P, O'Mahony D. Secure routing for mobile ad hoc networks [J]. IEEE Communications Surveys & Tutorials, 2006, 7(3): 2-21

[22] Mavropodi R, Kotzanikolaou P, Douligeris C. SecMR—A secure multipath routing protocol for ad hoc networks [J]. Ad Hoc Networks, 2007, 5(1): 87-99

[23] Shu Tao, Krunz M, Liu Sisi. Secure data collection in wireless sensor networks using randomized dispersive routes [J]. IEEE Trans on Mobile Computing, 2010, 9(7): 941-954

[24] Talipov E, Jin D, Jung J, et al. Path hopping based on reverse AODV for security [G] //LNCS 4238: Proc of the 9th Asia-Pacific Network Operations and Management Symp. Berlin: Springer, 2006: 574-577

[25] Duan Qi, Al-Shaer E, Jafarian H. Efficient random route mutation considering flow and network constraints [C] //Proc of the 1st IEEE Conf on Communications and Network Security. Piscataway, NJ: IEEE, 2013: 260-268

[26] Jafarian J H, Al-Shaer E, Duan Qi. Formal approach for route agility against persistent attackers [G] //LNCS 8134: Proc of the 18th European Symp on Research in Computer Security. Berlin: Springer, 2013: 237-254

[27] Shi Leyi, Jia Chunfu, Lü Shuwang, et al. Port and address hopping for active cyber-defense [G] //LNCS 4430: Proc of the 5th Pacific Asia Workshop on Intelligence and Security Informatics. Berlin: Springer, 2007: 295-300

[28] Wei Feng. Research and implementation of the address and port hopping technology for network communication [D]. Wuhan: Huazhong University of Science and Technology, 2013 (in Chinese)
(丰伟. 网络通信中地址端口动态跳变技术的研究与实现 [D]. 武汉: 华中科技大学, 2013)

[29] Luo Yuebin, Wang Baosheng, Wang Xiaofeng, et al. RPAH: Random port and address hopping for thwarting internal and external adversaries [C] //Proc of the 14th IEEE Int Conf on Trust, Security and Privacy in Computing and Communications. Piscataway, NJ: IEEE, 2015: 263-270

[30] Lee H C J, Thing V L L. Port hopping for resilient networks [C] //Proc of the 60th IEEE Vehicular Technology Conf, Volume 5. Piscataway, NJ: IEEE, 2004: 3291-3295

[31] Badishi G, Herzberg A, Keidar I. Keeping denial-of-service attackers in the dark [J]. IEEE Trans on Dependable and Secure Computing, 2007, 4(3): 191-204

[32] Lin Kai, Jia Chunfu, Weng Chen. Distributed timestamp synchronization for end hopping [J]. China Communications, 2011, 8(4): 164-169

[33] de Oliveira R L S, Schweitzer C M, Shinoda A A, et al. Using Mininet for emulation and prototyping software-defined networks [C] //Proc of IEEE Colombian Conf on Communications and Computing. Piscataway, NJ: IEEE, 2014

[34] Linux Foundation. Open vSwitch [CP/OL]. (2014-08-14) [2014-12-25]. http://openvswitch.org/releases/openvswitch-2.3.0.tar.gz

[35] Gude N, Koponen T, Pettit J, et al. NOX: Towards an operating system for networks [J]. ACM SIGCOMM Computer Communication Review, 2008, 38(3): 105-110

[36] Sanfilippo S. hping3 [CP/OL]. (2005-11-05)[2014-12-14]. http://www.hping.org/hping3-20051105.tar.gz

Zhang Liancheng, born in 1982. PhD, lecturer. His main research interests include SDN security and flow watermarking.

Wei Qiang, born in 1979. PhD, associate professor, master supervisor. His main research interests include SDN security and network security (funnywei@163.com).

Tang Xiucun, born in 1980. PhD, engineer. His main research interest includes SDN security (tang-xc@sohu.com).

Fang Jiabao, born in 1993. Master candidate. His main research interest is network security (2014xdfjb@sina.com).