保证源和路径真实性的转发验证机制

徐 恪 杨 帆 吴 波 等
清华大学

关键词：路径验证 源验证 动态适应

引言

当前互联网的规模正在快速扩张，网络为用户提供的服务内容更加新颖，类型日趋多元化，用户对网络服务的安全性、可信可保障能力的需求也日益提高。随着网络安全事件的不断曝光，用户开始关注网络潜在的安全威胁。2015年，连一向以封闭安全著称的苹果移动操作系统iOS也“栽”在了源码病毒手里，应用程序受感染后可能造成用户私有数据外泄[1]，成为受到公众广泛关注的网络安全事件之一。网络承载着用户数据互联互通，而用户对网络交付的工作经过一无所知，即使是网络运营商也不能完全保证所有的服务策略被真实执行。因此，检验网络真实行为、保障策略可信执行的工作显得尤为重要。

源和路径验证是确保网络策略真实执行的基础。分布式拒绝服务攻击(Distributed Denial of Service, DDoS)仍然是目前互联网面临的最具威胁性和破坏性的攻击。源和路径是分布式拒绝服务攻击过程中涉及的关键要素，如果能够强化源和路径验证功能，无疑可以缓解分布式拒绝服务攻击的破坏效果并提升主动防御效能。

网络服务提供商在面向具有更高层次安全需求的重要大中型客户，逐步拓展多种增值业务时，借助源和路径验证功能，不仅可以保障客户数据流确实经过服务区节点成功送达目的端，而且可以帮助服务提供商确认所处理对象来自付费购买业务的客户。

早在1984年图灵奖颁奖仪式上，美国科学家Unix之父肯尼斯·汤普森(Kenneth L.Thompson)就发表了题为“对深信不疑之信任的反思”[2]的演说，认为没有相应的详细审查验证环节，用户不应该完全信任那些并不是由自己创造的代码，表达了对当时软件产业的担忧。相比软件系统，互联网发展至今已形成复杂协议交织的庞大体系，对网络协议执行情况进行检测验证更加具有重大意义。文献[3]在构建安全可信网络及保障路由交换设备行为安全可控方面提出建议，指出路由交换设备任何一种数据处理行为都必须事先定义和声明，并且验证其实际行为是否与之前的定义一致。基于此，我们提出了一种能够灵活适应网络环境变化的源和路径验证机制，重点关注路由转发策略是否真实执行，同时在设计时还考虑了验证处理流程对简便、快速、低开销方面的要求，确保其在高速骨干网络中的可实施性。

源和路径验证相关技术

在互联网传输数据过程中，数据发送源端、中间节点和目的端共同构成一条完整的转发路径。源和路径验证是指：以发送源端为起始，检查路径各

组成节点要素是否依次真实完成了与路由策略相一致的转发操作，进而确保从源端到目的端的数据可信传输。单独针对数据源进行检验的研究工作较多，例如网络攻击的源抑制、目的端源过滤防御、安全接入访问控制 [4~8] 等，其中文献 [8] 提出了一种源地址验证架构 (Source Address Validation Architecture, SAVA)，能够保证网络接收转发的任意数据包源地址的真实性。但是将源端作为路径检测的第一关键要素，并执行完整路径验证的研究工作相对缺乏。

基于回溯恢复的思路

面向分布式拒绝服务攻击追踪防御的相关方法主要包括基于路径回溯的随机包标记法 (Probabilistic Packet Marking, PPM) 和基于路径标识的包标识及过滤机制 (Pi)。这两类典型的方法都对后来的源和路径验证工作起到了一定的启发作用。随机包标记法 [9] 的基本原理是：路由器在转发数据包时按照一定的概率将部分路径信息（如当前转发节点的 IP 地址）标记在数据包中，随着一定数量的标记数据包陆续到达接收端，接收者根据标记数据包中的部分路径信息，完整恢复出整条传输路径，并最终检测出发送源端。但是，这类随机包标记法存在接收端存储累积开销较大、计算复杂度较高且路径回溯恢复难以保证实时性等不足。包标识及过滤机制 [10~12] 的主要特点是标记数据包所经过路径的各路由器的特征标识，即 Pi 值（如节点链路地址的哈希值最后 1 位或 2 位），而非路径信息本身，以较小的标记开销就可以完成源和路径结果的判断。然而，因为路径特征标识 Pi 值相比完整路径信息损失较多，不同源和路径的特征标识序列可能相同，导致检测所得到的源和路径结果真实性受到影响。

基于状态存储的思路

数据包由路由器的一个端口输入，从另一端口输出，在此过程中路由器会采集数据包信息以及有关状态，并将这些状态信息以日志等形式记录下来，这可作为不同研究目标的分析来源和参考凭证。例如，斯诺伦 (Snoeren) 等人 [13] 提出的基于数据包日志的 IP 追踪系统，即源路径隔离引擎 (SPIE)，追踪过程要求各路由器按需将记录信息传递给追踪管理器 (STM)，经查询分析获得追踪结果（如图 1 所示）。杜瓦艾利（Duwairi）等人 [14] 提出的 DLLT 算法以及景 (Jing) 等 [15] 提出的 DLS 算法都减少了日志信息量。文献 [16] 使用数据包历史信息进行网络故障检测，在一台多核服务器上搭建 NetSight 平台，可同时对多条 10 Gb/s 的链路流量进行包历史信息处理，具有更大网络规模的扩展能力。收集数据包在传输过程中各路由节点上的日志信息，借助全网拓扑进行路径重构，是实现源和路径验证功能的一种途径，但大量日志信息的存储、传递、处理等额外网络开销是必须考虑的因素。

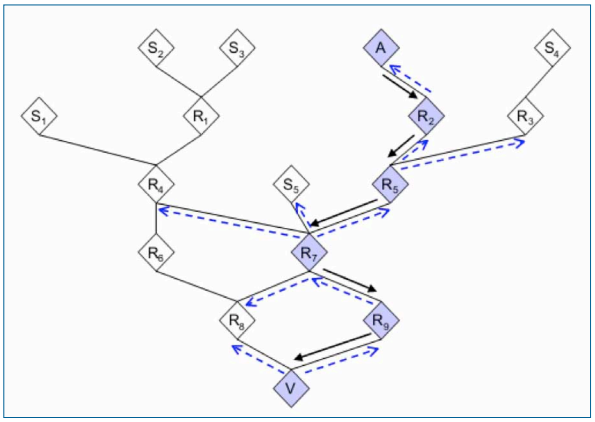

图1　追踪管理器STM查询恢复攻击图谱

基于加密认证的思路

在发送者事先预知数据如何传递给接收者时，预知方法可以从源路由、域间路由协议的 AS Path 通告或与服务运营商协定 [17] 等方式产生。此时，发送者可根据预知路径以加密方式生成一段源和路径验证信息，并封装插入数据包头部空间，提供给后续节点（含目的端）进行检验。例如，文献 [18] 提出的 ICING 源和路径验证方案能够在数据包传输过程中完成源以及当前节点之前路径是否真实可信的验证，实时对验证异常的数据包进行处理。然而，ICING 方案中的每个节点需要为所有后续节点计算并插入自己的加密字段，整个验证处理环节负担较大；同时，每个节点需要与其他各节点之间生成维

护共享密钥，进一步增加了状态管理的难度。文献[17]提出的OPT源和路径验证方案则使用了MAC算法，提出的验证信息结构更加完备，且降低了验证过程的开销。但是，选用加密认证的技术途径都无法绕开密钥的管理维护问题，OPT方案的工作准备阶段（或是事后追溯）都要借助公钥基础设施(Public Key Infrastructure, PKI)或相应机制实现整条路径上各节点密钥从源端到目的端的传递，目的端的最终验证需要获得路径各节点密钥(如图2所示)，不同会话的不同密钥都要进行传递，对大规模网络来说，其复杂度可想而知。

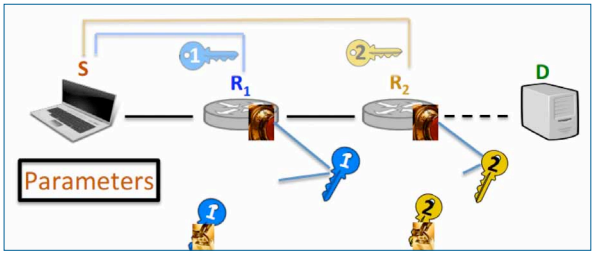

图2 OPT方案中密钥信息传递

对于源和路径验证问题，待检测验证信息的安全性非常重要。采用加密认证技术思路，如何做到使密钥生成使用和维护管理保持适度，且保证验证信息处理环节简便高效是研究者们探究的关键。

灵活简便的源和路径验证机制

我们在保障整体数据传输安全可信的基础上，以路由转发真实性为驱动，提出了灵活简便的源和路径验证机制。

源和路径验证机制架构

为承载源和路径真实转发验证机制，我们将整个网络架构组成划分为辅助和实施两个层次。辅助层包含各可信担保节点，这些可信担保节点在验证机制运行过程中承担认证加密所需密钥的维护管理，负责源和路径验证信息主体结构的生成，响应数据发送源端、目的端或网络服务商等机制申请。因此，可信担保节点既能够接收网络服务商提供的策略信息，也可以与数据收发双方实现交互。不同的可信担保节点还与所属网络传输节点分别构成独立的信任域。在信任域中可信担保节点和每一网络传输节点之间都维护了二者共享的密钥信息。全网可信担保节点的数量可以是一个或多个，其本身可以是某网络实体或虚拟功能，该功能既可以灵活地由涉及转发过程的网络服务商指定相应代理，也可以由涉及转发过程的某一可信网络节点代理，以保持辅助层可信担保节点的生命力。

实施层主要包含数据发送源端、目的端和各网络传输节点。这些节点直接执行整个验证机制环节的各个步骤。数据发送源端可以向辅助层可信担保节点发出验证信息结构申请，网络传输节点和目的端也可以向相应的可信担保节点发出安全可信相关机制申请，而且这些节点还会对可信担保节点的通告（例如查询通告、应急通告等）做出响应。源和路径验证机制架构和组成关系如图3所示。

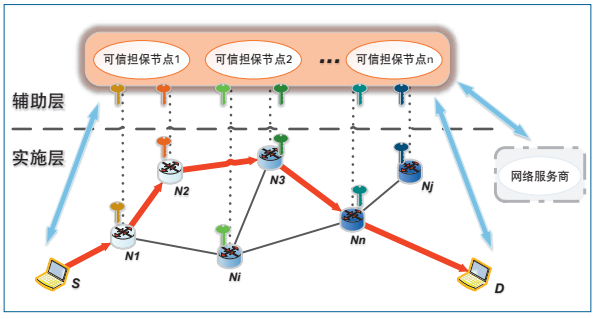

图3 源和路径验证机制架构和组成关系示意图

拍照拼接式源和路径验证结构及有关前提假设

现有研究一般将待验证的转发路径看成一个整体，而我们试图将以源端为起始第一要素的转发路径拆分成具有先后次序的多个片段，这些片段按照前后关系相互拼接构成源和路径验证信息结构的主体。真实转发验证过程分别针对每个片段依次逐个进行。如果所有片段均验证成功，则表明包括源端在内的完整转发路径验证成功。就像是预先对出行路线下载了一套从起点至终点逐一路段的可信拍摄照片，全套照片依次拼接展示了路线全景。出行

者从起点出发以照片为依据核对不同路段的实际情况，能实时判断当前的行进状态是否异常，直至到达终点，行程安全结束。

源和路径验证信息结构的核心部分是前后拼接的路径序列片段 Pic，片段 Pic 之间设计了部分节点信息重合，以保证整条路径的紧密连接关系。图 4 中，以第 n 个片段 Pic n 为例，需要包含前一节点 N_{n-1}、后一节点 N_{n+1} 的信息，并且用 N_n 节点密钥 Key_{Nn} 对该片段安全加密，特别是最后一个片段 Pic D 添加了源端 S 的信息，为目的端强化源验证功能提供可信证明。

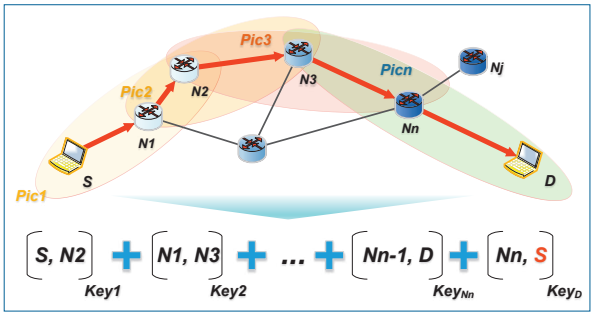

图4　源和路径验证信息结构核心部分示意图

为确保源和路径验证机制顺利运行，这里给出如下前提假设：(1) 发送者对数据如何传递给接收者能够与网络服务商达成一致，或者通过源路由等其他方式事先预知路径方案；(2) 各网络节点与可信担保节点之间有安全通道可以通信，通信的数据包不会在安全通道中出现拥塞甚至丢失；(3) 各网络节点维护自己与相邻节点的对应关系；(4) 源端到目的端的一次会话过程中，参与会话的各网络节点保持松散的时间同步，如采用网络时间协议 (Network Time Protocol, NTP) 实现时间同步。

基础机制

整个机制的工作流程可以分为四个阶段来描述：辅助阶段、源端初始化阶段、网络节点验证处理阶段和目的端验证处理阶段（如图 5 所示）。

辅助阶段　发送者与网络服务商协定统一路径方案后，将该方案告知可信担保节点。可信担保节点与网络服务商完成方案确认后（包括身份验证、方案核查等预处理），采用加密算法加工生成各路径序列片段 Pic，并拼接生成待验证路径序列 PS，随后将这些生成的序列返回给数据发送申请者 S。各片段 Pic 中已插入时间期限参数 Time.exp，以保证该会话过程中源和路径验证信息结构有效。

源端初始化阶段　数据发送源端按照会话编号 Session Num 关联相关参数，包括路径长度 Len、路径序列索引 Path Index Sequence、待验证路径序列 PS、载荷加密摘要 $H(P)_{KeyS}$ 等内容，合并成完整的验证结构封装入数据包头部，执行数据发送。

网络节点验证处理阶段　中间网络节点 N_i 收

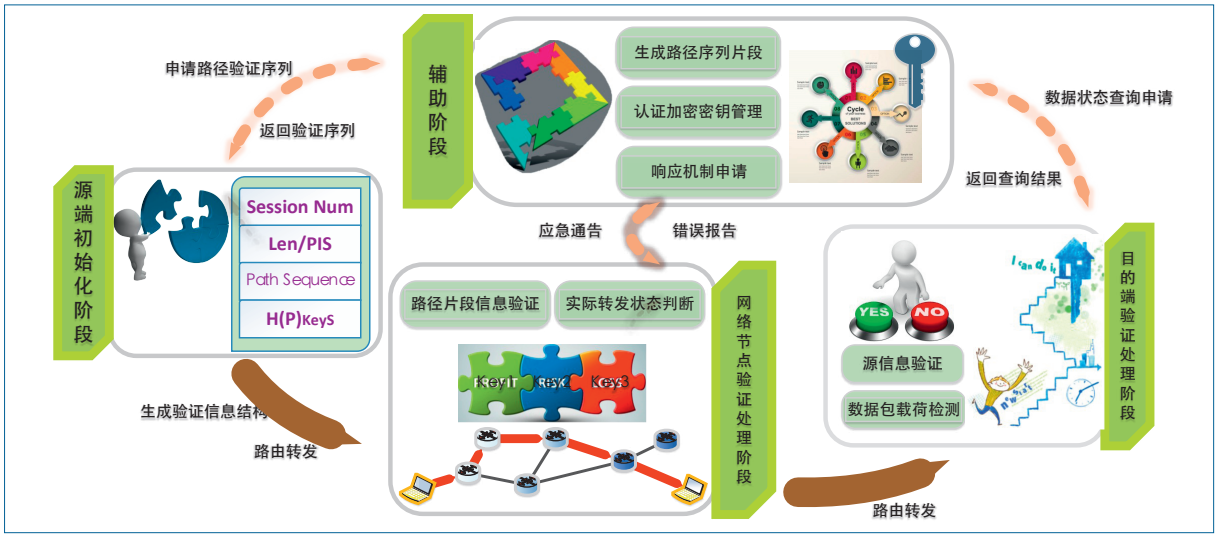

图5　源和路径验证基础机制工作过程示意图

到数据包后，在源和路径验证信息结构中提取出需要验证的片段 Pic i 进行验证计算。首先，由于该片段生成时的加密密钥 Key_i 只有可信担保节点与之共享，所以使用密钥 Key_i 能够成功解密该片段，表明节点 N_i 属于数据包的原协定路径，片段内部信息被认为是经过可信担保节点的事先确认，因此真实有效。其次，提取数据包的实际到达情况，并以解密后的片段内部信息为依据进行判断，如果在正常时间期限 Time.exp 内到达，实际转发情况与片段内部信息一致，表明当前数据包路由转发情况可信。最后，无法通过以上验证步骤的数据包将被丢弃，网络节点 N_i 向可信担保节点反馈相应错误报告。通过验证的数据包，其封装验证结构无须任何修改更新，直接发送给下一节点。

目的端验证处理阶段 数据包在途中未被丢弃且成功到达目的端后，除执行上述网络节点验证步骤外，还要对源信息和数据包载荷进行检测计算（载荷验证环节可随机执行）。如果检测结果正常，则表明包括源端在内的整条路径真实完成了与路由策略相一致的转发操作，进而担保从源端到目的端的数据可信传输。

源和路径验证的基础机制中，中间路由节点的验证过程不需要进行任何更新操作，只须完成一次解密（或摘要）计算，极大降低了处理开销，同时也给进一步简化机制打好了基础。例如某中间节点可以基于会话数据包的正常验证结果，启动任意较短时间间隔的计时，在计时间隔内可以只执行会话编号 Session Num 和实际接收情况验证，而无需做会影响效率的验证结构解密计算，也同样能够保证该会话数据包传输可信。在计时结束时恢复完整基础机制，并等待下一次计时开始，再次进入简化模式实现处理加速。

在考虑机制处理效率的同时，其对网络环境的适应能力更加重要，机制只有贴合网络实际运行情况，才能发挥出最大的效能。现实网络环境下，链路状态会因为故障、切换等原因发生变化，但目前针对源和路径验证问题的相关研究缺乏应对网络动态变化情况的策略，为此，我们在基础机制运行架构基础上，提出了源和路径验证的增强机制。

增强机制

源和路径验证增强机制建立在基础机制的基本功能之上，主要包括应对网络环境动态变化的机制灵活适应，网络受到安全威胁躲避潜在恶意节点时的机制快速迁移以及补充基础机制相关查询挑战、响应申请等。

下面以网络节点 N_i 探测出原协定路径方案的下游发生链路故障为例，说明增强机制的关键步骤：

1. 网络节点 N_i 向信任域可信担保节点发出带会话编号 Session Num 标识的链路故障应急申请。可信担保节点联合发送源端规划备用路径方案，重新生成源和路径验证序列及源和路径验证信息结构。

2. 发送源端将新生成的源和路径验证信息结构重新封装到该会话后续数据包中，保证数据发送的继续进行，而可信担保节点同步向网络节点 N_i（也可能是路径变更交叉节点）下发新生成的源和路径验证序列，网络节点 N_i 依据收到序列重新组织源和路径验证信息结构（方法与源端相同），并将新验证结构替换封装入该会话陆续到达的数据包头部，确保数据包的源和路径验证工作沿调整后的路径继续执行。

3. 网络节点 N_i 执行对验证片段 Pic i 中下一节点 N_{i+1} 信息的检测，此时收到的会话数据包验证片段 Pic i 所指示的下一节点 N_{i+1} 信息仍然是下游故障节点，直到检测到下一节点信息 $N_{i+1}' \neq N_{i+1}$ 且属于调整后的路径，网络节点 N_{i+1} 即可以停止对该会话数据包验证结构的替换插入步骤，表明整个机制同步适应工作完成。

整个增强机制的灵活调整方法较为简单，源和路径验证信息结构是检测机制的关键安全要素，这一要素的灵活可拼接能力也奠定了增强机制灵活动态的技术基础，填补了相关研究工作在网络动态环境下应对策略的空白。

安全能力分析

从构建潜在对手模型的角度分析，有两方面

表1 潜在安全威胁与机制抵御能力分析

潜在安全威胁	验证结构解密结果	路径信息检测结果	载荷验证结果	机制抵御关键点及说明
重放攻击	√	√	√	当time.exp时间参数过期时，验证结构内部的路径信息检测将会失败，发送错误报告。
假冒篡改	√	√	×	在目的端，载荷加密摘要值比对将会失败，发送错误报告。
恶意转发（转发路径跳过节点、增加节点、错误顺序、存在隐匿节点等）	√	×	√	当前验证节点、检测数据包实际到达情况和路径序列片段不一致，发送错误报告。
	√	×	×	
流重定向或共谋攻击	×	×	√	流重定向，当遇到不属于预定路径的网络节点时，该节点无法得到路径相关密钥，自身密钥无法成功解密验证结构，判断出存在异常输入，发送错误报告。 共谋攻击，共谋节点之间出现了恶意转发情况，被转发会话数据包只要经过一个正常（非恶意）节点，该节点就会因为无法成功解密验证结构，判断出存在异常输入，发送错误报告。
拒绝服务式攻击（可信担保节点遭受拒绝服务攻击）				当前可信担保节点将可信担保功能转移给其他与网络服务商确认的正常可代理节点。
网络节点的密钥信息泄露				可信担保节点下发应急通告，密钥泄露节点更换会话密钥信息，且启动增强机制进行数据传输的安全同步适应过程。

的威胁：一是针对路由真实转发的安全威胁，主要通过改变数据包头部信息、数据转发路径情况以及数据包载荷内容等方式对数据传输过程产生恶意影响；二是针对验证机制本身的安全威胁、拒绝服务式攻击（可信担保节点遭受拒绝服务攻击）、网络节点密钥信息泄露等。我们综合考虑各种因素，结合不同的机制验证结果，对潜在的以恶意转发、流重定向、假冒篡改、重放攻击、隐匿攻击等为代表的攻击情况进行归纳分类，可以列出机制抵御攻击的关键点及说明（见表1）。

结语

面对日益复杂的网络安全形势，各类加固网络协议的安全策略不断涌现并逐步受到关注。如果说网络协议的升级防护至关重要，那么协议策略执行的真实性检验同样意义重大。灵活简便的源和路径验证机制引入了拍照拼接式验证信息结构，控制检验信息传递过程中无须迭代更新，从而极大地提升了路由节点机制运行效率。源和路径验证增强机制，能够实现验证功能受控调整迁移，促进验证机制发挥最大潜在效能，最终保障数据信息传输的真实安全性。■

徐 恪

CCF杰出会员、本刊编委。2011 CCF青年科学家奖获得者。清华大学教授。主要研究方向为计算机网络软件和P2P等大规模分布式系统。
xuke@mail.tsinghua.edu.cn

杨 帆

清华大学硕士研究生。主要研究方向为计算机网络体系结构、网络安全等。
y-f14@mails.tsinghua.edu.cn

吴 波

清华大学博士研究生。主要研究方向为计算机网络体系结构、网络安全等。
wub14@mails.tsinghua.edu.cn

其他作者：吴建平 沈 蒙

参考文献

[1] http://tech.sina.com.cn/mobile/n/n/2015-09-22/doc-ifxhytwp5513912.shtml.

更多参考文献：www.ccf.org.cn/cccf