



专题：数据网络技术与应用

基于区块链技术的可信网络

李聪, 雷波, 解冲锋, 李云鹤

(中国电信股份有限公司北京研究院, 北京 102209)

摘要: 随着网络安全问题不断频发, 传统补丁式外置安全方案已经不能满足业界需求, 产业各方更希望从网络架构层实现内生安全, 因此提出了去中心化可信网络架构。在研究现有网络底层协议安全的基础上, 提出了基于去中心化技术/区块链技术的可信网络的架构方案, 能够有效地解决现有网络缺乏内生安全的问题, 并在中国下一代互联网 (China's Next Generation Internet, CNGI) 进行了验证。此方案从协议层实现了网络安全, 避免恶意网络攻击或者因配置失误造成的网络故障。

关键词: 网络架构; 去中心化; 网络安全

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019226

Trustworthy network based on blockchain technology

LI Cong, LEI Bo, XIE Chongfeng, LI Yunhe

Beijing Research Institute of China Telecom Co., Ltd., Beijing 102209, China

Abstract: With the frequent occurrence of network security issues, the industry had not satisfied the patch-based external security solution, and it was hoped that the endogenous security could be realized from the network architecture layer. The decentralized trustworthy network architecture was proposed. Based on the research of the security of existing network underlying protocol, a trustworthy network architecture based on decentralization technology was proposed, such as blockchain technology, which could effectively solve the problem of lack of endogenous security in existing networks. Layers implement network security to avoid malicious network attacks or network failures caused by configuration errors.

Key words: network architecture, decentralization, network security

1 引言

近几年, 全球网络攻击事件频发, 世界经济

论坛的《2018 年全球危险报告》称, 目前网络攻击成为自然灾害和极端天气以外的全球第三大风险因素。随着 IT 技术的进步与发展, 各个行业的

收稿日期: 2019-07-29; 修回日期: 2019-10-10

基金项目: 国家重点研发计划基金资助项目 (No.2018YFB1800100)

Foundation Item: The National Key Research and Development Program of China (No.2018YFB1800100)

业务不断地进行数字化转型,维护网络安全的工作已经史无前例的重要。目前网络安全形势非常严峻,习总书记提出:“没有网络安全就没有国家安全。互联网核心技术是我们最大的‘命门’,核心技术受制于人是我们最大的隐患。”网络安全已上升为国家级战略,建立安全可信的下一代互联网是世界各国的共同关注点。

面对日益严重的网络安全态势,需要从源头解决如今的网络安全问题,建立具有安全性的网络技术体系。目前网络安全问题的根本原因在于互联网体系结构的设计本身存在缺陷,网络层是互联网体系结构的核心,由传送格式、转发方式、路由控制三大要素组成。但是目前终端编址的安全可信要素仍有缺失,终端的隐私面临挑战。现有的互联网在设计之初,没有严格地对转发分组的IP源地址进行验证,导致大量伪造源地址分组的出现以及基于此的大量安全攻击,对网络安全、网络管理和网络计费等方面提出了挑战。随着物联网市场的快速发展,物联网终端的数量呈指数级增长,预计2020年终端数量将增长至204亿台,其安全风险也日益提高。

目前路由控制策略也较为简单,路径安全无法保障,以互联网域间路由协议——边界网关协议(border gateway protocol, BGP)来说,该协议用于自治系统之间交换网络侧可达信息,是互联网路由基础设置中的重要组成部分。但是该协议在设计之初没有设计相关的机制以保障域间路由系统的安全,存在着明显的安全漏洞。在BGP路由传播过程中,各自治系统之间只向外通告自己所拥有的地址块,其他自治系统会无条件地信任并接受对等体通告的路由信息。边界网关协议中没有对网络中传播的路由信息的真实完整性进行验证的功能,错误的路由信息将在网络中传播,会导致许多安全问题发生。

网络层的相关协议在设计之初对于安全性的考虑不足,补丁式的外置安全方案无法从源头上

保证网络的安全性。为建立完整的安全互联网体系结构,需要从网络架构层出发,以实现网络的内生安全。本文提出一种可信网络架构,基于去中心化技术保证终端标识以及路由交换信息的可信性。这样的网络架构方案能有效解决现有网络缺乏内生安全的问题,能从协议层实现网络安全,避免恶意网络攻击或者因配置失误造成的网络故障。

2 目前存在的问题及解决方案

2.1 常见的路由安全问题

在BGP中,互联网中任何一个自治系统都可以通过发布路由信息来影响其他自治系统的决策,这样的特性容易导致一个错误配置或者恶意攻击使得互联网受到大规模的影响。目前典型的边界路由协议安全问题有以下3种。

(1) BGP 前缀劫持

前缀劫持指某个自治系统宣告一个属于其他自治系统或尚未分配的前缀。由于路由器不会对接收到的前缀源信息进行验证,会导致流量被转发至错误的自治系统中。此类问题出现的主要原因是内部网关协议(interior gateway protocol, IGP)到BGP的路由重分发配置错误,黑客可通过伪造BGP update中的网络层可达信息(network layer reachability information, NLRI)来实现前缀劫持。

(2) BGP 路径劫持

使用某个伪装的自治系统(autonomous system, AS)制造一个更短的路径到达某个前缀,那么其他的AS想要路由到此前缀时就会沿着这个伪装的路径,进而受到感染,之后攻击信息会向其他AS传播,造成BGP路径劫持。

(3) BGP 路由泄露

路由泄露是将路由通告给了非法对象,导致流量重新定向。虽然其信息本身是合法的,但是使用了错误的策略。路由泄露会造成源网络终端或者AS穿越、ISP(internet service provider, 互



联网服务供应商) 穿越等问题。

近年发生了许多网络安全事件, 以下列举了几件典型的由于网络协议架构缺乏安全性造成的安全事件。

- 2017 年, 由于美国谷歌公司的工程师配置错误, 导致了路由泄露。此次事件中, 谷歌劫持了日本运营商 NTT 的流量, 使得日本国内的流量传送至谷歌在美国的数据中心, 日本与美国之间的链路拥塞严重并出现了数据分组丢失, 此次事件导致日本互联网中断 40 min。
- 2018 年, 美国亚马逊公司的域名服务器遭到了 BGP 路由劫持攻击, 此次事件中用户流量被重定向到位于俄罗斯的加密“货币”网站, 据称窃取了价值近 2 000 万英镑的数字“货币”。
- 2019 年, 由于瑞士 Safe Host 公司的自治系统 AS21217 错误地更新了路由器, 导致中国电信传输欧洲移动流量持续两小时, 在此期间银行交易等应用无法使用且全球的通信质量下降。

2.2 现有的解决方案

目前为解决 BGP 存在的安全缺陷, IETF 提出了互联网码号资源公钥基础设施 (resource public key infrastructure, RPKI) 用来防御日益频繁的互联网路由劫持事故。该解决方案通过签发和认证一种特定格式的 x.509 数字证书和数字签名, 帮助路由器检验 BGP 消息的真实性, 从而增强 BGP 的安全, 帮助避免互联网路由劫持。

RPKI 的认证体系依附于互联网码号资源分配系统, 互联网码号分配系统采用层次化的结构。系统以互联网码号分配机构为根节点, 根节点将互联网码号分配给向 5 个 RIR, RIR 再将资源向其下级节点如本地互联网注册机构、国家级互联网注册机构等, 然后下级节点再逐级向下分配。为实现地址与 AS 号码的认证, 路由器需要使用自己的私钥为路由起源认证 (route origin author-

ization, ROA) 的信息进行签名。所有的证书及 ROA 均通过一套分布式的 RPKI 证书库系统进行集中和分发, 每台 BGP 路由器都可以从所属的 ISP 分发点获取各类证书和 ROA。

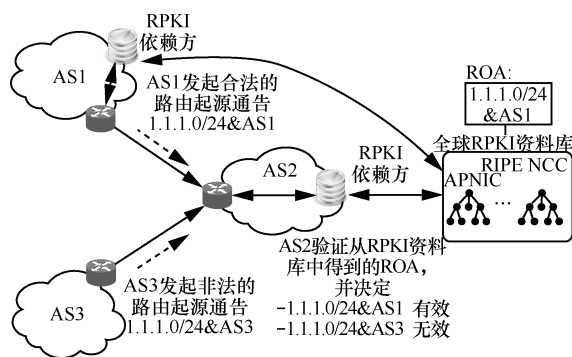


图1 RPKI 层次化运行机制

但是这种自上而下的中心化认证体系存在问题, 在这样的系统中上级节点是下级节点的资源分配者和资源证书的颁发者, 根节点能决定下级所有节点的行为策略。这样的结构也导致权力高度集中, 一旦被黑客攻击或者错误配置会导致全局系统受到恶劣影响。由于存在系统性风险, 即使部署了 RPKI 方案仍不足以抵御路由泄露等安全性问题。所以本文提出了去中心化的可信网络架构, 从根本上消除中心化架构的风险性, 从协议层实现网络安全, 避免恶意网络攻击或者因配置失误造成的网络故障。

3 基于去中心化的网络架构

从第 2 节的分析可以看出, 网络安全问题频发造成了广泛的不良影响, 现有的解决方案难以实现网络的内生安全。去中心化的网络架构是解决网络安全问题的可行方案, 方案中引入区块链技术实现去中心化的基础设施建设。区块链概念起源于比特币应用, 其本质上是一种去中心化的记录技术, 其中存储使用密码学方法相关联产生的数据块。区块链具有以下几项特征。

(1) 去中心化

区块链中的数据由所有的节点共同维护, 整

个系统中不需要集中的控制每个参与节点即可达成共识,从而各个节点形成了一个分布式的系统。

(2) 安全性

系统中通过密码学的相关机制,系统中的参与节点共同维护一条不断增长的链,这个数据链中只能增加记录,无法删除或者修改,这样能够保证区块链数据的安全性。

(3) 开放性

区块链中的数据对每个节点开放,每个节点都可以获得一份完整的数据记录。

由于区块链具有以上技术特性,所以把区块链技术应用至网络基础设施的建设中可解决网络安全问题。区块链技术最早用于记录比特币交易的账目历史,其支持了海量的交易记录。当区块链技术应用用于网络时,网络中 IP 地址、AS 号、域名映射关系等信息的变更可以理解为一次交易,交易会导致账本状态的改变,记录网络数据映射关系的账本由若干个组织的网络基础设施共同维护。去中心化可信网络基础设施中包括提供共识服务的网络节点 (orderer)、维护账本信息的网络节点 (peer) 和访问并使用账本的网络节点。系统中应用程序可发送交易请求,维护账本信息的多个节点通过验证签名的方式确认提交者是否有权执行操作,应用程序收集以上背书结果并提交至共识服务节点,共识服务节点执行共识过程并生成区块。区块中记录一段时间内发生的交易和状态结果,是对当前账本状态的一次共识。这样记录了网络信息映射关系的区块形成了线性的链表结构,这个链表只允许添加不允许删除,能够保证网络映射信息的安全性。

去中心化的网络架构如图 2 所示,整体由网络设施层、去中心化互联网基础设施功能层以及应用层 3 层组成。互联网的网络设施形成去中心化的系统结构,各个 ISP 以联盟链成员的身份加入此联盟链系统中。在整个系统中没有特定的特权节点,所有的区块链节点以去中心的方式形成

共识。去中心化互联网基础设施功能层中每个 ISP 的网络基础设施共同维护一个共同的分布式账本,主要完成互联网名字空间映射管理,名字空间管理主要实现 IP 地址、终端标识、AS 号、域名间的映射记录管理,并将映射记录分布式的存储于各个节点之间。通过名字空间管理可以实现以下 3 个方面的可信验证。

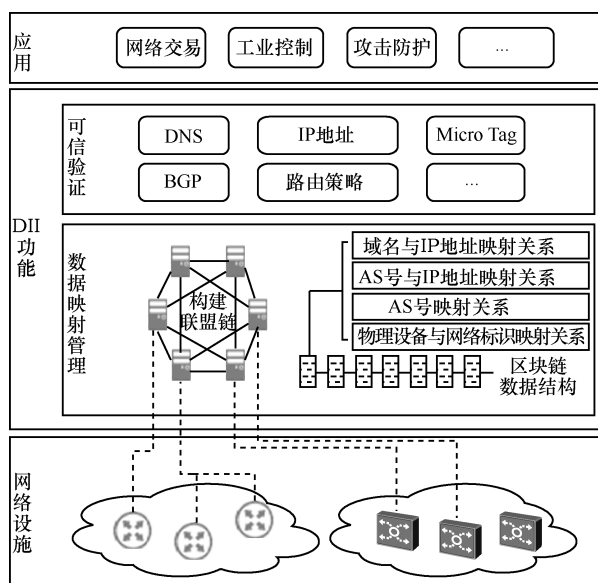


图2 去中心化网络架构

(1) 标识与地址可信

接入网络的实体需要通过 ID 或 IP 地址进行标识,ID 与 IP 的归属权可信性决定了身份的合法性,可信的身份管理是通信可信的基础。通过对终端标识进行去中心化的存储校验能够解决网络中 IP 分组“从哪来”以及“谁负责”的问题,从网络体系结构上保证网络信息来源的真实和可追溯,提高了互联网管控能力,为构建可信任的下一代互联网提供了重要的技术基础。

(2) 域名解析与映射

网络应用与服务依赖于域名解析系统,域名映射信息的可靠性与架构可信性决定了依存其之上的网络服务能否正常工作。通过分布式的域名与 IP 地址之间的映射管理可以避免一些域名劫持等安全问题的发生。



(3) 路由可信

域间路由的可信性决定了数据分组可以被按照正确的路径转发至对端，需要有能够抵抗恶意劫持或配置失误的影响，保证网络良好的连通性。通过 IP 地址与 AS 号之间的映射关系可以计算出相应域间路由，防止由于恶意攻击或者错误配置导致的前缀劫持和路径劫持等路由安全问题的发生。

去中心化的网络架构中顶层为应用层，应用层可以基于底层网络的去中心化可信能力，为各种业务提供可信应用，例如去中心化的终端标识地址验证服务、BGP 源地址验证、DDoS 攻击防御等方面的业务应用，从而提供网络可信服务能力，避免恶意网络攻击造成网络故障的发生。

4 面向去中心化网络的实践

4.1 实验环境搭建

本次实验基于去中心化的网络架构搭建环境，基于域间联盟创建区块链系统提供去中心化的 IP 地址分配、所有权管理和资源映射功能，实现真实地址验证和 BGP 安全（源验证、路径验证、路由泄露）解决方案和检测告警。

本次实验依托 CNGI 搭建网络拓扑，CNGI (China's Next Generation Internet) 是以 IPv6 为核心的中国下一代互联网。CNGI 为国家级战略项目，由工业和信息化部、科技部、国家发展和改革委员会、教育部、国务院信息化工作办公室、中国科学院、中国工程院和国家自然科学基金委员会 8 个部委联合发起，并经国务院批准于 2003 年启动。CNGI 骨干网拓扑如图 3 所示，包括 6 个主干网络，并在上海、北京分别设置互联中心来实现各子网间互通以及获取外部路由信息，该网络通过国际联网和交换中心（CNGI6IX）可以与国际网络互连。CNGI 内采用 ISIS（intermediate system to intermediate system）协议作为 IGP，北

京互联中心和上海互联中心通过 EBGp 连接，网内的所有设备均运行 IBGP。中国电信负责 CNGI 中一个主干网络的规划建设以及上海互联中心的维护管理，中国电信的 CNGI 拓扑如图 4 所示，目前一期测试由中国电信 CNGI 提供测试网络。实验对去中心化互联网基础设施（decentralized internet infrastructure, DII）的基本功能进行测试，包括 IP 地址管理、AS 号码管理、ROA 管理、AS 邻居信息管理、BGP 路由源验证、路径验证、路由泄露检测等功能，未来第二期将由多参与方搭建多节点测试床进行全功能集测试。

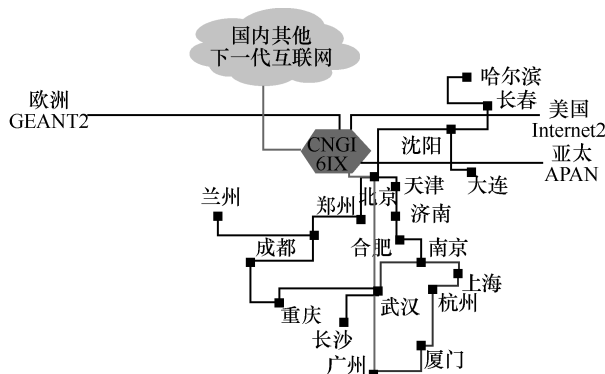


图3 中国下一代互联网骨干网拓扑

整个测试系统的组成包括基于 Hyperledger Fabric 开源分布式账本框架开发的区块链系统、具有 BGP 安全功能的边界路由器以及介于之间的信赖方和 BGP 监控协议服务器模块。基于 CNGI 的去中心化互联网基础设施测试床结构如图 5 所示，测试床中包含 5 台路由器和 2 台服务器。4 台路由器上分别配置现网 CNGI 自治域号（AS4134）和 3 个测试自治域号，路由器 4 与 CNGI 现网中北京网管中心型号为 NE80E 的路由器相连。两台服务器分别与路由器 1 和路由器 4 连接，分别部署 Hyperledger Fabric 节点，节点中包括共识服务功能、Fabric CA 功能、对等体功能，拓扑中路由器需要支持并开启信任体、BGP 监控协议（border gateway protocol monitoring protocol，BMP）服务。路由器与服务器之间配置

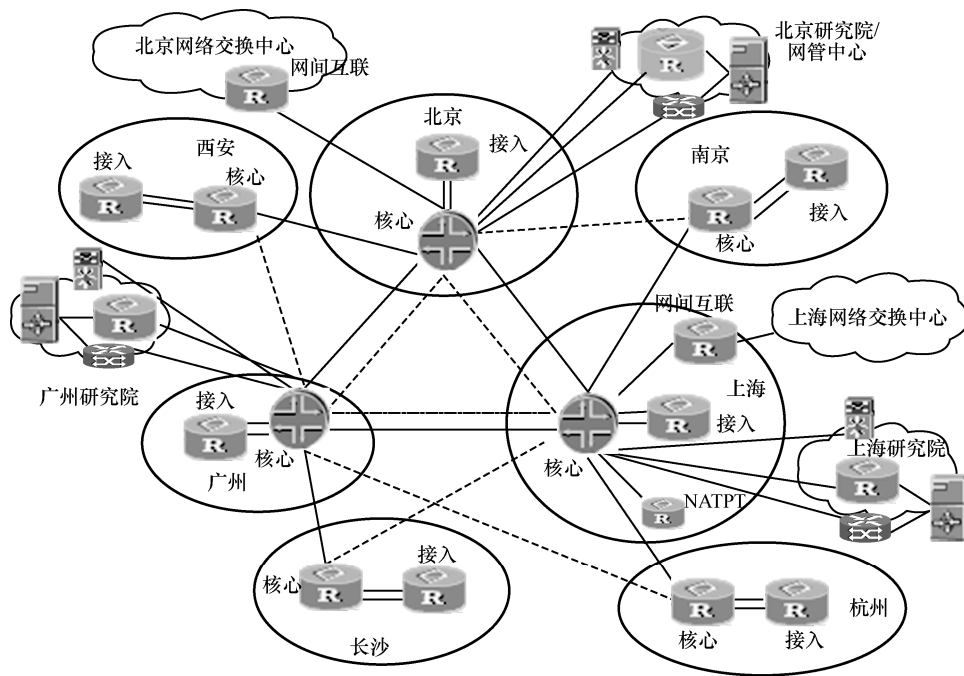


图 4 中国电信 CNGI 网络概况

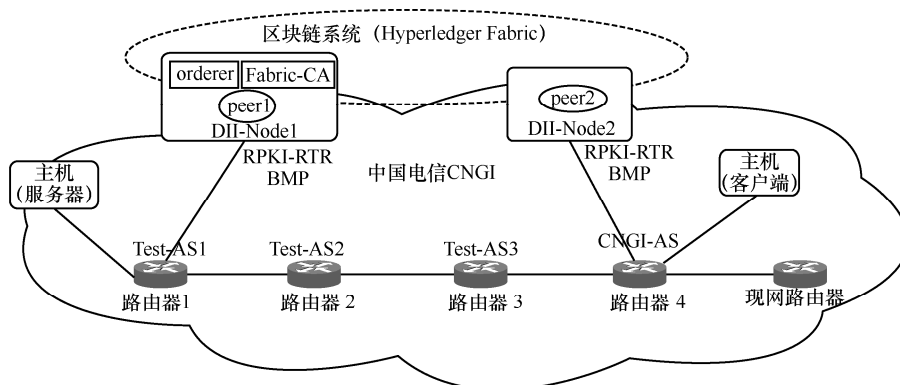


图 5 测试床结构

RPKI-RTR 和 BMP 接口：RPKI-RTR 用于 ROA 数据同步，BMP 接口用于将路由器本地路由信息同步到区块链节点。另外两台服务器分别部署视频应用服务器和视频客户应用用于流量测试。实验中采用 eNSP 软件模拟黑客进行前缀劫持、路径劫持攻击。

4.2 实验典型案例

此次实验中对于 BGP 安全、IP 地址管理、ASN 管理等多种场景进行了模拟验证，本文将对 BGP 安全的 3 个典型场景的实验进行说明。

(1) 前缀劫持防御

前缀劫持防御场景中实验拓扑如图 6 所示，主要模拟了黑客对运营商 AS4134 域中的 IP 地址发起了前缀劫持攻击，导致正常的视频服务中断，运营商通过 DII 系统发布 ROA 交易，全网达成共识并同步该信息，前缀劫持攻击失效，视频服务恢复。

在此场景中视频客户应用位于 AS100 域内，视频应用服务器在 AS1314 中，AS1314 向 AS100 宣告正确的路由（2F00:800::/32, [200,300,4134]），视频客户应用能够通过

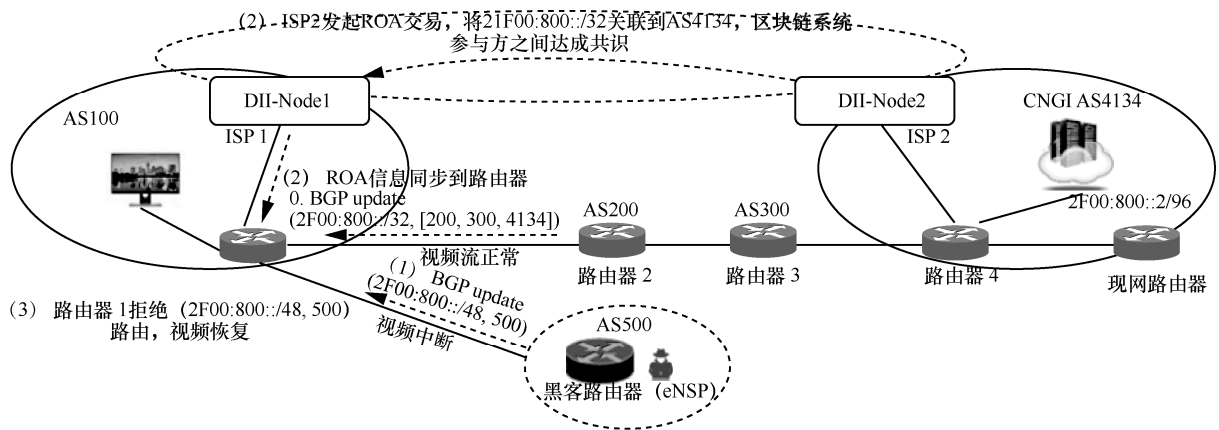


图6 前缀劫持测试拓扑

2F00:800::2 地址访问视频应用服务器并正常观看视频。黑客控制或冒充 AS500 发起更长前缀劫持,向 AS100 宣告(2F00:800::/48,500),AS500 由 eNSP 进行模拟实现攻击行为。AS500 发布前缀劫持路由并将该路由宣告给 AS100,AS100 根据“最长前缀匹配”原则,将去往 2f00:800::2 地址选择 AS500 发来的路由进行转发,意味着 AS500 对 AS100 发起前缀劫持攻击,出现路由黑洞,视频中断。

ISP2 发现前缀被劫持,通过 DII 系统发布 ROA 交易,将 2F00:800::/32 关联到 AS4134,AS 之间达成共识后,将 ROA 数据同步到路由器。ROA 信息发布后,路由器 1 获得该条 ROA 信息,拒绝 (2F00:800::/48, 500) 路由,引发前缀劫持的长前缀路由失效,视频服务恢复。

(2) 路径劫持检测告警

路径劫持防御场景中实验拓扑如图 7 所示,主要模拟了黑客发起对运营商的路径劫持攻击,导致正常的视频服务中断,DII 系统检测到该路径劫持攻击后发起告警,运营商根据告警信息,进行相应处理,路径劫持攻击失效,视频服务恢复。

在此场景中 ISP1、ISP2、ISP3 正常宣告 AS 邻居信息,配置视频应用服务器的地址,并向 AS100 宣告正确的路由保证视频客户应用能够正常访问视频应用服务器。黑客通过 AS500 发起路径劫持,向 AS100 宣告(2f00:800::/48,[500,4134])。AS500 由 eNSP 进行模拟实现攻击行为。AS500 发起路径劫持后,AS100 根据“最短路径”原则,将去往 2f00:800::2 地址选择 AS500 发来的路由进行转发,意味着 AS500 对 AS100 发起路径劫持攻

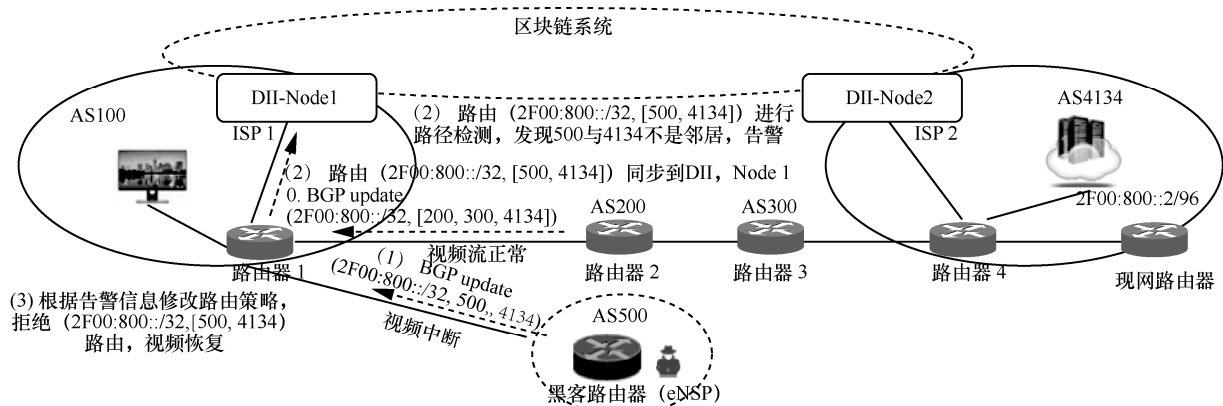


图7 路由劫持测试拓扑

击,出现路由黑洞,视频中断。DII节点1对该路由进行路径检测,提示500与4134不是邻居,发出路径劫持告警,告警信息中包含具体的路径劫持信息。ISP1查看告警信息并根据告警信息修改路由器1上的路由策略,过滤(2f00:800::/32,[500,4134])路由,在ISP1修改路由策略后,视频恢复。

(3) 路由泄露检测告警

路由泄露检测告警场景中实验拓扑如图8所示,主要模拟了由于某一运营商误配置造成路由泄露,导致正常的视频服务中断,DII系统检测到路由泄露后,发起告警,运营商根据告警信息,对误配置进行处理,视频服务恢复。

在此场景中AS100-AS300和AS200-AS4134为服务提供者自治域与客户自治域的关系,AS100-AS200和AS300-AS4134为对等体关系。AS300误配与AS100为服务提供者自治域与客户自治域的关系,AS300将其对等体AS4134的路由泄露给AS100。AS300发生误配置后,路由(2f00:800::/32,[300,4134])泄露给AS100,AS100根据“客户自治域优先”原则,将去往2f00:800::2地址选择AS300发来的路由进行转发,但AS300不是中转自治系统,它将转发流量丢弃,视频中断。路由(2f00:800::/48,[300,4134])同步到DII节点1,DII节点对该路由进行路由泄露检测,发现

其违背了路由泄露规则,即从对等体来的路由发给了服务提供者自治域,DII节点发出路由泄露告警。AS300查看告警信息,根据告警信息改回正确的配置,即将与AS100的关系纠正为客户自治域与服务提供者自治域关系,纠正配置后,路由(2f00:800::/48,[300,4134])不再泄露给AS100,视频恢复。

除此之外,本次实验还对于IP地址和ASN管理功能进行了测试,能够实现网络服务供应商用户和终端用户两种用户对IPv6地址和ASN的申请、转让以及终端用户对IPv6地址转让、续费和召回的操作。实验中也对创建、删除ROA和AS邻居关系的功能进行了测试,当用户输入非其拥有的IPv6地址和AS邻居关系时,系统都能识别错误并显示创建失败的信息。以上的实验说明在去中心化的可信网络架构下通过对IP地址以及AS号等信息的映射管理,可以实现对常见的BGP安全问题的预防检测及告警,运营商能够在网络攻击发生时自动告警并进行应急响应保证相应业务快速恢复服务。

5 结束语

本文提出的新型去中心化的网络架构,基于区块链技术建立了网络基础设施,能够从网络架构层来实现内生安全。内生安全体现在自适应性

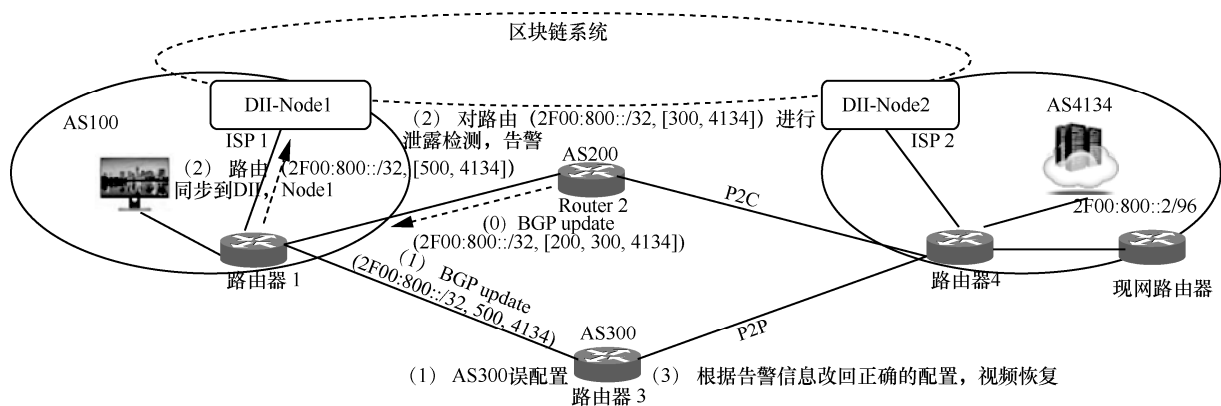


图8 路由泄露测试拓扑



上,此网络架构在一般的网络攻击发生时能够自动发现网络中的异常情况并进行相应的处理使业务自动恢复正常;内生安全也体现在自主性上,各个运营商作为区块链内容的生产者也是内容的使用者,能够从自身的安全需求与业务出发,建立自主的安全能力。去中心化的可信网络架构通过对互联网名字空间映射管理,能够保证终端标识和路由控制两方面的安全性,从而实现网络中端到端的安全保障。本系统模型的简单原型实现证明了该体系结构的可实施性和可部署性,能够对常见的网络安全问题进行响应。

参考文献:

- [1] 吴德福.《2018 全球风险报告》发布网络攻击排名前三[J]. 计算机与网络, 2018, 44(4): 1.
WU D F. 2018 global risk report ranked the top three for cyber attacks[J]. Computer & Network, 2018, 44(4): 1.
- [2] BUSH R. Origin validation operation based on the resource public key infrastructure (RPKI): RFC 7115[S]. 2014
- [3] HUSTON G, MICHAELSON G. Validation of route origination using the resource certificate public key infrastructure (PKI) and route origin authorizations (ROA): RFC6483[S]. 2012.
- [4] LEPINSKI M, KENT S. An infrastructure to support secure internet routing: RFC 6480[S]. 2012.
- [5] IETF. Problem definition and classification of BGP route leaks:7908[S]. 2016
- [6] 刘冰洋, 杨飞, 任首首, 等. 去中心化互联网基础设施[J]. 电信科学, 2019, 35(8): 74-87.
LIU B Y, YANG F, REN S S, et al. Decentralized internet infrastructure[J]. Telecommunications Science, 2019, 35(8): 74-87.
- [7] CACHIN C. Architecture of the hyperledger blockchain fabric[C]//Workshop on Distributed Cryptocurrencies and

Consensus Ledgers, July 25, 2016, Chicago, USA. [S.l.:s.n.], 2016.

- [8] ANGIERI S, GARCÍA-MARTÍNEZ A, LIU B, et al. An experiment in distributed internet address management using blockchains[J]. arXiv:1807.10528, 2018.

[作者简介]



李聪 (1993-), 女, 中国电信股份有限公司北京研究院新兴信息技术研究所 IP 与未来网络研究中心工程师, 主要研究方向为未来网络架构、新型网络技术等。



雷波 (1980-), 男, 中国电信股份有限公司北京研究院新兴信息技术研究所 IP 与未来网络研究中心主任、高级工程师, CCSA “网络 5.0 技术标准推进委员会”管理与运营组组长, 主要研究方向为未来网络架构、新型 IP 网络技术等。

解冲锋 (1974-), 男, 博士, 中国电信股份有限公司北京研究院新兴信息技术研究所总工程师, 中国电信集团公司科学技术委员会数据组委员, 北京市 IPv6 重点实验室主任、教授级高级工程师, 长期在中国电信进行 IPv6 的技术及部署应用研究, 主要研究方向包括互联网网络架构、IPv6、目标网、NFV/SDN、网络管理运营等, 国家“863”计划、CNGI、国家重大科技专项等多项国家级科研项目负责人。2017 年获得全球 IPv6 论坛颁发的“IPv6 世界领袖奖”。

李云鹤 (1981-), 男, 中国电信股份有限公司北京研究院新兴信息技术研究所 IP 与未来网络研究中心工程师, 主要研究方向为新型 IP 网络技术及设备等。