安全可信的互联网体系结构与端到端传送关键技术

Secure and Trusted Internet Architecture and Key Technologies of End-to-End Transmission

徐恪/XU Ke，冯学伟 /FENG Xuewei，
李琦/LI Qi，朱敏/ZHU Min

（清华大学，中国 北京 100084）
(Tsinghua University, Beijing 100084, China)

DOI：10.12142/ZTETJ.202206004
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221128.1433.002.html
网络出版日期：2022-11-28
收稿日期：2022-10-16

摘要：围绕无连接网络中安全可信的端到端传送关键问题，从互联网的工作原理出发，提出了具备安全可信和主动防御能力的互联网端到端传送关键技术，包括层间交互、语义一致的协议栈安全漏洞检测与防御，随机标识、层次验证的分组转发正确性检测，以及频域分析、交互图构造的传送连接可信检测，实现了分组数据可靠生成、安全传输、可信应用3个阶段全生命周期的安全闭环，有效增强了互联网的整体安全性。在实际网络环境中进行规模化应用及部署的结果表明，所提出的技术方法能够有效抵御拒绝服务（DoS）、流量劫持、身份欺骗、路由篡改等针对互联网的各种攻击威胁。

关键词：互联网体系结构；端到端传送；语义一致性；路径验证；恶意流量检测

Abstract: The key issues of secure and trusted end-to-end transmissions in connectionless are addressed. Aiming to ensure the consistency between network policies and the end-to-end transmission behavior, a new technique based on the working principles of the Internet is presented, i.e., identifying and mitigating vulnerabilities in protocol stacks by leveraging cross-layer interactions and semantic consistency analysis, detecting the correctness of packets forwarding path by leveraging random labels and hierarchical verification, as well as identifying the reliability of transmission connections by leveraging frequency domain analysis and interaction graph construction. Our technique can ensure the reliable generation, safe transmission and trusted application of IP packets in the three-stage life cycle, thus enhancing the security of the Internet. Through large-scale applications and deployments in the real world, experimental results show that our technique can effectively mitigate the threats of denial of service (DoS), traffic hijacking, identity spoofing, and route tampering.

Keywords: Internet architecture; end-to-end transmission; semantic consistency; path verification; malicious traffic detection

互联网已经成为国民经济赖以发展的重要信息基础设施。与此同时，互联网安全也是国家能源、交通、国防、教育等关键领域安全的重要保证。近些年，美国Colonial Pipeline输油管道网络勒索停服、委内瑞拉电网异常断电、乌克兰电信运营商Ukrtelecom服务中断、Log4j远程代码执行等大量网络安全事件表明，当前的互联网存在严重的安全缺陷和风险，可被攻击者所利用，从而对基础设施服务造成破坏，严重影响人们的日常生活[1]。

总的来说，网络应用的破坏和服务安全性的攻击主要来自3个方面：首先，在分组生成过程中，利用协议栈漏洞实施攻击破坏[2-6]；其次，在分组传输过程中，利用网络路由协议与转发机制设计的缺陷实施攻击破坏[7-10]；最后，在分组应用过程中，利用传送连接不可信开展大规模隐蔽攻击[11-12]。产生上述3个方面攻击威胁的根本原因在于：互联网体系结构在设计之初假设了通信双方和通信过程是真实可信的，无连接的网络状态也没有设计保障端到端传送安全可信的相关技术。这导致恶意攻击者有机会针对网络空间中的特定目标发起地址欺骗、流量劫持、分布式拒绝服务等多种类型的网络攻击，最终严重破坏网络中关键基础设施、服务等的安全性[13]。

本文围绕无连接网络中安全可信的端到端传送这一关键问题，从互联网的功能和原理出发，深入分析了分组数据生命周期中不同阶段面临的攻击威胁，然后从网络规范策略与端到端传送行为一致性保证出发，提出了基于语义一致性的

基金项目：国家自然科学基金（61825204、61932016、62132011）；北京卓越青年科学家计划项目（BJJWZYJH01201910003011）

协议栈漏洞发现与修复机制、随机协作的分组恶意转发检测机制、基于频域特征和图结构的传送连接可信机制，实现了分组数据的可靠生成、安全传输、可信应用3个不同阶段的安全闭环，增强了网络向用户提供正常、有序、可信的端到端传送服务能力，有效提高了互联网的整体安全性。

1 互联网端到端传送基本原理和关键安全问题

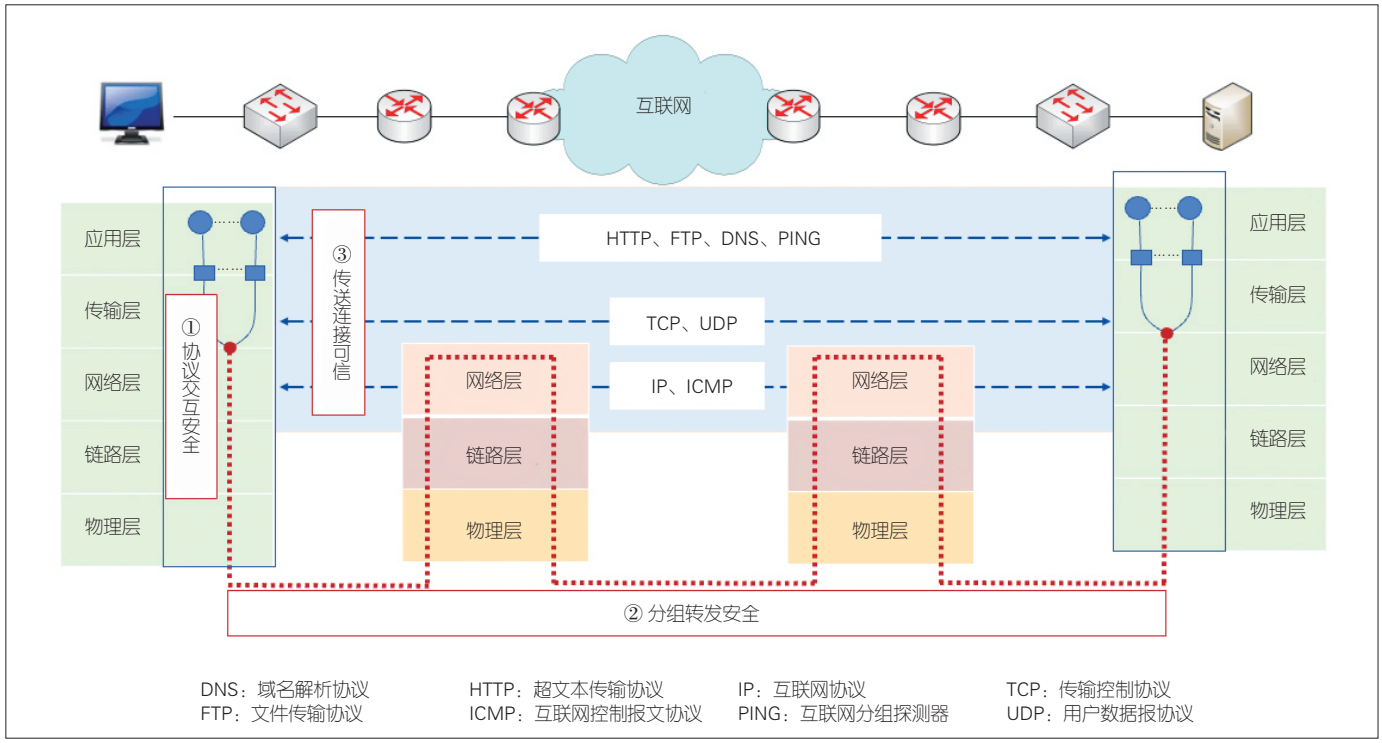
网络协议、系统及应用服务在设计和实现过程中不可避免地存在缺陷。为了增强网络的安全性，本文从互联网的工作原理出发，依据分组数据的不同生命周期，将分组数据在端到端传送过程中面临的安全威胁，归纳为以下3个方面，具体如图1所示。

（1）在分组数据生成过程中，协议栈交互安全问题引起的攻击威胁。终端协议栈承担分组数据的可靠生成和安全接收任务。协议栈安全直接关系到分组数据源的安全。我们发现经典的传输控制协议（TCP）/互联网协议（IP）的协议栈模型存在着一种隐蔽的共性缺陷模式。协议栈在跨层交互过程中会产生安全问题，这在当前被严重忽略。诸如二义性、信息泄露、语义缺失、身份欺骗等安全漏洞可被攻击者远程触发利用，对分组数据的可靠生成造成严重威胁和破坏[2-6]。

（2）在分组数据传输过程中，路由转发安全问题引起的攻击威胁。路由劫持、数据拦截和篡改、流量窃听等攻击行为会给分组数据的安全传输带来极大威胁。因此，如何保证分组数据能够按照预期的路由配置进行正常转发，使路由节点和目的节点能够验证数据包的来源并过滤恶意流量，是保证分组数据安全转发的关键[7-10]。

（3）在分组数据应用过程中，传送连接不可信问题引起的攻击威胁。随着互联网用户规模和应用复杂性的不断上升，以及新型攻击技术的不断出现，保证海量异构分组数据中没有隐蔽恶意分组的混淆嵌入，实现高精度、低延迟的恶意分组识别和检测，是实现传送连接不可信条件下分组数据可信应用的关键[11-12]。

为了提高整个网络空间的协同防御能力，有效解决分组数据生命周期中3个阶段的安全问题，本文提出了无连接网络中安全可信的端到端传送体系结构，具体包括：面向分组数据可靠生成的协议栈安全，提出基于语义一致性的终端协议栈漏洞发现与修复机制，整体上揭示并解决协议层间交互的深层安全问题，增强了协议栈的鲁棒性和安全性；面向分组数据安全传输的路由转发安全，提出通过安全边界网关协议（BGP）和真实路径验证为互联网提供数据转发真实可信保障能力，从控制平面和数据平面杜绝流量被恶意劫持、重定向或恶意丢弃；面向分组数据可信应用的传送连接安全，提出基于频域特征和图结构的恶意分组流量检测识别技术，对抗加密低速等逃逸手段，实现泛化性，适应多场景，为分



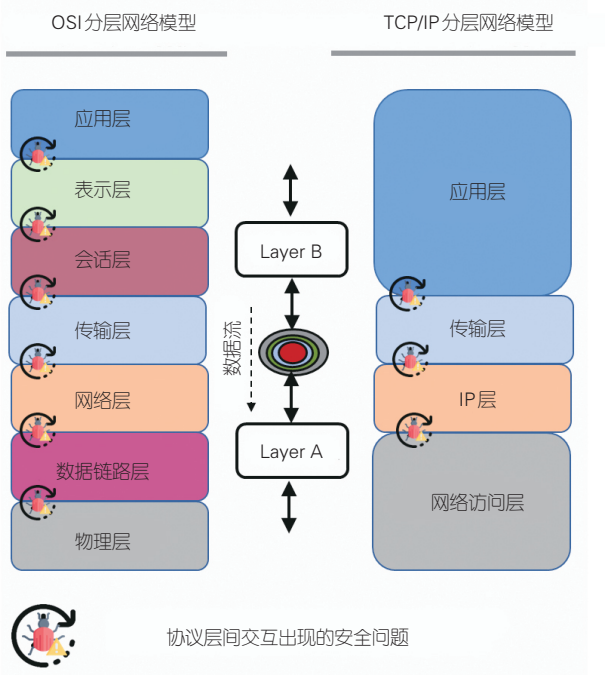
▲图1 互联网端到端传输基本原理和关键安全问题

组数据的可信应用提供保证。

通过上述3个有机协作的组成部分，本文提出的无连接网络中安全可信的端到端传送体系结构，整体上增强了互联网的安全性和鲁棒性，使分组数据具备了全生命周期的安全可信和主动防御能力，从而有效对抗多样化的攻击威胁。

2 面向分组数据可靠生成的协议栈安全

协议栈是网络空间数据生成的基础。在生成和解析分组数据过程中，不同层次间的协议需要动态跨层交互和协同。如图2所示，在这一过程中，虽然单层协议足够安全鲁棒，但将它们组合在一起进行跨层交互，则可能会出现严重的安全问题，例如协议跨层交互二义性问题、信息泄露问题、语义缺失问题、身份欺骗问题等。这些问题一旦被攻击者触发利用，将会对数据分组的可靠生成（即数据源）造成严重的破坏和威胁。当前，协议跨层交互安全问题并未引起足够的重视。本文通过对网络协议跨层交互的共享变量及资源进行特征分析，发现并形式化定义了协议在交互过程中存在的5种典型安全问题。在此基础之上，我们还提出了链式验证的防御机制，有效解决了协议层间交互安全问题，并通过热修复机制为异构平台提供统一的漏洞自动修复方法，实现了漏洞发现、防御和修复的安全闭环。



IP：互联网协议　OSI：开放系统互联　TCP：传输控制协议

▲图2 分层网络模型跨层交互安全问题

2.1 TCP/IP分层网络模型的交互式安全性分析方法

我们发现了TCP/IP协议栈模型中存在的5种典型跨层交互式安全问题，并提出了形式化的方法以便对这5种安全问题进行归纳概括，抽象出各类安全问题的共性范式。在TCP/IP网络协议栈中，我们假设层A和层B在交换数据（以层B向层A write数据为例），将这一过程简化为两个实体间的数据传递模型。这里我们揭示了5种跨层交互式漏洞范式：

（1）同步问题引起的二义性。B.write ! = A.read，即在层B对内核中某字段进行状态更新后，层A并没有完整读取到该更新。这将导致层A读取的字段值不完整或者不正确，致使层间由于状态不同步而出现安全漏洞[5]。

（2）封装不完备引起的信息泄露。A.field = f (B.key) and observable (A.field) == Ture，即层B中的关键字段key属于隐私受保护信息，不可被攻击者探测到。但层A中某个可观测字段值field的计算方法依赖于层B中的关键字段key，它可以直接由层B中的关键字段key计算获得，也可以根据层B中的关键字段key进行判断，然后筛选相应的计算方法。封装不完备将导致攻击者通过A的字段值field推理出B的关键字段key，进而导致信息泄露[2-3]。

（3）语义缺失引起的误操作。A.write = f(B.payload) && trace (B.payload) ==False，即层A将根据层B的载荷来执行写操作。但是由于层A无法对层B的载荷进行溯源，即无法验证其是否伪造或者包含错误，因此会默认层B的载荷正确合法。这导致层A会潜在地执行错误操作，形成恶意攻击[4]。

（4）输入源缺乏验证引起的身份欺骗。A.read==X.write and X!=B，即层A所读取到的字段来自X，而非来自其所期待的B。由于协议栈中层A的协议缺乏对其输入来源进行验证的安全措施，层A可能接收到伪造信息进而引发身份欺骗漏洞[6]。

（5）语义过载引起的误操作。A.read == B.write and A.$write_1$ = f_1(A.read) and A.$write_2$ = f_2(A.read)，即层A能够正常读取层B所写内容，同时层A的某个写操作$write_1$紧密依赖于从层B读取到的内容。但是，在进行其他不同的写操作$write_2$时，该操作也会依赖从层B所读取到的内容。这将可能导致层B所写的内容语义过载，进而导致内核发生误操作漏洞[2-3]。

描述每类安全问题的共性特征和漏洞规则，然后借鉴经典的程序分析方法，如污点分析、模型检验、符号执行等，能够自动化地挖掘协议栈跨层交互式安全漏洞，提高协议栈安全漏洞的分析效率和协议栈的鲁棒性。

2.2 基于轻量级链式验证的协议栈安全性增强

为了增强协议栈的安全性，我们提出了一种基于轻量级链式验证的传输层安全性增强方法。基于哈希验证的方式，该方法使TCP连接双方能够对传输层报文形成彼此可验证的共识，避免攻击者或中间人窃取和伪造类似敏感信息，从而消除网络协议栈面临的典型安全威胁。我们重新设计了传输层报文的校验和机制，采用链式哈希计算的方式，生成报文中可验证的checksum字段。每一个传输层报文校验和的计算，是根据当前报文数据和上一个报文的校验和计算获得的。这有助于形成一个完整的校验链，从而能够对抗攻击者的伪造和破坏。这种新型的传输层报文验证方式，使传统报文的校验和字段信息不再孤立，具备了链式完整性传递和验证的功能，可以有效抵御攻击者针对报文的破解、伪造等威胁，实现了协议栈安全能力的增强。

2.3 基于语义的异构平台协议栈漏洞热修复

为了有效应对不同系统和平台的异构性，提高协议栈防御方法的自动化部署能力和防御效果，我们提出并实现了一种通用的漏洞热修复机制RapidPatch[14]。该机制支持在不修改原始代码的情况下，通过实时注入扩展的伯克利数据包过滤器（eBPF）字节码实现通用的Patch。该Patch可以适配所有不同软件、硬件异构系统上相同的漏洞，在不重启系统的情况下进行动态加载并实现热修复。同时，自动验证和软件错误隔离机制可有效减少人工测试工作量，确保通过验证的Patch能在各个平台上安全地运行。

3 面向分组数据安全传输的路由转发安全

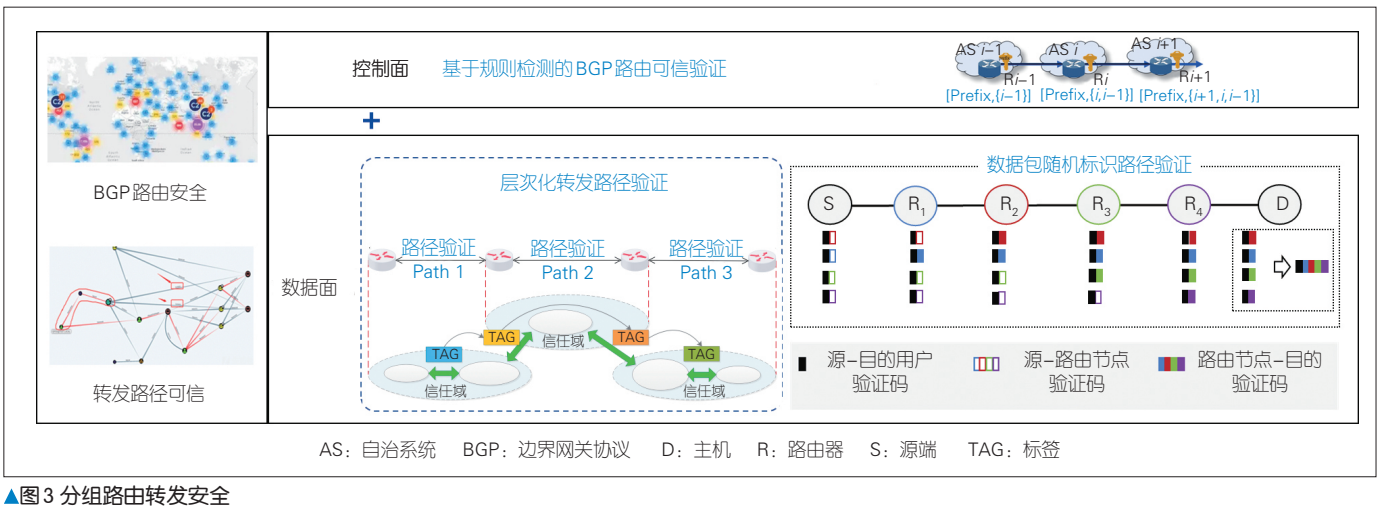
协议栈安全保证了数据分组的可靠生成，确保了数据源的真实可信。但在分组传输过程中，攻击者可能会在中间链路上进行数据拦截与篡改、流量窃听、分组恶意转发和错误路由等。如图3所示，为应对分组传输过程中的恶意攻击行为，我们从网络层控制面、数据面两个层次设计安全检测机制，实现了分组的路由转发安全[15-16]。基于规则检查的BGP路由信息验证机制能够保障控制面真实有效。同时，针对数据面域间高吞吐、高扩展性要求，我们设计了层次化的可扩展路径验证方法，实现了规模化路径验证的技术基础，保证了分组传输路径的真实可信。使用随机标识方法可进一步降低路径验证开销。为此，我们提出了更高效的基于随机标识的路径验证机制，实现了灵活可扩展、安全收益明确且可支持域间大吞吐的高效验证能力。

3.1 基于规则检测的BGP路由信息验证

BGP易产生错误配置或者受到路由攻击。由于误配置或者路由攻击，任何自治系统（AS）都可以通告自己是每一个前缀源的所有者，即实施前缀劫持攻击，或者通告一个不存在的AS路径，即伪造路径攻击。因而，目的网络会被劫持并产生路由黑洞。对此，我们提出了基于规则检测的BGP（TBGP）路由验证方案，通过在路由器上检测路由是否符合BGP路由通告的规范来验证路由，并实现了一种自动路由过滤机制。在TBGP中，如果一个BGP路由器在出口过滤器中成功验证路由通告（即符合路由验证规则），则路由器签名这个路由。邻居路由器通过在入口过滤器验证路由签名的有效性，可以确定这个路由通告是否符合BGP的路由通告规范。通过这个机制，TBGP路由器可以在每个路径中建立一个可传递的信任关系[17]。

3.2 层次化的可扩展转发路径验证机制设计

为了简化控制平面的设计，降低分组转发路径验证的复



▲图3 分组路由转发安全

杂度，实现可扩展的分段转发路径验证，我们通过在AS之间建立信任联盟，实现了层次化的可扩展分组转发路径验证机制。AS按照位置可以划分为3种角色，即主域、边界域以及非主非边界域。这里的主域是指子信任联盟的代表节点，用于同其他子信任联盟的主域建立联系。这样信任联盟之间最后形成的是树状关系，不在同一分支下的AS之间不会有直接建联的关系。边界域是位于子信任联盟边界的域。数据包从该域发出，即发往其他子信任联盟或者发出信任联盟。非主非边界域是指既不是主域也不是边界域的域。上述信任域的构建能够实现层次化的分段转发路径验证，有助于将端到端的完整路径验证拆分成分段的信任传递，达到基于层次化和分段机制的可扩展路径验证能力[7]。

3.3 基于数据包随机标识的高效真实性路径验证

在层次化的路径验证机制基础之上，我们提出了数据包标识的随机添加及验证机制，进一步实现低开销、高效率的域间转发路径验证能力[8-9]。从流的角度出发，我们提出基于数据包随机标识的高效真实性路径验证机制。该机制使源、目的节点能够有效验证数据包经过的自治域路由节点是否和预期一致。基于层次化信任，高效真实性路径验证共享各自治域路由节点之间的动态标签；使用动态标签为每个数据包生成验证码，并将其作为源、目的节点与路由节点验证数据包的标识；结合随机标识技术降低路由节点开销和网络通信开销，从而实现基于数据包随机标识的高效真实性路径验证。

4 面向分组数据可信应用的传送连接安全

在协议实现与分组转发安全可信的基础上，攻击者也可能会利用安全可信的基础设施进行攻击，发送恶意的数据包到合法流量中，危害互联网端到端通信安全，破坏应用服务的可用性。因此，传送连接不可信条件下的分组数据的可信应用是另一个关键安全需求。然而，分组数据流中恶意分组的检测与剔除目前仍存在很大的挑战。主要原因在于传统的恶意流量检测方案通常仅针对少数已知的攻击和低速网络设计，而且无法应对流量动态变化的特征，即没有考虑攻击者的逃逸行为。如图4所示，我们提出了基于频域特征的恶意流量实时检测方案和基于图结构的高效隐蔽恶意行为检测方案，两组检测方案可以分别识别短期与长期恶意数据行为。

4.1 基于频域特征的恶意流量实时检测

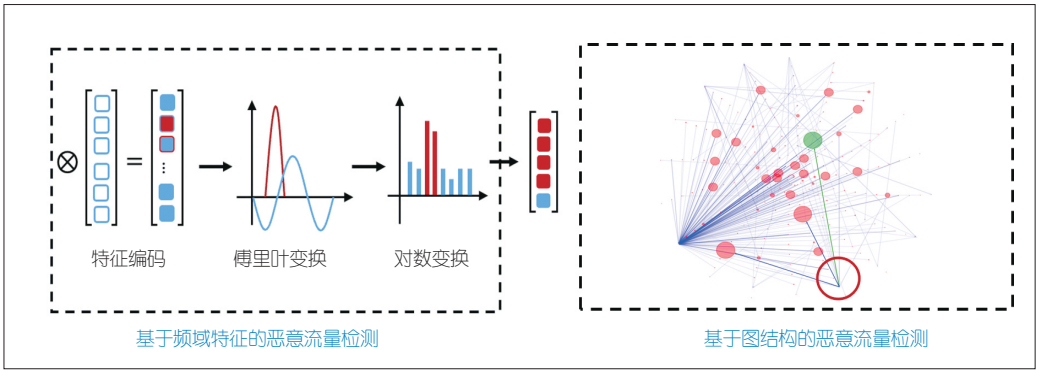
基于频域的检测方案针对短时恶意行为，解决了传统恶意流量检测系统中检测速度和鲁棒性不可兼得的难题，最终实现了在高带宽环境下对抗逃逸行为的实时鲁棒性检测。

基于频域特征的恶意流量实时检测主要包含两个模块：频域特征抽取和轻量级的机器学习。频域特征抽取模块首先对观测到的高速流量进行解析，以获取原始的细粒度逐包特征，对逐包特征进行压缩编码；随后对于编码后的特征进行频域特征抽取，并将频域变换作为特征增强方法来进一步降低特征冗余性，提升特征有效性；最后利用对数变换，防止检测过程中机器学习算法的数值出现不稳定。该方法采用轻量级无监督机器学习算法，来学习流量的频域特征向量，在检测阶段将聚类损失率大的流量标注为异常流量。通过真实世界实验证实，采用频域分析的方法能精准检测拒绝服务（DoS）、侧信道等42种典型恶意流量，并保证单核1.65 Gbit/s的吞吐量和毫秒级延迟[11]。

4.2 基于图结构的高效隐蔽恶意行为检测

基于图结构的检测方案针对长期恶意行为，解决了传统检测方案不能应对低速加密且隐蔽的恶意流量问题，最终实现了多场景通用的低速隐蔽恶意流量检测。流量交互图可有效表示网络用户的长期交互信息，能够挖掘异常的交互模式，检测出隐蔽的加密恶意流量。

在构建出流量交互图之后，我们使用四步轻量级图学习方法，利用图结构上维护的丰富历史交互信息来检测加密的恶意流量。（1）通过提取强连通分量来分析图的连通性，并通过对粗粒度统计特征进行聚类来识别图上异常的强联通分量。其中，排除正常的联通分量可显著降低图学习算法的开



▲图4 传送连接不可信条件下的恶意流量检测

销。（2）由于边特征具备局部邻接性，使用图学习算法对边进行预先聚类，可以显著降低特征处理开销，保证检测的效率。（3）使用Z3 SMT（指一种求解器）求解顶点覆盖问题，以提取关键顶点，然后逐一分析关键节点就可以分析全部的边。（4）对连接到相同的关键节点的边特征进行聚类，从正常交互模式相关的边当中区分异常的交互模式相关的边，即识别表示加密恶意流量的边。在80个场景下，该方法能高精度地检测各类异常流量，包括传统暴力洪范攻击流量、低速率探测流量、加密的洪范流量、代表性恶意软件流量。相比于传统方案，基于图结构的检测方案可以实现17.5%～31.2%的检测准确度提升[12]。

5 结束语

针对无连接网络中安全可信的端到端传送这一关键问题，我们基于互联网的工作原理，从分组数据的可靠生成、安全传输和可信应用3个阶段出发，提出了基于语义一致性的协议栈漏洞发现与修复机制、随机协作的分组恶意转发检测机制、基于频域特征和图结构的传送连接可信机制，改善了互联网现有协议实现不安全、分组转发不安全和传送连接不可信的现状，整体增强了互联网提供正常、有序服务的能力。同时，本文所提出的技术方法已在奇安信、新华三等实现产业化和规模化应用。

参考文献

[1] LIGHTFOOT L. The top 10 biggest cyber attacks of 2021 [EB/OL]. (2022-06-24) [2022-08-25]. https://expertinsights. com/insights/10-high-profile-attacks-2021/

[2] FENG X W, FU C P, LI Q, et al. Off-path TCP exploits of the mixed IPID assignment [C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2020: 1323-1335

[3] FENG X W, LI Q, SUN K, et al. Off-path TCP hijacking attacks via the side channel of downgraded IPID [J]. IEEE/ACM transactions on networking, 2022, 30(1): 409-422. DOI: 10.1109/TNET.2021.3115517

[4] FENG X W, LI Q, SUN K, et al. Off-path network traffic manipulation via revitalized ICMP redirect attacks [C]//Proceedings of the 31st USENIX Security Symposium (USENIX Security 22). USENIX, 2022: 2619-2636

[5] FENG X W, LI Q, SUN K, et al. PMTUD is not panacea: revisiting IP fragmentation attacks against TCP [C]//Proceedings 2022 Network and Distributed System Security Symposium. IEEE, 2022: 1-18. DOI: 10.14722/ndss.2022.24381

[6] FENG X W, LI Q, SUN K, et al. Man-in-the-middle attacks without rogue AP: when WPAs meet ICMP redirects [C]//Proceedings of the 2023 IEEE Symposium on Security and Privacy. IEEE, 2023: 1-16

[7] FU S T, XU K, LI Q, et al. MASK: practical source and path verification based on multi-AS-key [C]//Proceedings of 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS). IEEE, 2021: 1-10. DOI: 10.1109/IWQOS52092.2021.9521345

[8] WU B, XU K, LI Q, et al. Enabling efficient source and path verification via probabilistic packet marking [C]//Proceedings of 2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS). IEEE, 2019: 1-10. DOI: 10.1109/IWQoS.2018.8624169

[9] WU B, XU K, LI Q, et al. Robust and lightweight fault localization [C]//Proceedings of 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC). IEEE, 2018: 1-8. DOI: 10.1109/PCCC.2017.8280428

[10] FU S T, LI Q, WANG X L, et al. D3: lightweight secure fault localization in edge cloud [C]//Proceedings of 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS). IEEE, 2022: 515-525. DOI: 10.1109/ICDCS54860.2022.00056

[11] FU C P, LI Q, SHEN M, et al. Realtime robust malicious traffic detection via frequency domain analysis [C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2021: 3431-3446. DOI: 10.1145/3460120.3484585

[12] FU C P, LI Q, XU K. Detecting unknown encrypted malicious traffic in real time via flow interaction graph analysis [C]//Proceedings of the 2023 Network and Distributed System Security (NDSS) Symposium. 2023: 1-18

[13] 徐恪, 李琦, 沈蒙, 等. 网络空间安全原理与实践 [M]. 北京: 清华大学出版社, 2022

[14] HE Y, ZOU Z H, SUN K, et al. RapidPatch: firmware hotpatching for real-time embedded devices [C]//Proceedings of the 31th USENIX Security Symposium (USENIX Security 22). USENIX, 2022

[15] 徐恪, 付松涛, 李琦, 等. 互联网内生安全体系结构研究进展 [J]. 计算机学报, 2021, 44(11): 2149-2172. DOI: 10.11897/SP.J.1016.2021.02149

[16] 徐恪, 凌思通, 李琦, 等. 基于区块链的网络安全体系结构与关键技术研究进展 [J]. 计算机学报, 2021, 44(1): 55-83. DOI: 10.11897/SP.J.1016.2021.00055

[17] LI Q, XU M W, WU J P, et al. Enhancing the trust of Internet routing with lightweight route attestation [J]. IEEE transactions on information forensics and security, 2012, 7(2): 691-703. DOI: 10.1109/tifs.2011.2177822

作 者 简 介

徐恪，清华大学教授；主要研究领域为计算机网络体系结构、网络安全和区块链系统；主持和承担重点研发项目5项，近5年发表论文100余篇，出版专著10余部，获授权中国及国际发明专利70余项。

冯学伟，清华大学在读博士生；主要研究领域为网络安全及程序分析技术。

李琦，清华大学副教授；主要研究领域为互联网与云计算安全。

朱敏，清华大学高级工程师；主要研究领域为互联网体系结构及安全。