



专题：数据网络协议架构创新——NewIP

内生安全网络架构

江伟玉, 刘冰洋, 王闯
(华为技术有限公司, 北京 100095)

摘要: IP 网络通过连接全球大量的网络设备给人类带来了便利, 但网络面临持续性的安全和隐私问题令人担忧。由于网络缺乏内生安全的设计, IP 地址伪造、隐私泄露、中间人攻击、分布式拒绝服务 (DDoS) 攻击等顽固安全问题难以根治, 传统的补丁式解决方案补不胜补。在研究 IP 网络面临的各类安全威胁及相关安全技术的基础上, 剖析了 IP 网络固有的安全缺陷, 提出了具有内生安全特性的网络架构, 包括具有内生安全的隐私 ID/Loc、安全验证和审计协议、跨域联合防御机制等, 能够为端到端通信保驾护航。

关键词: IP 网络; 内生安全; 隐私; 可审计性; DDoS

中图分类号: TN915.08

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019215

Network architecture with intrinsic security

JIANG Weiyu, LIU Bingyang, WANG Chuang
Huawei Technologies Co., Ltd., Beijing 100095, China

Abstract: IP network brings big benefits for human's life by connecting most devices all over the world, but its security and privacy issues make people frustrating when using end to end communication. Without intrinsic security design of the network, it is difficult for patch-like solutions to cure stubborn security issues (IP spoofing, privacy leakage, MITM attack, DDoS, etc.). On the basis of surveying different kinds of security threats and related security techniques, an overview of the security weakness analysis was given, and network architecture with intrinsic security (NAIS) was presented, including dynamic ID/IP with intrinsic security, security verification and audit protocols, and cross-domain cooperation defense mechanism, which could provide security and trustworthiness for end to end communication.

Key words: IP network, intrinsic security, privacy, accountability, DDoS

1 引言

基于 IP 协议的网络作为数据世界的管道, 在构建万物互联的世界中扮演重要角色。然而, 频

发的安全事故显示, 当前的网络面临巨大的信誉挑战, 用户很难相信 IP 网络能够为端到端通信提供安全和隐私保护。IP 地址伪造是攻击者隐藏身份、发动攻击的惯用手段, 然而应用网络数据分

收稿日期: 2019-08-10; 修回日期: 2019-09-10

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)

析中心 (Center for Applied Internet Data Analysis, CAIDA) 数据显示, 23.5% 的 IPv4 和 25.4% 的 IPv6 自治域系统依然允许携带虚假 IP 的数据分组流出^[1]。暴露在头部的 IP 地址使用户面临较大的隐私泄露风险, 已成为各网站识别用户身份、关联用户行为的重要指纹, WebRTC 的数据显示 80% 以上的主流网站会通过提取用户数据分组中的 IP 地址追踪用户^[2]。另外, 网络层各类 DDoS 攻击依然是网络安全的一大顽疾, 服务中断事件时有发生, 严重破坏了网络服务的可用性。

由于 IP 网络设计之初缺乏安全考虑, 外挂的补丁式安全技术难以为网络通信提供保障。在耦合了多种语义的 IP 地址基础上, 现有方案难以平衡地址伪造带来的真实性破坏和 IP 地址追踪带来的隐私泄露问题, 可审计性和隐私保护矛盾重重。虽然密码技术可为通信内容提供机密性和完整性保护, 但是由于 IP 缺乏可信的自验证机制, 作为安全锚的密钥交换过程存在欺骗威胁。DDoS 攻击源也已不再局限于外部网络, 来自内部的攻击流量同样不可小觑。由于缺乏协议面内生的防御机制, 外挂的防御方案无法低成本自适应迅速增长的攻击流量规模, 联合作战也难以在现网部署。在边缘计算、雾计算、5G 等技术兴起的未来, 基于安全域内部设备可信的假设更加难以立脚, 依靠安全域隔离的防御方案已无法应对内部攻击。随着大量异构设备接入, 网络环境将变得更加复杂, 凸显的安全问题将成为网络技术广泛应用的主要障碍。IP 网络固有的安全缺陷使得外挂式安全方案无力对抗各类网络攻击, 亟需内生的安全技术来构建安全可信的未来网络。

本文工作以解决顽固安全问题为出发点, 以安全视角重新设计通信协议和安全机制, 旨在为未来网络提供内生安全特性。本文首先给出了 IP 网络的安全分析总览, 剖析了 IP 网络固有的安全脆弱性。在研究现有技术的基础上, 设计了内生安全网络架构, 通过将身份 ID 与位置 Loc 从 IP

地址中分离, 提出了 4 种核心安全技术。

- 动态可审计的隐私 ID/Loc 技术。面向隐私保护和可审计性平衡难题, 使用动态变化的隐私 ID 支持真实性验证和审计追踪, 使用非对称的最小隐私揭露 IP 地址进行路由寻址。
- 去中心化的 ID 内生密钥技术。构建去中心化信任锚点, 为域级身份及密钥管理提供可信保障, 免除单点权威沦陷危机。基于 ID 内生密钥技术, 规避 ID 与密钥脱绑带来的中间人攻击问题。
- 基于最小化信任模型的真实性验证技术。域内域间多步快速验证, 过滤虚假流出/流入流量。基于最小化信任模型, 防止接触网络流量的内部节点作恶, 可辅助快速定位失效节点。
- 跨域联合审计和多级攻击阻断技术。新增安全审计组件, 通过审计协议实现跨域追溯、源域定位和多级阻断非法流量。在源域过滤失效情况下, 依然可赋予目的域有效的攻击防御能力。

2 安全脆弱性及技术需求

端到端通信安全脆弱性分析如图 1 所示, 用户在使用 IP 协议进行端到端传输数据分组的过程中, 存在源 IP 地址伪造、IP 地址头部隐私泄露、审计逃避、密钥交换欺骗、DDoS 攻击等顽固安全威胁。本节将具体分析现有的安全问题和脆弱性, 提出确保端到端通信真实性、隐私性、可审计性、机密性、完整性和可用性等多种安全特性的技术需求。

(1) 真实性需求分析

伪造源 IP 地址是破坏通信真实性的持久威胁。IP 地址伪造常被攻击者采用, 用于发动会话劫持、中间人攻击和 DDoS 攻击等网络攻击, 也是反射放大型 DDoS 攻击的必要攻击手段。在缺乏有效验证的情况下, 攻击者可以轻易地生成大

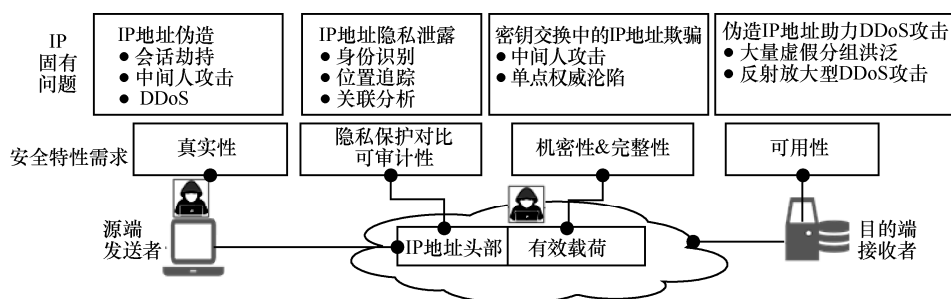


图1 端到端通信安全脆弱性分析

量包含虚假IP地址的攻击流量,欺骗无辜接收者,逃避过滤和审计追踪。

为了对抗IP地址伪造,多种防御技术均被提出,但依然无法消除IP地址伪造威胁。由于IP地址缺乏内生的自验证机制,大量伪造IP地址的流量依然可在网络中畅行。即使部署了流入权/流出权过滤等技术^[3-6],受害主机依然难以识别经过精心构造的虚假IP分组,也无法有效处理IPSec和Tor等加密流量。例如,可在路由器上广泛部署的uRPF技术^[7],难以识别来自同一个源域的伪IP地址流量。实际上,到目前为止,仍有20%以上的AS都没有部署源过滤机制,允许其流出的流量伪造IP地址,AS在没有遭受攻击时部署自滤机制动力不足。因此,仅依靠源域自滤的流出权过滤技术(如(SAVI^[8])难以凑效,大量的虚假数据分组依然可到达受害主机。虽然基于密码学的路径验证技术(Passport^[9])在理论上有效,依赖数据分组传输路径上的多个AS添加密码学标记,缺乏激励多个AS协作的机制,很难直接在现网上快速部署。可见,由于缺乏内生安全的顶层设计,补丁式的安全方案难以根治IP地址伪造带来的真实性问题。

因此,对于持续的IP地址伪造威胁,未来网络需要从顶层设计真实验证机制。一方面,随着网络规模的进一步扩大和网络接入设备的倍增,不仅需要防止外部虚假流量在受害主机侧汇聚,也需要验证来自内部的虚假数据分组。另外,在目的网络边界甚至近源对流出流入数据分组进

行多级验证,可以免受单点验证失效威胁,大大削减基于IP地址伪造的DDoS攻击流的破坏力。另一方面,在真假流量混杂的大量数据分组转发背景下,网络层真实性验证机制应该不仅准确且高效。在确保准确性的前提下,需要考虑采用高效轻量级的密码验证技术以支持高速大吞吐的分组转发能力。

(2) 隐私保护与可审计性需求对比分析

提供以真实性为基础的可审计性是确保网络可信的必要条件,但是可审计性的实现也给隐私保护带来巨大挑战。通过验证标识符是否由合法权威颁发可以保证真实性,但不一定能实现合法权威对非法流量进行快速精准的在线追踪和溯源。在真实性保障的前提下,可审计性需要一个静态且可验证的持久实名身份标识符,来实施非法流量的在线快速追踪溯源。然而,持久实名身份标识符的使用又会给合法用户的隐私带来威胁。近年来,隐私的关注率一直在上升,特别是随着欧盟GDPR(General Data Protection Regulation)和我国网络安全法的发布。用户为了限制非授权的设备、链路窃听者以及访问的网络服务,根据数据分组中携带的持久标识符,识别发送者的身份、跟踪位置和关联发送者的网络行为。因此,未来网络需要平衡隐私保护与可审计性的关键技术。

尽管网络隐私保护与可审计性被研究了多年,但是依然缺乏非常有效的解决方案。例如,Passport^[10]和ISP隐私方案^[11]能够提供源IP地址

的隐私,但是不能隐藏发送者ISP的位置信息。Mailbox^[12]通过提供多个代理位置来为多个IP地址接收数据分组,可以隐藏接收者的真实IP地址,但是并没有提供发送者的隐私保护。洋葱网络^[13]被认为是一种有效的隐私保护技术,但在支持高速分组转发方面存在性能弱势。虽然IETF也有多项针对IPv6地址隐私保护的工作,但是大部分工作(如临时地址^[14]、SLAAC^[15])聚焦在后64位的接口标识符隐私,没有考虑前缀隐私。实际上,5G网络的IPv6 PDU session使用唯一的前缀作为发送者的标识符,并且在共用同一IPv6前缀的用户比较少的情况下,前缀隐私同样需要提供保护。为了提供可审计性,学术界也提出了多种方案,如AIP^[16]、APIP^[17]、APNA^[18]等。然而,AIP仅考虑可审计性,却忽略了隐私保护;APIP仅考虑源IP地址隐私,由于没有对所有分组进行验证,伪造的数据分组依然可以绕过审查。APNA通过引入临时ID及证书,能够很好地平衡隐私保护和可审计性,但是需要频繁的请求、计算、颁发临时PKI证书来抵御长时间的关联分析。

实际上,由于当前IP网络固有的设计缺陷,耦合了身份(身份标识)和位置(定位符)语义的IP地址使外挂式安全方案很难兼顾隐私保护与可审计性。出于路由寻址目的,一方面需要在报文头部暴露精确的定位符,另一方面移动性也使得定位符会动态变化。因此,使用一种必然要暴露、动态变化的定位符以唯一标识用户,显然是不合适的。原因有两点:出于网络提供商对可审计性的考虑,需要一个可被合法实体唯一识别的、静态持久标识符,而定位符不满足静态持久特性;出于用户的隐私考虑,需要一个非授权实体无法识别的、足够匿名、动态不可关联的标识符,暴露在头部的定位符不满足匿名不可关联特性。显然,对于耦合了定位符语义的IP地址而言,难以身兼身份标识符语义,无法满足可审计性和隐私保护需求。因此,需要打破当前IP地址的安全设计缺陷,为未来网络提供一

个动态不可关联、可审计追踪的隐私ID机制。

(3) 机密性与完整性需求分析

人们普遍认为IP数据分组有效负载的机密性和完整性可以采用基于密码技术的安全协议来保证。例如,可以采用TLS/SSL或其他上层安全协议提供机密性和完整性,通过IPSec隧道模式甚至还可以实现IP报头信息的机密性。但是,所有这些协议的安全性都建立在安全的密钥协商基础上。如果密钥协商过程不可信,则数据安全性也就无从谈起。

在端到端通信场景中,动态的密钥交换协议广泛应用在密钥协商过程中,然而动态密钥交换又面临诸多安全威胁。由于静态的密钥配置方法复杂且不灵活,难以适用大量连接下的密钥交换需求。因此,基于Diffie-Hellman的动态密钥交换协议得到了广泛的应用。然而,在缺乏对IP地址与密钥进行绑定和验证的情况下,Diffie-Hellman密钥交换过程容易遭受中间人攻击,中间人可以使用伪造的IP地址欺骗合法实体与其进行密钥交换,从而可以解密、窃听甚至篡改合法实体之间的加密流量。虽然通过PKI证书机制可以将ID与身份公钥进行绑定来防止中间人攻击,但是又会引入单点中心化权威作恶或者单点故障问题。由于IP缺乏内生的密钥生成和验证机制,现有外附的多级中心化PKI机制又存在可信和多级证书链验证带来的大计算开销等问题,难以满足大量多样化异构设备之间的安全通信需求。

因此,未来网络需要解决当前密钥交换中的欺骗问题,保障数据分组有效负载的机密性和完整性。针对单点权威失效问题,去中心化的公钥基础设施已成为构建安全信任锚的必然选择,具体方案需结合场景设计以满足性能和安全的差异化需求。在此基础上,未来网络还需要具备内生的密钥自验证功能,以根治密钥交换过程中的欺骗问题。

(4) 可用性需求分析

DDoS攻击依然是破坏网络可用性的顽疾。在



2018年,DDoS攻击流量已突破1.7Tbit/s量级^[19]。2016年广为人知的Mirai僵尸网络^[20]、通过沦陷大量IoT设备,给网络带来了多起巨大安全风暴。随着越来越多的异构IoT设备的接入,DDoS攻击威胁将会加剧,并且会打破现有基于防火墙的安全防御基线。作为5G的目标,未来5G网络将支持每平方千米百万量级的设备连接,因此,来自同一管理域内部的DoS攻击流量也不容小觑。

由于网络在设计之初缺乏安全考虑,现有主流的DDoS防御思想类似一场基于网络资源的军备竞赛。广泛应用的黑洞技术,虽然将攻击流量引入了黑洞,同样也致使了合法流量不能被处理。并且,大部分外附的DDoS防御技术通常实现在昂贵的专用硬件设备上(如部署在企业内部的DDoS防火墙设备^[21]或部署在云中的DDoS流量清洗设备^[22]),依赖于对深层数据分组的解析,滞后有时延,无法在网络层精准快速过滤。虽然,基于BGP Spec Flow的方案使得受害主机能够通过协议消息请求其他的AS协助DDoS流量过滤,但缺乏有效的激励机制来促动或约束非受害AS主动部署和协助DDoS防御。此外,现有大多数易于部署的DDoS防御方案无法独立于攻击流量规模,也难以做到有效的近源阻断,当大量的DDoS流量汇聚到受害主机侧时,正常的服务已受到影响。虽然SIBRA^[23]提供的DDoS防御能力可以独立于攻击流量规模,但是其预留带宽的机制依赖于复杂的分级层次化的AS关系设计,难以被广泛接受。总而言之,如果没有大量的计算或带宽等资源优势,现有的补丁式防御方法仍然难以对抗压倒性的DDoS攻击流量。

因此,在未来的网络架构及协议设计中,需要内嵌多层次的DDoS防御技术,在可能的攻击流量路径上,尽可能早地发现攻击流量、在靠近攻击源侧进行阻断,同时使目的端具备区分合法和非法流量的能力,使得网络节点或实体具备

DDoS攻击免疫特性,从而确保网络服务或节点的可用性。

3 系统方案设计

本文针对网络面临的顽固安全问题,通过重新设计IP网络协议及安全机制,提出了一种具有内生安全特性的网络架构(network architecture with intrinsic security, NAIS)。NAIS基于最小信任模型,不完全信任管理域(如自治域系统)内部和外部的实体。所有来自内外部的流量真实性都将被验证。仅根据功能需要向少部分网络节点揭露IP地址分组头部的隐私信息,对于内部不可信的网络节点同样采取了保护措施避免隐私泄露。NAIS充分利用了:

- 身份标识符和位置标识符分离技术,将身份标识符ID与位置标识符Loc从当前IP地址中解耦,以兼顾真实性、可审计性和隐私性;
- 临时身份标识,短期有效的主机标识符和身份凭证,用于对抗标识符伪造攻击和身份隐私泄露;
- 动态的位置标识符,频繁变化、部分信息加密的Loc以防止识别、关联分析和位置追踪。

为了确保端到端通信安全,NAIS提供了5类安全功能组件:身份管理者(identity manager, IDM)、审计代理(accountability, AA)、本地DHCP服务器、ID验证者和边界路由器。身份管理者负责管理AS域内的身份以及签发动态临时的匿名身份标识符(ephemeral and encrypted identifier, EID)及其凭证给终端主机。审计代理负责对非法流量进行追踪审计。ID验证者是一种具备真实性验证功能的路由器,负责验证发送者的真实性,过滤虚假或恶意的数据分组。本地DHCP服务器管理和分发动态变化的位置标识符(ELoc)给终端主机。内生安全网络架构如图2所示,数据分

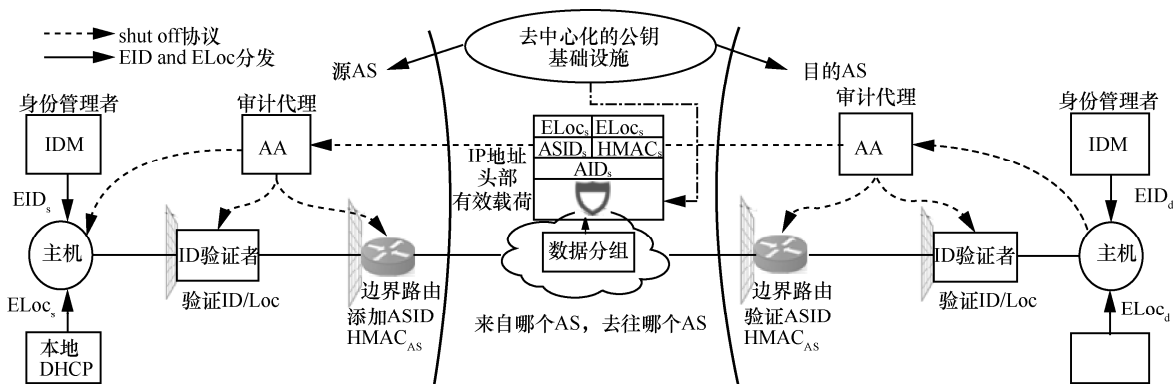


图2 内生安全网络架构

组在源端主机生成、经网络传输、到达目的主机的过程中，发送者数据分组中的标识符信息，会被ID验证者检查以确保流量的真实性和合法性，源AS边界路由器在转发数据分组到互联网时同样会校验源的真实性和添加一个 $HMAC_{AS}$ 作为可验证的域标记，数据分组在到达目的AS边界路由器时，AS边界路由器通过验证 $HMAC_{AS}$ 可以过滤掉虚假来源的数据分组。

为了确保端到端通信安全，NAIS通过设计和修改具备安全特性的网络协议，新增和部署具备安全功能的网元，提出了4种核心技术，具体如下。

(1) 动态可审计的隐私ID/Loc

具有迷惑攻击者的动态ID和Loc可用于防止隐私泄露和关联追踪。源AS域外部的网络节点仅能揭露数据分组来源于哪个AS，而无法获知发送者具体所在的子网和位置信息以及发送者的长久标识符。路由器仅能从IP地址头部获得最小必要信息进行数据分组转发。当攻击发生时，受害主机可以追溯非法流量到其所属的源域，只有源AS域的AA才能打开发送者的真实身份，根据其安全策略，发送控制命令进行流量过滤。NAIS通过对永久ID和真实Loc进行加密，生成的EID和ELoc不仅具有匿名性，并且通过动态变化标识符可以防止关联分析和追踪。

(2) 去中心化的ID内生密钥

在本安全架构中，采用了去中心化的公钥基

础设施来确保信任锚的安全域可信，AS域级别的身份ID及密钥管理基于去中心化的基础设施，可以防止单点权威失效或作恶带来的安全问题。终端主机的密钥管理可被隔离在一个管理域内，即域密钥的沦陷仅会影响域内终端主机的可信性。而实际上，当前PKI权威在分发和撤销证书时，缺乏具体且清晰的边界，某个权威CA的沦陷带来的安全问题具有蔓延扩散特性。在NAIS中，用于协商会话密钥的身份公钥内生于主机标识符，即接收端可以根据主机ID直接派生出信息验证公钥，赋予了ID自验证公钥的特性，从而能够防止密钥交换过程中的欺骗。

(3) 基于最小信任模型的真实验证

去除安全域划分机制中对域内流量的信任弊端，域间和域内流量都将被验证。对于需要跨域传输的网络流量，当数据分组从源端发送后，源AS域>ID验证者和边界路由器均都会对其流出流量进行验证。NAIS不假设ID验证者完全可信，根据不同场景，通过部署不同的匿名验证方法，如零知识证明技术、盲签名技术等，可以在ID验证者处实现匿名验证功能，兼顾真实性和隐私保护。当域间流量到达目的AS时，目的端的边界路由器根据域间共享的密钥，对流入流量进行验证。因此，跨域传输流量的真实性可以通过流出和流入权多步验证得到保障。对于来自AS域内部的网络流量，接收者侧的ID验证者同样需要验



证其来源真实性，从而使得当 AS 域内部发生故障和攻击时，网络管理面能够快速定位错误进行恢复。

(4) 跨域联合审计和多级攻击阻断

本方案赋予了目的域区分合法流量和非法流量的能力，设计的审计协议可以实现跨域的追踪溯源和攻击切断。目的 AS 域的边界路由器基于源域边界路由添加的 $HMAC_{AS}$ ，对每个流入的数据分组进行验证，识别和阻断所有携带虚假域 ASID 的 DDoS 攻击流量。同时，根据不同目的端需求，可在 IP 地址头部携带可被目的端验证的 AID，从而使目的端网络具备区分合法用户流量与攻击者流量的能力。当一个具体的攻击流被识别后，受害主机通过发送一个 shut off 审计协议消息给其所在域的 AA，再到达目的域的 AA，进行非法流量的溯源和阻断。源 AS 域的 AA 验证该审计请求、提取出原始数据分组中的隐私标识，打开发送者的真实身份和位置，最后发送过滤非法流量的控制命令给源主机或验证者或边界路由。在源主机沦陷的情况下，审计者可以根据安全策略和指控同一主机的 shut off 请求数量，请求验证者过滤掉虚假流量。即使在验证者沦陷的情况下，边界路由器也具备过滤非法流量的能力。对于源 AS 不诚实执行攻击阻断的情况，目的端依然可以通过限流等措施减轻 DDoS 攻击的危害。

4 应用探讨和案例分析

随着 5G 网络和边缘计算^[24]的发展，为了提高响应效率和充分利用资源，大量的连接请求处

理和计算操作将下沉到靠用户侧的网络节点。本文提出的内生安全架构基于最小化信任模型，在隐私保护、真实性、DDoS 防御等方面，不完全信任管理域内外部的所有节点，可应用在边缘计算、5G 网络等存在不完全可信内部节点的场景。

边缘计算应用探讨如图 3 所示，在主机接入和使用网络的过程中，某些计算操作将从运营商的核心机房走出到位于开放物理环境的不可信设备。例如公共可用的 Wi-Fi 设备、基站以及其他下沉的路由设备等。由于暴露在开放式环境中、安全防护措施难以部署等原因，此类设备容易遭受攻击、泄露隐私或被攻击者控制。一方面，出于路由目的，此类不完全可信设备依然需要接触身份标识符或位置标识符等敏感信息；另一方面，针对未来小空间大规模的网络连接需求，存在将某些验证终端主机的计算下放到此类设备的需求，以减小集中化处理带来的大计算开销和 DDoS 攻击风险。如何确保这些设备在保护隐私的情况下，依然能够诚实地执行验证计算是一个挑战。因此，采用本文提出的动态可审计隐私 ID/Loc 技术，可面向不完全可信计算节点，实现基于隐私 ID 的匿名鉴别技术，不仅可以防止内部节点和外部 Internet 节点泄露隐私，减轻集中式处理大量连接请求带来的 DDoS 攻击风险，同时能确保真实性和可审计性。

5G 网络应用案例如图 4 所示。5G 网络在支持合法监听和追踪溯源等可审计性时，也非常重视隐私。在 5G 控制面的主鉴别流程中，为了防止永久标识符 SUPI 在空口泄露，采用了非对称密码

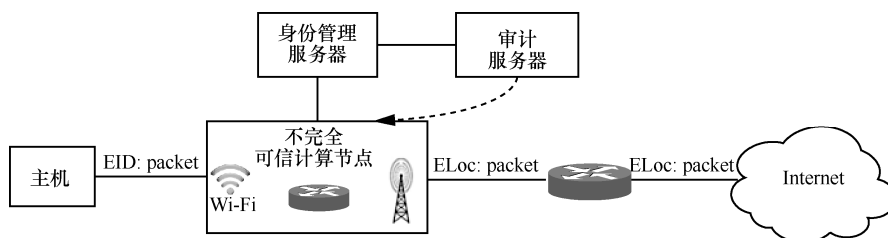


图 3 边缘计算应用探讨

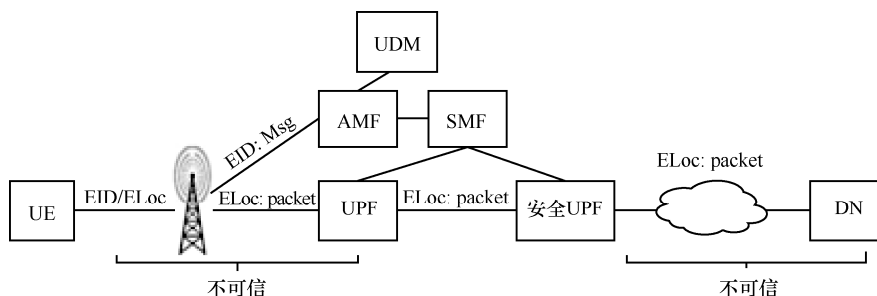


图4 5G网络应用案例

技术加密 SUPI, 但也给集中式的身份数据管理服务 UDM (unified data manager) 带来了 DDoS 攻击威胁。本文的隐私 ID 技术可实现在 UDM 中, 而匿名验证技术可实现在分布式的 AMF 中。通过 UDM 分发控制面的隐私 ID, 不仅可以防止空口窃听者、不可信基站甚至漫游场景中不同安全域的 AMF 获得永久标识符, 也能支持必要的审计追踪。通过将身份验证计算下发给 AMF 或者基站, 可以在确保接入用户真实合法的情况下, 规避针对 UDM 的 DDoS 攻击。另外, 隐私 Loc 技术也可以应用在 5G 数据面。由于 5G 的 IPv6 类型流量使用唯一的 IPv6 前缀识别用户身份和位置, 采用本文的动态 ELoc 替代数据面静态的位置标识, 可以大大地减小隐私泄露风险。

5 结束语

本文通过分析当前网络面临的顽固、持续性安全威胁, 对网络固有的安全缺陷进行了剖析, 提出了新型的具有内生安全特性的网络架构。该安全架构面向未来网络, 基于最小化信任模型, 提出了 4 种核心技术, 能够为端到端通信提供内生的安全与可信能力。通过将身份和位置从 IP 地址中解耦, 在协议层面, 提出的动态可审计的隐私 ID/Loc 技术, 以安全视角设计新的 IP 地址头部, 不仅能够确保网络流量的真实性, 也能很好地兼顾隐私保护与可审计性。内生安全网络架构依赖于去中心化公钥基础设施、验证者、审计代理等新增功能组件的实现和部署, 不仅能够打造

坚实可信的通信协议信任锚, 也能防止通信过程中的欺骗和隐私泄露问题。同时, 跨域审计协议和多级攻击阻断技术也进一步加固了网络的安全性。最后, 本文探讨了边缘计算应用场景和 5G 应用案例, 阐述了本文技术的安全优势。

参考文献:

- [1] Caida spoofer program report[R]. 2019.
- [2] ENGLEHARDT S, NARAYANAN A. Online tracking: a 1-million-site measurement and analysis[C]//the 2016 ACM SIGSAC Conference on Computer and Communications Security, Oct 12-16, 2015, Denver, Colorado, USA. New York: ACM Press, 2016: 1388-1401.
- [3] FERGUSON P, SENIE D. Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing: RFC 2827[S]. 2000.
- [4] DUAN Z, YUAN X, CHANDRASHEKAR J. Constructing interdomain packet filters to control IP spoofing based on BGP updates[C]//INFOCOM, April 23-29, 2006, Barcelona, Spain. Piscataway: IEEE Press, 2006.
- [5] BREMLER-BARR A, LEVY H. Spoofing prevention method[C]//IEEE INFOCOM, 2005(1):536-547.
- [6] JIN C, WANG H, SHIN K. Hop-count filtering: an effective defense against spoofed DDoS traffic[C]//the 10th ACM Conference on Computer and Communications Security, Oct 27 - 30, Washington D.C., USA. New York: IEEE Press, 2003.
- [7] BAKER F, SAVOLA P. Ingress filtering for multihomed networks: RFC 3704[S]. 2004.
- [8] BI J, LIU B. Problem statement of SAVI beyond the first hop, Internet Draft[R]. 2012.
- [9] LIU X, YANG X, WETHERALL D, et al. Efficient and secure source authentication with packet passports[C]//2nd conference on Steps to Reducing Unwanted Traffic on the Internet, San Jose, CA, USA. New York: ACM Press, 2006.
- [10] LIU X, YANG X, WETHERALL D, et al. Passport: secure and adoptable source authentication[C]//5th USENIX NSDI, April



- 16-18, 2008, San Francisco, California, USA. New York: ACM Press, 2008.
- [11] RAGHAVAN B, KOHNO T, SNOEREN A C, et al. Enlisting ISP to improve online privacy: IP address mixing by default[C]//PETS '09, August 5-7, 2009, Seattle, WA, USA. New York: ACM Press, 2009.
- [12] CHAUM D. Untraceable electronic mail, return address, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2):84-88.
- [13] DINGLEDINE R, MATHEWSON N, SYVERSON P F. Tor: the second-generation onion router[J]. Journal of the Franklin Institute, 2004, 239(2):135-139.
- [14] NARTEN T, DRAVES R, KRISHNAN S. Report from the IAB workshop on routing and addressing: RFC4941[S]. 2007.
- [15] GONT F. Method for generating semantically opaque interface identifiers with ipv6 stateless address autoconfiguration (slaac), RFC 7217, Internet engineering task force, request for comments[S]. 2014.
- [16] ANDERSEN D G, BALAKRISHNAN H, FEAMSTER N, et al. Accountable internet protocol[C]//ACM SIGCOMM 2008 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, August 17-22, 2008, Seattle, WA, USA. New York: ACM Press, 2008.
- [17] NAYLOR D, MUKERJEE M K, STEENKISTE P. Balancing accountability and privacy in the network.[J]. ACM Sigcomm Computer Communication Review, 2014, 44(4).
- [18] LEE T, PAPPAS C, BARRERA D, et al. Source accountability with domain-brokered privacy[C]// the 12th International on Conference on emerging Networking Experiments and Technologies, December 12 - 15. 2016, Irvine, California, USA. New York: ACM Press, 2016.
- [19] US service provider survives the biggest recorded DDoS in history[Z]. 2018.
- [20] ANTONAKAKIS M, APRIL Y, BAILEY M, et al. Understanding the mirai botnet[C]//26th USENIX Security. [S.l.:s.n.], 2017.
- [21] CloudFlare. Advanced DDoS attack protection[Z]. 2018.
- [22] FAYAZ S K, TOBIOKA Y, SEKAR V, et al. Bohatei: flexible and elastic DDoS defense[C]// Usenix Conference on Security Symposium, August 12 - 14, 2015, Washington, D.C., USA. New York: ACM Press, 2015.
- [23] BASESCU C, REISCHUK R M, SZALACHOWSKI P, et al. SIBRA: Scalable internet bandwidth reservation architecture[J]. arXiv preprint arXiv:1510.02696, 2015.
- [24] 李子姝, 谢人超, 孙礼, 等. 移动边缘计算综述[J]. 电信科学, 2018, 34(1):87-101.
- LI Z S, XIE R C, SUN L, et al. A survey of mobile edge computing[J]. Telecommunications Science, 2018, 34(1): 87-101.

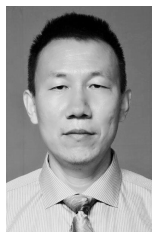
[作者简介]



江伟玉 (1987-), 女, 博士, 华为技术有限公司 2012 实验室中央研究院网络技术实验室高级工程师, 主要研究方向为网络安全架构及协议、可信身份管理、数据安全等。



刘冰洋 (1985-), 男, 博士, 华为技术有限公司 2012 实验室中央研究院网络技术实验室主任工程师, 主要研究方向包括网络架构、网络安全及可行、路由和命名解析、确定性网络等。



王闯 (1975-), 男, 华为技术有限公司 2012 实验室中央研究院网络技术实验室技术专家, 主要研究方向为未来网络架构与技术探索。