防御数据窃听攻击的路由交换范式体系

徐 恪[1),4)] 赵玉东[1)] 陈文龙[2)] 沈 蒙[3)] 徐 磊[1)]

[1)](清华大学计算机科学与技术系 北京 100084)

[2)](首都师范大学信息工程学院计算机科学与技术系 北京 100048)

[3)](北京理工大学计算机学院 北京 100081)

[4)](清华大学信息科学与技术国家实验室(筹) 北京 100084)

摘 要 近年来,利用路由交换设备漏洞窃听用户流量的攻击事件不断曝光,凸显了核心网络信息安全传输的重要性.由于用户和网络运营商不掌握设备漏洞控制权,导致此类攻击具有成本低、隐蔽、单向和顽固等特点,不易被识别和约束.文中通过分析嵌入漏洞的路由交换设备可能执行的异常服务行为,提出了一种静态路由交换范式体系.该体系对利用设备漏洞窃听用户流量攻击的安全完备性可论证,范式规则通用于TCP/IP网络,并基于该体系设计范式检测设备模型,该模型可设计实现,利用该设备可检测路由交换设备违反范式的输出分组.系统仿真实验结果显示,文中设计的范式设备可放行全部正常分组,同时可识别和约束99.92%以上的窃听分组,被检测路由交换设备吞吐率可达Gbps级.

关键词 流量窃听攻击;路由交换范式体系;设备漏洞;核心网络;范式检测设备

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2017.01649

Paradigm-Based Routing & Switching System for Data Interception Attacks

XU Ke[1),4)] ZHAO Yu-Dong[1)] CHEN Wen-Long[2)] SHEN Meng[3)] XU Lei[1)]

[1)](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

[2)](*Department of Computer Science and Technology, College of Information Engineering, Capital Normal University, Beijing* 100048)

[3)](*College of Computer, Beijing Institute of Technology, Beijing* 100081)

[4)](*National Laboratory of Information Science and Technology (Preparing), Tsinghua University, Beijing* 100084)

Abstract In recent years, the network attacks that adversaries take advantage of router/switch vulnerabilities to perform data interception continue to be exposed, which highlights the importance of secure communication within core networks. As the most affected victims, users and Internet Service Providers have little control on router vulnerabilities, which results in such attacks always being performed in low cost, unidirectional, concealed mechanisms, and being difficult to be recognized let alone restrained. Researchers have proposed many solutions, and most of them are able to prevent or mitigate data interception attacks, however, it is our humble opinion that these solutions are either only fit for specific core networks and specific types of DIAs, or are difficult to implement. To the best of our knowledge, there are still no security complete, universal and easily implementable mechanisms for defending data interception attacks. Based on analyzing all possible abnormal behaviors that vulnerability routers and switches perform, this paper designs and implements a static routing and switching paradigm, a paradigm-based detection algorithm

收稿日期:2015-09-21;在线出版日期:2016-05-17.本课题得到国家"八六三"高技术研究发展计划项目"地址驱动网络关键技术和验证"基金(2015AA015601)资助.**徐 恪**,男,1974年生,博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为计算机网络体系结构、网络安全.E-mail:xuke@mail.tsinghua.edu.cn.**赵玉东**(通信作者),男,1973年生,博士研究生,中国计算机学会(CCF)会员,主要研究方向为网络安全.E-mail:zhaoyd10@mails.tsinghua.edu.cn.**陈文龙**,男,1976年生,博士,副教授,主要研究方向为互联网体系结构、路由及交换技术.**沈 蒙**,男,1988年生,博士,讲师,主要研究方向为互联网流量管理、网络虚拟化.**徐 磊**,男,1982年生,博士研究生,主要研究方向为网络安全.

and detector model to recognize the paradigm-violation output-packets. It proves that the routing and switching paradigm is security complete to data interception attacks. Also all rules of the paradigm are universal applicable to TCP/IP networks, the detector is designable, and the paradigm violations are detectable. The detection algorithm is optimized to gain high performance. Based on simulations, we show that not only 100% of normal packets can pass through the optimized paradigm-based detector, but also about 99.92% of intercepting ones would be caught. In addition, the throughout put of the detected routers/switches can reach Gbps level.

Keywords data interception attacks; paradigm-based routing and switching system; vulnerabilities; core network; paradigm-violations detector

1 引 言

多年来,利用路由设备漏洞在核心网络窃听用户数据的攻击行为一直严重威胁网络用户信息安全,而用户和网络运营商以往低估了此类攻击的危害.2013 年 6 月,前美国中央情报局技术分析师爱德华·斯诺登(Edward Snowden)公开的一些涉密文档显示,美政府自 2007 年起利用国家安全局启动的"棱镜(PRISM)"项目监控和挖掘民众信息,其监控方式除直接进入微软、谷歌等互联网公司的中心服务器获取流量外,还收集流入和流经美国的数据流量①.另外,该项目通过直接攻击互联网大型路由设备,即可获取数十万计算机流量."棱镜门"计划的曝光凸显出提高信息在核心网络传输安全的重要意义.

从棱镜门曝光的文档看,网络设备及组件存在的安全漏洞引发的异常路由转发行为是核心网络信息泄露的内在原因,利用漏洞实施的流量窃听攻击不仅成本低、危害大,还具有顽固、隐蔽、单向等特点.顽固体现在不但设备使用者难以识别漏洞,受研发人员认知水平和编码水平限制,设备供应商自身也难以根除漏洞.隐蔽指漏洞攻击行为与正常路由交换行为有较强的相似性,网络运营商难以对二者进行区分.攻击者单方面掌握设备漏洞,导致网络攻防双方漏洞利用严重失衡.上述特点使得利用漏洞窃听用户信息的网络攻击行为难以被用户及运营商感知和阻止,当前尚未发现理论完备而又可实现的解决方案.

针对路由交换设备漏洞引发的网络窃听攻击,我们在文献[1]提出路由交换范式的概念,力图设计路由交换范式体系,并利用范式设备识别和约束路由交换设备的异常服务行为,防止窃听分组的输出.文献[1]还对范式的验证方式和实现难点进行了分析.该思想可以从根本上解决设备漏洞的安全威胁,但在其实现过程中需要研究理论完备的路由交换范式体系,以及设计可实现的路由交换设备范式检测模型.

总体上,范式及范式检测设备的设计模式可分为动态和静态两种,二者均试图通过识别和约束窃听分组防御数据窃听攻击,其区别在于动态模式下范式设备的检测对象是路由交换设备对分组的操作行为,而静态模式下范式设备的检测对象是路由交换设备输入输出分组的特征.动态模式的主要实现手段包括功能模拟、动作编码匹配,通过即时识别和约束路由交换设备的违规操作,防止违反范式分组的输出,其检测效率高,逻辑上更适应于网络窃听攻击方式的变化,但路由交换设备对分组的操作行为复杂,而窃听攻击行为同样复杂隐蔽,难以设计通用范式对复杂环境下的正常与攻击操作行为进行精确区分.静态模式的主要实现手段包括代码分析、行为结果检测等,试图通过检测路由交换设备输出分组的合法性防御数据窃听攻击,由于该模式的实现以路由交换设备完成分组输出为前提,其检测效率相对较低,但当前互联网以 TCP/IP 协议为基本协议框架,因此以网络层输出结果为检测目标,有利于设计通用于核心网络,对路由协议、网络规模、拓扑结构、管理配置等因素透明的路由交换范式.

作为该领域的一种尝试性探索,本文基于路由交换设备服务行为结果检测设计静态路由交换范式体系及可实现的范式检测设备模型,范式检测设备作为独立设备,可额外专门部署于路由交换设备,使

① PRISM/US-984XN Overview. http://www.aclu.org/files/natsec/NSA/20130816/PRISM%20Overview%20Powerpoint%20Slides.pdf

后者服务行为结果符合范式约束，也可后续部署，用以检测当前在用的路由交换设备是否输出窃听分组. 范式及范式检测设备模型设计与实现主要需解决以下 3 个问题：一是范式的安全完备性，即范式由一系列分组输出规则构成，在核心网络所有路由交换设备均受范式规则约束下，正常分组可全部通过范式检测，窃听分组全部被识别和约束，且范式各规则对识别和过滤窃听分组都是必要的，缺一不可；二是通用性，即这些规范通用于 TCP/IP 网络，对网络拓扑、路由协议、管理配置方案等因素透明；三是可实现性，即在当前技术条件下，范式检测设备可设计，其时间开销足够低，使得路由交换设备性能可基本满足当前网络需求.

为解决上述问题，本文选择分组的〈源 IP，目的 IP，载荷〉为特征三元组，通过检测分组输入输出设备前后特征三元组的变化识别和过滤异常输出分组. 防御数据窃听攻击的关键在于防止分组流向非目标 IP 地址主机，将源 IP、目的 IP 和载荷作为总体特征考察分组流向，有利于制定完备的分组输出规则，以精确识别可能造成数据泄露的窃听分组. 与行为操作检测不同，行为结果检测不关注设备对分组的具体路由交换过程，也无需关注分组网络层以外的数据特征，只考察分组输入设备前后的特征变化，即范式检测设备判断和约束窃听分组的行为是在分组输出路由交换设备之后发生的，因此本文所提的静态路由交换范式可通用于所有 TCP/IP 网络. 将载荷纳入特征码，可通过约束各路由交换设备行为，实现防止载荷流向非目标用户主机的目的，但也严重影响了输入输出分组匹配效率，本文对原始范式优化，以特征码的部分摘要值作为匹配特征，通过查表实现匹配，以牺牲较低比例的安全性为代价，较大程度提高了范式检测效率.

本文第 2 节介绍国内外对利用设备漏洞实施的流量窃听攻击开展的相关工作；第 3 节提出通用和可实现的安全路由交换范式；第 4 节论证范式对流量窃听攻击的安全完备性；第 5 节设计和优化范式检测设备模型；第 6 节对范式设备的检测能力和检测效率进行理论计算和仿真评估，并讨论其关键实现技术；最后总结全文并分析尚待深入研究的问题.

2　国内外相关工作

由于路由设备漏洞严重威胁核心网络信息传输安全，研究者自下向上从路由交换操作、操作系统及设备、核心网络 3 个层面提出了相应的安全解决方案.

在路由交换操作层面，Xu 等人在文献[2]中提出一种构建开放、灵活、模块化的可重构路由器的可行途径，可重构路由软件平台支持组件的动态组合、替换和升级，一些生产商已经利用该技术设计商用路由设备. 在提供可编程功能的同时，可重构也为漏洞攻击带来可乘之机. 为此，Dobrescu 等人在文献[3]中设计一种验证工具，通过结合当前分组验证技术与特定的分组操作软件技术，使软件数据平台在验证路由交换行为是否正常的同时保障工作效率. 由于该工具的验证过程依赖给定的约束条件，因此只能检测特殊异常行为，应用范围较小. 在路由交换设备执行协议的过程中，攻击者可通过发送伪造信息，诱骗目标设备执行错误的路由交换行为. Kothari 等人在文献[4]中结合静态协议代码分析与动态攻击模拟，给出此类攻击行为的自动识别方法，该方法的局限性在于无法识别设备收到伪造信息后延后执行的操作. 另外，由于网络管理者不总是掌握第三方开发的功能构件代码，代码分析并非总是可行的.

在操作系统及设备层面，一种提高信息设备服务可信性的思想是从软硬件组件、操作系统等基础工作做起，自下向上地保障计算系统安全，可信计算组织(Trusted Computing Group，TCG)据此提出了可信计算平台①. Challener 等人在文献[5]中介绍利用可信计算为计算机硬件子系统提供完整和开放工业标准的可行性，并展示其保障服务可信的原理及工作流程. 虽然可信计算技术已经经历了较长的发展历程，但至今仍没有公认的可信计算理论模型和有效的软件动态可信性度量的理论和方法，使得可信计算的发展受到限制[6]. Chen 等人在文献[7]中建议当前的操作系统启用虚拟系统，在无需检测操作系统及应用程序可信性的前提下，提供安全登录、入侵防御及检测、计算环境变迁等服务. 虚拟系统的灵活性为用户带来了诸多方便，但 Garfinkel 等人在文献[8]中质疑该思想忽略了当前相对静态的安全体系依赖于主机数量、配置、位置可预测和可控这一事实. 受自然界伪装大师拟态章鱼的启发，邬江兴等人在文献[9]中提出基于多维重构函数化结构与动

① Trusted Computing Group. TCG Specification Architecture Overview [EB/OL]

态多变体机制的拟态计算(Mimic Computing)及拟态安全防御(Mimic Security Defense)体系,并研制出世界上第一台基于认知的可变结构的拟态计算原理验证样机.拟态计算固有的随机性、动态性和不确定性阻断了目前攻击技术所依赖的攻击链完整性,因此基于拟态计算的信息系统具有内在的主动防御能力,可以有效应对网络设备开放与重构带来的安全挑战.拟态安全主要需解决复杂度高、功耗增加和随机系统测试验证困难等3个问题.

在核心网络层面,互联网体系结构评估模型可以对运营商提供网络体系结构设计建议,徐恪等人在文献[10]中介绍了包括可信性评估等与互联网体系结构发展密切相关的5种基本评估模型,并提出一种基于适应能力的互联网体系结构可演进性评估系统,对服务可信网络设计具有一定的理论与现实意义.解决信息传输安全最直接的思路是设计安全可信的核心网络体系.首先是可信计算思想进一步向网络层面推广,从而形成可信网络链接[11]的思想.受制于可信计算本身发展的局限,当前可信网络链接的理论研究滞后,应用范围较小.类似地,Kim等人在文献[12]中提出一种利用密码技术,通过保障通信双方以及所有参与通信路由设备身份的真实性,提高通信链路信息传输安全的机制.实现该机制的计算开销较低,但需要在每一个传输分组头部增加不定长的端/路由设备认证码,认证码长度为(路径长度+3)×128比特,因此路径长度直接影响信息传输的有效吞吐率.Toby等人在文献[13]中认为互联网体系结构不具备地址真实性验证机制,源地址伪造与路由地址前缀欺骗对网络安全造成了极大危害.在介绍IP地址欺骗实现原理与危害、列举3类主要防御机制及相应的典型方案的基础上,对各方案的综合性能进行比较.徐恪等人在文献[14]中从研究体系、实现机制和关键技术等3个维度对地址安全研究思路进行了归纳分析,并给出了一个地址与标识通用实验管理平台的设想,基于该平台可以为不同的地址标识方案提供统一的部署实验环境.为使安全成为嵌入到网络内部的一种服务,并力图从体系结构的设计上保障网络服务的安全持续,林闯等人在文献[15]中给出可信网络的定义,并在总结可信网络研究现状的基础上,提出其实现过程中主要需解决的4个关键问题.尽管可信网络的概念已经被提出多年,在部分领域也有了较为深入的工作进展,但是当前多数工作只是围绕可信网络在理论与技术的某个局部展开,并没有形成完整的体系,可信网络的许多概念还处在摸索阶段,尤其对其基本属性和面临的关键问题上并没有清晰一致的描述.

不同于上述策略,另一种提高信息传输安全的方法是从信息自身出发,利用用户端系统加密IP分组,保障明文信息不被攻击者获取,其典型应用为IPSec①.由于信息以密文形式在核心网络中传输,攻击者难以获取明文,但随着客户端数量增加,服务端为每个客户端提供的链路带宽会严重缩减[16],同时IPSec无法感知流量窃听攻击、定位攻击主机.

综上,我们认为理想的流量窃听攻击解决方案应具备有效、通用、可实现、高效、可感知攻击并可定位攻击主机等特点,上述方案与现实需求相比均存在不足.通过设计安全路由交换范式体系和部署可实现范式设备,可识别和约束漏洞设备的异常服务行为,从而有效解决利用设备漏洞窃听用户流量的网络攻击.

3 流量窃听攻击路由交换范式设计

本节首先分析流量窃听攻击的特征及其带来的挑战,之后在给出范式总体设计思路的基础上提出通用和可实现的路由交换范式.

3.1 动机与挑战

核心网络信息攻防主要包括合法用户、攻击者、网络运营商和网络设备供应商等四类参与者.在数据传输过程中,合法用户期望所发数据能且仅能被目标用户接收,但由于不掌握核心网络管理权,用户只能要求网络运营商保障信息传输安全.为获取稳定的付费用户,运营商通常也尽力维护核心网络信息传输安全,但作为网络数据处理与传输枢纽的网络设备可能存在漏洞,窃听攻击者可以利用漏洞设备非法获取数据.

通常路由交换设备具有固定的基本逻辑结构和分组路由交换操作流程[17],但漏洞可引发路由交换设备的异常行为.总体上,路由交换设备的数据处理异常行为可以归纳为图1所示的3种[1].

对于图1中的异常行为①,路由交换设备数据转发平面所发送的分组既不是来自上游路由交换设

① Security Architecture for the Internet Protocol, IETF RFC 2401

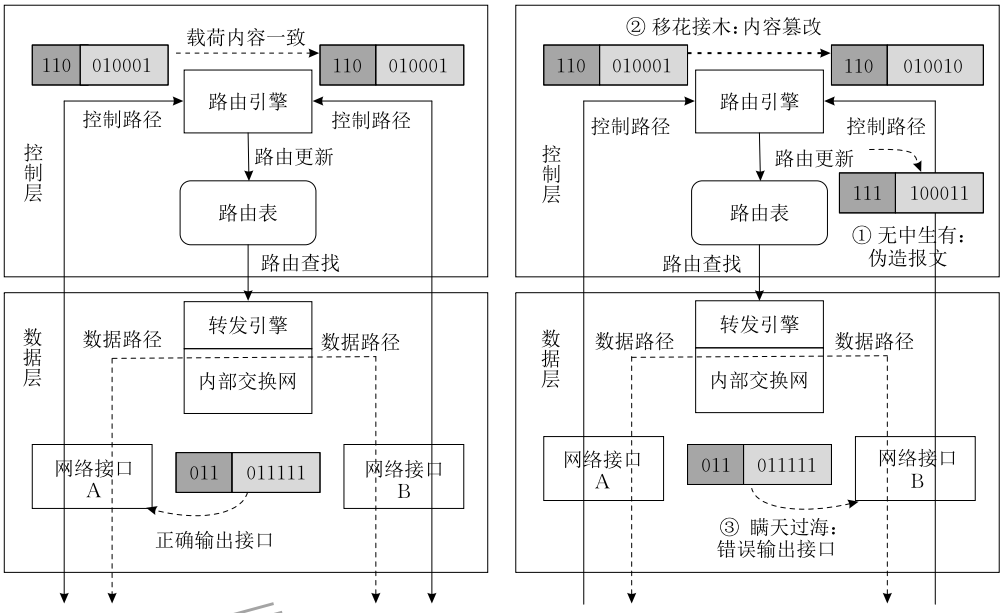

图 1　分组路由转发处理过程(左)与异常行为(右)[1]

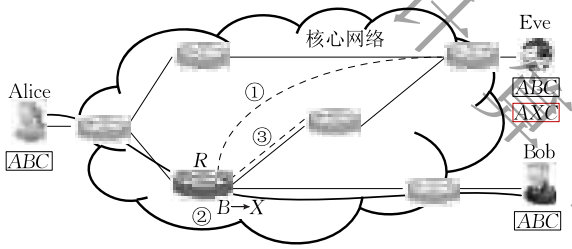

图 2　可引发流量被窃听的 3 种异常输出分组

备，也不是由控制平面产生的，而是由设备自身生成的新分组. 对于异常行为②，路由交换设备对报文的内容进行篡改或替换. 对于异常行为③，路由交换设备看似正常地转发了数据分组，但其以隐蔽方式篡改了分组的输出接口. 一旦利用漏洞控制设备，攻击者可通过上述 3 种异常行为实施图 2 所示的数据窃听攻击.

窃听攻击不干扰用户分组的正常路由与转发，当流经漏洞设备 R 时，原始分组继续沿图 2 中黑色粗线所示的正常路径发送给 Bob，但 R 会备份分组内容，并利用图 1 所示的 3 种异常路由转发操作将备份分组发送给攻击者 Eve. 对以获取用户数据载荷为目标的攻击行为，可引发流量被窃听的异常输出分组无外乎以下 3 种：① 伪造新报文，将备份分组目的 IP 地址篡改为 Eve；② 篡改备份分组载荷，该方式下 Eve 可接收篡改载荷的分组，并根据 R 篡改载荷的算法还原原始载荷，攻击者借助该方式可以规避运营商利用载荷识别窃听分组；③ 错误输出接口，此时备份分组沿着错误链接输出设备，当 R 为链接 Eve 与核心网络的边界设备时，该行为也可能造成用户信息泄露，反之，若 R 为内网路由交换设备，该行为只可能改变分组的传输路径，而不会直接引起分组被非目标 IP 地址主机接收.

约束窃听攻击的关键在于识别漏洞设备的上述 3 种异常行为. 由于当前路由设备不检测输出分组是否有输入分组匹配，运营商无法判断窃听分组是否为新分组，因此异常行为①和②难以被识别. 当前多数核心网络采用动态路由协议，由于设备、链路状态变化直接影响路由表，管理者难以判断设备为分组选择的瞬时输出接口是否符合路由协议，因此难以设计异常行为③的通用识别机制. 综上，由于当前缺乏通用、完备和可行的异常行为检测机制，流量窃听攻击难以被识别和约束.

另一种约束流量窃听攻击的思路是要求供应商提供无漏洞设备，从根本上避免 3 类数据处理异常行为的发生，但该想法在当前难以实现. 在主观态度方面，生产商可能受某些行政部门的委托或国家法律限制，在设备或组件中植入“后门”. 在客观能力方面，受生产商设计和编码等能力限制，设备中的软硬件漏洞难以避免. 在现实需求方面，当前网络对路由交换设备软硬件的开放需求不断提高，可编程设备在给用户提供更加灵活服务的同时，也给网络攻击者带来更多可乘之机. 当前多数国家不掌握芯片、板卡等路由设备核心组件的研发技术，部分使用进口组件的“国产”设备仍可能存在漏洞. 可以预见，设备漏洞的顽固性导致其将长期危害网络安全.

基于上述分析,设计、研发和部署范式体系和范式检测设备,以识别和约束路由交换设备的异常路由转发行为,可有效约束流量窃听攻击,增强核心网络信息传输的安全性,但设备漏洞无法根除、窃听攻击依赖的异常路由转发行为难以检测是实现该方案所面临的主要挑战.

3.2 范式的总体设计思路

范式(Paradigm)的概念最早由托马斯·库恩在《科学革命的结构》[18]中提出,指代可体现某种科学发展在某特定阶段内在结构的模型,它保证了在一个特定的历史时期内某些问题具有特定的解.具体到核心网络信息传输安全,我们的理解是:

(1)路由交换范式由一系列规则构成,是核心网络信息传输安全问题特定的解;

(2)该系列规则因不同历史时期特定的攻击特征、安全需求和技术条件等因素的变化而改变;

(3)范式通用于核心网络,对路由协议、网络规模、拓扑结构、管理配置等因素透明;

(4)范式是可行的,即当前阶段满足所有范式规则的路由设备可设计,违反规则分组可检测,执行和检测规则的开销可容忍.

识别路由交换设备数据处理异常行为的方法总体上可归纳为功能模拟、动作编码匹配等动态方式,以及代码分析、行为结果检测等静态方式.动态方式的工作原理是把路由交换设备对分组的操作区分为合法和非法两类行为,各行为由读取、保留、舍弃、输出等一系列组件组合构成,一次分组操作已经发生的组件组合不属于合法行为,即可判定该行为非法.反之,静态方式的识别方法需要路由交换设备的一次服务行为已经完成后,根据行为结果可能造成的影响判断其是否合法.对比而言,动态方式能够即时判定非法操作,具有迅速快捷的特点,理论上更适应于网络窃听攻击方式的变化,但当前路由交换设备对分组的操作行为复杂,而窃听攻击行为同样复杂隐蔽,因此难以设计通用范式对复杂环境下的正常与攻击操作行为进行精确区分.静态方式采取后验方式检测输出分组,因此反应速度慢,但路由交换设备的服务行为不受检测过程影响,因此易于设计对路由协议、网络规模、拓扑结构、管理配置等因素透明的通用检测系统.

作为该领域的一种尝试性探索,本文基于路由交换设备服务行为结果检测设计静态路由交换范式体系及可实现的范式检测设备模型,范式检测设备作为独立设备,可额外专门部署于路由交换设备,使后者服务行为结果符合范式约束,也可后续部署,用以检测当前在用的路由交换设备是否输出窃听分组.此类范式体系及设备的特点是不关心路由交换设备对分组的具体操作行为,只考察分组在输入设备前后自身的特征变化,通过识别可能造成数据窃听的输出分组,防止其传输到非目标用户.

静态范式体系设计的关键在于分组特征的选择.以〈源 IP,目的 IP,载荷〉作为三元特征组,图 2 中 3 种异常输出分组都没有相同特征的输入分组与之匹配,据此制定分组输出规则(范式),以识别和过滤可引发数据窃听的异常输出分组.由于不关注设备对分组的具体路由交换过程,只通过考察分组输入设备前后的三元特征变化过滤违反范式的分组,该思路的工作流程不受路由协议、网络规模、拓扑结构、管理配置等因素的影响,因此通用于 TCP/IP 网络,也有助于设计对流量窃听攻击安全完备的路由交换范式及构建可设计、可检测和高效的范式检测设备模型.其难点在于范式规则的准确性,既不能漏掉危害数据传输安全的分组,又不能错误过滤正常分组.窃听分组与原始输出分组的三元特征组不同,这使得准确制定安全路由交换范式成为可能.

3.3 路由交换范式

在图 2 所示的通用场景中,Eve 欲窃听 Alice 发送给 Bob 的信息,其手段无外乎利用 R 实施以下 3 种异常行为.①通过伪造目的 IP 地址为 Eve 的新分组,将保留的用户流量发送给 Eve;②按约定编码方式篡改备份分组载荷,将备份分组发送给 Eve,并由 Eve 还原原始分组,该行为同样需要将备份分组 IP 地址篡改为 Eve,因此本质上与①相同;③将保留流量沿错误输出接口发送给 Eve.从行为结果上看,对于①和②,R 伪造的新输出分组没有相同的三元特征码〈源 IP,目的 IP,载荷〉的输入分组与之匹配,此时可通过三元特征码匹配判断该输出分组是否为 R 新生成分组,该行为通常是非法的,其特例是 R 同时将新分组的源 IP 地址篡改为其自身 IP 地址,该行为等同于路由设备 R 以合法身份向端系统 Eve 传送数据.对于③,由于错误选择输出接口只能改变"下一跳"链接,Eve 成功非法窃听分组的前提只能是 R 为 Eve 的边界设备,此时分组的目的 IP 地址与实际接收目标 IP 地址不一致.综上,通过制定由一系列路由交换规则组成的范式,用以识别

设备异常行为结果，可有效防御利用漏洞设备实施的流量窃听攻击. 以下给出面向数据窃听攻击设计的基于输出分组特征检测的路由交换范式：

规则 1(R1). 对封装载荷的分组，当源 IP 地址不是路由设备本身时，以〈源 IP 地址、目的 IP 地址、载荷〉为匹配特征，输出分组有源；

规则 2(R2). 缺省状态下不允许路由设备向客户端主机发送自产分组，若确需发送需经访问权限审核；

规则 3(R3). 边界路由设备向外网直接转发分组时，分组的目的 IP 地址符合输出接口的指向.

4　范式的安全完备性证明

在证明所提范式对流量窃听攻击安全完备性的过程中，为表述方便，引入以下标识：

发送方及主机 IP：Alice；

接收方及主机 IP：Bob；

攻击者及主机 IP：Eve；

网络中的任意路由设备：R_{ARB}；

与 Eve 直接链接的路由设备：R_{NE}；

以上划线表示取反，例如以 $\overline{R_{NE}}$ 表示与 Eve 不直接链接的路由设备；

发送方发往接收方的分组(以 Alice、Bob 为例)：$Pack_{A-B}$；

$Pack_{A-B}$ 的载荷：$Payload_{A-B}$.

信息系统的安全属性包括保密性、完整性和可用性[19]，其中保密性是指网络信息不被泄露给非授权的用户、实体或进程，完整性指接收信息的准确与完全，可用性指合法用户对信息和资源的使用不会被非法拒绝. 由于数据窃听攻击的目标在于获取其他用户数据，而不是阻止目标用户接受数据，因此其安全性指用户信息保密性和完整性.

以下给出范式对利用设备漏洞窃听用户流量攻击的安全完备性证明.

引理 1.　在核心网络所有路由设备均满足本文所提的路由交换范式的前提下，若设备 Equ 收到以〈Sou, Des, $Payload_{Sou-Des}$〉为特征的分组 $Pack_{Sou-Des}$，则

$$\begin{cases} 1.\ Pack_{Sou-Des}\text{的发送端为 } Sou \\ 2.\ Payload_{Sou-Des}\text{为 } Sou \text{ 发送的初始载荷} \end{cases}.$$

证明.　首先证明 1. 设 $Path_{Sou-Equ}=[Sou, R1, \cdots, Ri, \cdots, Rn, Equ]$ 是 $Pack_{Sou-Equ}$ 从 Sou 到 Equ 的任一可达路径中的设备集合. 假设 1 不成立，则图 3 所示的网络中存在设备 $Sou' \neq Sou$，Sou' 可以向 Des 发送 $Pack_{Sou-Des}$，且 $Path_{Sou'-Des}$ 经过 Equ.

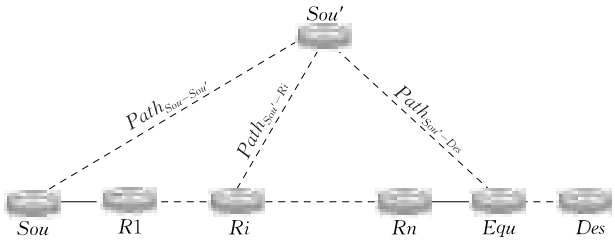

图 3　分组 $Pack_{Sou-Des}$ 的来源

若 Sou' 为端系统设备，发送 $Pack_{Sou-Des}$ 意味着 Sou' 已知 $Payload_{Sou-Des}$，此时 Sou' 可以以自身身份合法发送 $Payload_{Sou-Des}$，而无需以源地址欺骗的形式发送 $Pack_{Sou-Des}$，因此 Sou' 必为路由设备.

若 Sou' 为路由设备，且 Sou' 可发送以〈Sou, Des, $Payload_{Sou-Des}$〉为特征的分组 $Pack_{Sou-Des}$，由于 $Pack_{Sou-Des}$ 的源 IP 地址 $Sou \neq Sou'$，根据 R1，必存在特征为〈Sou, Des, $Payload_{Sou-Des}$〉的 Sou' 输入分组，即 Sou' 不是 $Pack_{Sou-Des}$ 的发送端，这与假设矛盾，因此 Sou 是 $Pack_{Sou-Des}$ 的唯一发送端.

其次证明 2. 对任意 $Path_{Sou-Equ}$，设 $R_0=Sou$；$R_{n+1}=Equ$，对任意 $1\leq i\leq n$，根据规则 R1，R_i 的每一输出分组都存在相同特征三元组的输入分组与之匹配. 若该输入分组来自设备 R_{i-1}，由 i 的任意性知 $Pack_{Sou-Equ}$ 在 $Path_{Sou-Equ}$ 所有设备中都以相同的三元组为特征，即 $Payload_{Sou-Des}$ 为 Sou 发送的初始载荷. 反之，若该输入分组来自非 R_{i-1} 的其他设备，不妨设该设备为图 3 中 Sou'，由于 $Pack_{Sou-Des}$ 先后可到达 Sou' 和 R_i，根据 1 的结论，必存在 Sou 到 Sou' 之间的路径 $Path_{Sou-Sou'}$，以及 Sou' 到 R_i 的路径 $Path_{Sou'-R_i}$，$Pack_{Sou-Des}$ 由 Sou 发送，并沿由 $Path_{Sou-Sou'}$、$Path_{Sou'-R_i}$ 和 $Path_{R_i-Equ}$ 组成的新路径 $Path'_{Sou-Equ}$ 到达 Equ，类似地，新路径 $Path'_{Sou-Equ}$ 中所有设备都以〈Sou, Des, $Payload_{Sou-Des}$〉为特征，即 $Payload_{Sou-Des}$ 为 Sou 发送的初始载荷.　　证毕

命题 1.　如果一个核心网络所有路由设备均满足本文所提的路由交换范式，在网络保障分组可达性的基础上，通信双方收发的信息一致.

证明.　特别地，在引理 1 中，当设备 Equ 为信息的接收方 Des 时，Des 收到的任意分组都由源设备 Sou 发送，且发送载荷与接收载荷一致.

由于网络保障分组可达，Bob 可完整接收每一

个 $Pack_{A-B}$，即通信双方收发的信息一致，本命题成立. 证毕.

命题 1 结论的实质是证明因为受范式约束，当分组传输路径上的任何路由交换设备试图篡改分组载荷时，其输出分组都会被范式检测设备识别和约束.

命题 2. 如果核心网络所有路由设备均满足本文所提的路由交换范式，那么核心网络可保障用户信息仅被目标用户接收.

证明. 使用反证法. 假定在图 4 所示的核心网络中，非目标用户 Eve 可以获取 Alice 发给 Bob 的分组 $Pack_{A-B}$，则必有核心网络中的某路由设备 R_{ARB} 备份了 $Pack_{A-B}$，并将其非法发送给 Eve.

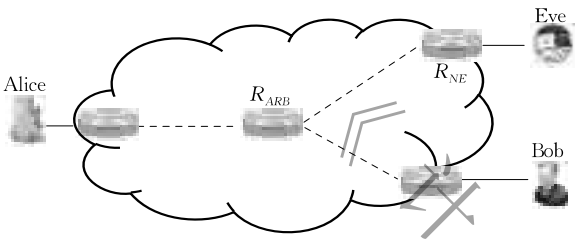

图 4 用户信息被窃听的情况分析

根据图 2 所示路由设备数据处理异常行为，可影响分组接收目标的攻击行为包括①和③两种，二者区别体现在输出分组 IP 地址的变化. ①中 R_{ARB} 将重定向分组的目标 IP 地址篡改为 Eve，其执行者可以是网络中任意设备；对于③，R_{ARB} 可不改变分组的三元特征组，只篡改分组的输出接口，由于接口篡改只能影响分组的“下一跳”接收目标，因此 Eve 以③形式成功获取分组载荷的前提是 R_{ARB} 是 Eve 的接入边界路由设备 R_{NE}.

①中 R_{ARB} 的目标输入分组特征三元组为〈Alice，Bob，$Payload_{\text{Alice}-\text{Bob}}$〉，其输出分组特征三元组为〈*，Eve，$Payload_{\text{Alice}-\text{Bob}}$〉，这里 * 可以被调整为任意有利于窃听攻击的设备. 当输出分组源地址 * 被调整为 R_{ARB} 自身时，R_{ARB} 试图以自身身份向 Eve 传送数据，这违反了 R2. 当 $*=\overline{R_{ARB}}$ 时，受 R1 限制，R_{ARB} 可执行此操作的前提是 R_{ARB} 有以〈$\overline{R_{ARB}}$，Eve，$Payload_{A-B}$〉为特征三元组的输入分组，由引理 1，该输入分组的发送端必为 $\overline{R_{ARB}}$，即 $\overline{R_{ARB}}$ 试图以自身身份向 Eve 传送数据，这同样违反了优化范式中的规范 R2.

当 R_{NE} 试图利用③将保留 $Pack_{A-B}$ 发送给 Eve 时，$Pack_{A-B}$ 的目的 IP 地址为 $\overline{\text{Eve}}$，而 R_{NE} 为 $Pack_{A-B}$ 选择输出接口指向 Eve，这违反了 R3.

综上，受本文所提范式限制，Eve 无法获取 Alice 与 Bob 之间的会话内容，本命题成立. 证毕.

命题 2 结论的实质是证明一旦漏洞路由交换设备试图实施窃听攻击时，窃听分组或者被范式检测设备识别与约束，或者无法输出网络（例如路由交换设备可以篡改分组传输路径，但最终窃听分组载荷无法抵达非目标终端设备）.

范式规则中规范 R2 和 R3 是必要的，否则漏洞设备可通过自生产和恶意篡改输出接口的方式向 Eve 发送分组载荷. 对于 R1，以〈源 IP 地址、目的 IP 地址、载荷〉为匹配特征也是必要的. 漏洞设备以重定向的方式发送分组载荷，必须将重定向分组的目的 IP 篡改为 Eve，此时，若仅以〈目的 IP 地址、载荷〉为匹配特征，攻击者可利用协作者 Carol 向 Eve 发送随机载荷的分组，并利用异常行为③，迫使这些分组流经漏洞设备 R，若其中某分组载荷与 $Payload_{\text{Alice}-\text{Bob}}$ 碰撞，则 R 可以合法向 Eve 发送 $Payload_{\text{Alice}-\text{Bob}}$. 若仅以〈源 IP 地址、目的 IP 地址〉，为匹配特征，Carol 只需向 Eve 发送任意分组，只要该分组流经 R，后者即可以〈Carol、Eve〉为匹配特征，向 Eve 发送 $Payload_{\text{Alice}-\text{Bob}}$. 据此得到以下结论.

命题 3. 本文所提范式中 3 条规范对识别和约束流量窃听攻击都是必要的.

综上，本文所提范式对利用设备漏洞窃听用户流量的攻击具有安全完备性.

需要注意的是，本文专注于核心网络范围内分组传输安全，分组发送端系统实施的地址欺骗攻击不在本文考虑范畴.

本文所提范式体系看似把数据窃取问题简化到了只有单个交换设备上的分组流的源目的地址问题上，其实质是基于范式设计范式检测设备，网络中所有路由交换设备的输出分组都受限于范式约束，导致漏洞路由交换设备生成的窃听分组一经输出即被识别与约束，或者只能在核心网络内部流窜，无法被第三方主机接收. 范式检测设备的作用在于通过检测被检路由交换设备输出分组特征，识别其地址欺骗攻击、漏洞攻击行为，约束窃听分组. 具体对于多台设备配合窃取数据的问题，即主机 A 和 B 正常通信，主机 C 和 D 是试图窃听 A 和 B 之间的交互信息，C 向 D 发送数据成为合法的，可通过范式检查. A 向 B 发送的分组，在路由器 R 上复制一份切换成 C 到 D 的地址后发送给 D，为了满足范式检查，每当 C 发送一个分组给 D 时，就在路由器上窃取一个 A 到 B 的分组，同时销毁一个自己的分组. 这种情

况下，所有的通信都看似正常的，但窃听分组的三元特征码是〈C，D，$Payload_{A-B}$〉，这是一个无源分组，受限于范式规则 R1，该分组一经输出，即被范式检测设备判断为窃听分组，因此无法被 D 接收.

5　范式检测设备模型

理论完备的路由交换范式体系只构成防御数据窃听攻击的理论基础，为解决实际问题，需要设计和部署范式检测设备，为此首先给出路由交换设备服务行为范式检测流程，并基于该流程设计范式检测设备模型. 另外，范式及范式检测设备是面向单播模式设计的，本节的最后分析组播对范式检测的影响.

5.1　路由交换范式检测流程

如图 5 所示，路由交换范式检测流程包括输入分组三元组特征采集和输出分组行为结果范式检测两部分.

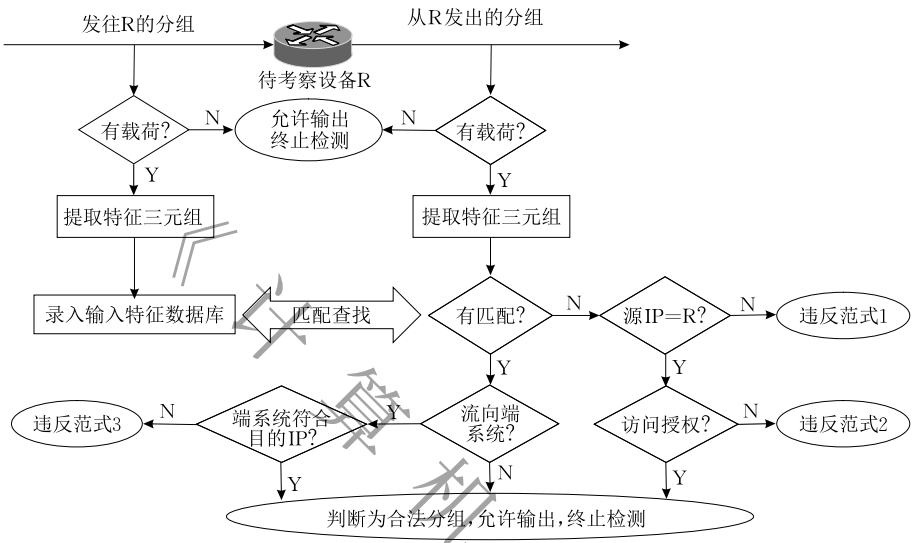

图 5　路由交换范式检测流程

在特征采集过程中，检测系统首先判断流入待考察路由设备 R 的分组是否包含载荷，对包含载荷分组提取〈源 IP 地址、目的 IP 地址、载荷〉三元组信息，并将其录入输入分组特征三元组数据库.

在分组输出行为结果范式检测过程中，检测系统采集输出分组特征三元组，并到输入数据库中查找特征匹配的源输入分组记录. 对有源输出，若 R 为边界设备，且输出接口指向端系统，检测系统根据端系统地址前缀与分组目的 IP 地址的一致性判断设备服务行为是否符合范式. 对无源分组，其唯一可行场景为路由设备向端系统传送数据，检测系统根据端系统是否为设备授权访问目标判断该行为是否符合范式.

注意直接向数据库中记录输入分组的特征三元组，并利用特征三元组查找输入输出匹配可能会带来较大的存储和计算开销，影响范式设备的可实现性，本节剩余部分将设计一种低开销匹配方案.

5.2　范式检测设备模型

图 6 给出了与路由交换设备并行部署的嵌入式范式检测设备模型和可后续部署的路由交换设备服务行为范式检测模型，其中深色长方形区域为嵌入式范式检测设备模型，长方形外区域为可后续部署的路由交换设备服务行为范式检测模型.

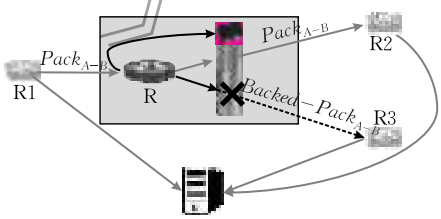

图 6　范式检测设备模型

如图 6 所示，嵌入式范式检测设备主要由信息采集模块和分组输出决策模块组成，范式检测设备不直接参与传统设备的分组路由交换操作，只是由信息采集模块旁路获取输入传统设备的分组内容，并传送给决策模块. 分组输出决策模块由基于路由交换范式检测流程设计的芯片，以及存储输入分组特征三元组数据库的内存构成，它负责提取和存储所有输入分组的特征三元组. 对于输出分组，决策模块提取其特征三元组，并通过在输入分组特征三元组数据库中查找匹配，判断分组输出行为是否符合

范式，同时禁止违反范式的分组输出设备.

从效果上看，正常的输出分组 $Pack_{A-B}$ 行为符合范式，范式检测予以放行；一旦传统设备保留 $Pack_{A-B}$ 的载荷并将其重定向到 Eve，该重定向分组的输出行为违反范式，范式设备禁止其输出. 该范式设备模型在保障合法用户之间数据安全传输的基础上，严格约束了漏洞设备通过备份重定向将用户数据传送给第三方的行为.

将范式检测设备额外并行部署于路由交换设备，可设计实现范式路由交换设备，但设备生产商研发的范式检测设备可能无法严格落实范式规则，需要为网络运营商设计可后续部署路由交换设备服务行为范式检测模型. 该模型一方面可用以检测范式路由交换设备是否合格，另一方面也可后续部署于当前在用的路由交换设备，用以约束后者的服务行为，防御数据窃听攻击并识别漏洞设备. 图 6 中阴影外的部分代表路由交换设备服务行为范式检测系统模型，与范式检测设备中的范式检测系统类似，该模型同样由信息采集模块和分组输出检测模块组成，信息采集模块由目标设备 R 的所有“邻居”设备构成，分组输出检测模块也可由一台具备路由交换范式检测功能的服务器替代，该服务器与 R 的所有邻居设备旁路直连. 在检测过程中，邻居设备向分组输出检测模块旁路发送全部输入输出 R 的分组，检测模块利用范式检测输出分组是否遵循范式. 除范式检测基本功能外，如果发挥服务器存储能力较强的特点，记录违反范式的分组，可以即时感知攻击、核对攻击者拟窃听用户流量的内容，同时定位攻击者接收端主机.

5.3 范式检测设备的可实现性优化

根据总体设计思路，理想的范式体系应具有通用性、安全完备性和可实现性等特点. 范式检测设备不直接干涉路由交换设备对输入分组的操作行为，仅关注输出分组特征，根据分组是否符合范式决定输出分组的合法性，因此其检测过程不受路由协议、网络规模、拓扑结构、管理配置等因素影响. 上一节论证了范式的安全完备性，这里分析范式设备的可实现性. 可实现性具体表现在范式设备可设计，违反范式行为可检测，检测效率可满足当前网络需求这三个方面.

在可设计性方面，由于范式检测系统独立于路由交换设备，网络运营商可以分别向不同生产商定制路由交换设备和范式检测系统. 另外检测模型结构简单，检测流程无需网络互动，有利于高可信检测系统设计. 从检测效果看，范式的 3 条规则在当前技术条件下均可实现，而且正常分组与窃听分组的三元特征组不同，系统可对二者精确区分. 在检测效率方面，相比传统设备，范式设备不可避免地增加了额外的存储、计算和通信开销，表 1 对上述开销进行总体分析.

表 1 范式检测系统开销分析

规范	存储	计算	通信
R1	维护输入分组特征三元组数据库，存储开销不确定	1. 提取输入输出分组特征三元组； 2. 在输入分组特征三元组数据库中查找输出分组匹配； 3. 对无匹配的输出分组，判断分组源 IP 地址和设备 IP 地址的一致性	输入输出分组向范式检测系统传输，通信量等于 2 倍分组长度
R2	维护授权端系统列表，存储量＝授权端系统数量×32 比特	在授权列表中查找目的 IP	—
R3	—	判断向端系统输出的有源分组 IP 地址是否符合端口指向	—

根据表 1 列举的范式检测开销，输出分组的输入匹配查找可能会占用大量资源并严重影响检测效率. 在存储开销方面，由于特征三元组包括分组载荷，因此其长度不固定，而且随着输入分组数量的增加，输入分组特征三元组数据库的总存储量将无限上升. 另外数据库中存储条目的增加还直接导致增加匹配比较的运算量. 为降低模型开销、提高检测效率，需要实现输入输出分组的快速匹配，以下给出一种基于摘要结果查表实现的快速匹配算法.

如图 7 所示，范式检测系统维护一张固定长度的分组输入记录表 table1，初始状态下全表置 0，对每一个输入分组，系统利用固定 Hash 算法计算输入三元特征组摘要 I-digest，选取摘要固定位置和长度（例如第 65 到第 94 位的 30 比特）作为摘要结果 I-digest-result，并将记录表中 I-digest-result 对应位置置 1. 对于输出分组，系统同样计算并提取输出三元组摘要结果 O-digest-result，并在 table1 中查找该 O-digest-result 对应位置的状态，如果该位置状

态为 1，则找到该输出分组的输入源，否则判断该输出分组无源.

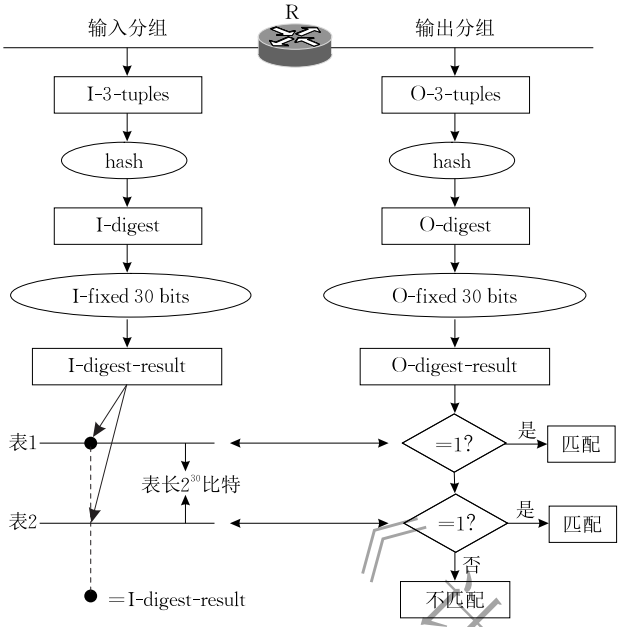

图 7　基于摘要结果查表实现的输入输出分组快速匹配算法

从效果上看，该算法以一张长度固定的分组输入记录表取代原始范式检测流程中的输入特征三元组数据库，解决了检测系统存储量大、存储需求不固定的问题. 另外，输入输出分组匹配过程从直接比对转化为根据摘要结果查表，显著降低了匹配查找的计算量.

具备上述优点的同时，该算法也带来了下述两个新问题，一是随着输入分组数量的增加，本算法中输入分组记录表的规模不断增大，攻击分组因耦合被判定为合法分组的可能性（假阴性）随之增加；二是受当前硬件研发水平限制，本算法无法维护原始特征三元组摘要表，只能以部分摘要表代替原始摘要，这进一步增加了检测结果假阴性的概率，因此需要对算法进行进一步优化. 考虑到运营商通常控制分组在设备中的生存时间，超出上限 τ 的分组将被设备丢弃，为将检测结果假阴性概率控制在一定范围，本算法进一步引入分组输入记录摘要表更新周期 ρ，令 $\rho \geq \tau$，table1 每隔 2ρ 清零并重新启动. 为防止 table1 更新过程中最新合法分组被误判为非法分组，系统维护图 7 中的另一张分组输入记录表 table2，table1 和 table2 分别在时间节点 $2i \times \rho$ 和 $(2i+1) \times \rho (i=0,1,\cdots)$ 清零重启，若输出分组摘要结果在两表相应位置的值均为 0，则判断该分组没有输入匹配.

当摘要结果长度为 30 比特时，范式检测系统的存储开销为 $2 \times 2^{30} = 2$G 比特，在当前技术条件下，检测模块配置 2G 内存是可行的.

5.4　组播对范式检测的影响

为节省网络带宽，减轻服务器负载，当前组播技术被广泛应用于网络音频/视频广播、视频点播、网络视频会议、多媒体远程教育等场景. 与单播模式不同，组播采用一点到多点的通信方式，要求路由器复制并转发多个分组，这种通信方式可能与范式检测产生相互影响. 一方面范式检测设备可能错误“识别”和约束组播分组，使其无法到达目标用户，另一方面攻击者可能利用组播分组封装试图获取的目标分组，达到流量窃听的目的.

由于 ICANN 分配给组播的 IP 地址固定，而且同一组播组的不同成员主机接收的组播分组采用相同的目标 IP 地址，使用相同的 IP 地址接收组播分组，造成路由器收到一个分组后，复制并向不同输出端口发送多个输出分组的情况发生，这些输出分组的特征三元组相同. 在这种场景下，范式检测设备提取各输出分组的特征三元组，并依次检测 3 条范式规则. 由于所有组播输出分组在被监测路由交换设备的匹配输入分组相同，且复制分组与匹配输入分组的特征三元组均为〈组播源 IP 地址，相同的组播目的 IP 地址，载荷〉，因此范式检测设备判断复制分组满足范式规则 R1；组播源 IP 地址与被检测路由交换设备 IP 地址不同，复制分组满足范式规则 R2；当被检测路由交换设备试图向终端设备直接转发分组，在终端设备加入组播组的情况下，复制分组满足范式规则 R3，因此复制分组总是被正常判断，即本文的范式体系规范允许组播分组在路由交换设备中的复制，各合法组播分组均不受范式设备影响到达各目标主机.

对于攻击者利用组播分组封装试图获取的目标分组的情况，漏洞路由交换设备会将其试图获取的载荷封装到组播分组中，此时数据窃听攻击成立的前提是窃听目标主机事先加入组播分组，且封装后分组的特征三元组是〈*，组播目的 IP，目标分组载荷〉，该分组在路由器输入分组中找不到匹配，因此被范式检测设备判断为窃听分组，无法到达窃听目标主机.

6　范式体系评估及关键实现技术

6.1　范式体系的功能评估

本文提出的安全范式体系由 3 条路由交换规则

构成，其功能是识别和约束流量窃听攻击分组，因此理想情况下，正常分组可通过所有 3 条规则，攻击分组则因违反某一规则被识别和约束. 对于规则 R2 和 R3，由于其检测过程与输入匹配查找无关，检测系统总是能够快速、正确判断输出分组是否符合规则，因此其正确率为 100%. 反之，在 R1 的检测过程中，为降低检测系统的部署开销、提高检测效率，我们引入定期更新的 hash 函数摘要表记录分组输入，受检测系统存储能力限制，摘要表中记录的只是输入分组的部分摘要，这可能导致正常分组被判断为违法规则(假阳性)，以及攻击分组被判断为符合规则(假阴性)的情况发生，以下对这两种情况进行理论计算分析和仿真实验评估.

根据 5.3 节设计的算法，检测系统维护两张输入记录摘要表，table1 在第 0 周期起始时间启动，table2 在第 1 周期起始时间启动，两表每隔 2 周期清零并重新记录输入分组. 对任意输入分组，假定其输入时间为 IT，其输出时间为 OT，令 $\rho_i=[\rho\times i,\rho\times(i+1)]$，则必存在 $i(i=0,1,2,\cdots)$，使得 $IT\in\rho_i$. 由 $\rho\geq\tau$ 知 $OT\in(IT,IT+\rho]$，则或 $OT\in\rho_i$，或 $OT\in\rho_{i+1}$，因此 table1 和 table2 中至少有一张表记录了该分组特征三元组的摘要结果，即正常分组被系统做出假阳性判断的概率为 0.

影响范式检测结果假阴性的因素包括设备的吞吐率 $Output$、分组输入记录摘要表的更新周期 ρ 以及规模 $HSize$，当 $Output=10$ Gbps，$\rho=0.5$ s 时，去重后两张摘要表记录的最大输入分组数量

$$\begin{aligned}InputNum&=\frac{Output}{\text{最长分组长度}}2\rho\\&=\frac{10\times10^9}{1500\times8}\times2\times0.5\\&=833\,333\text{ 个}.\end{aligned}$$

输入分组对摘要表更新过程服从 $P=\frac{1}{HSize}$ 的(0,1)分布，因此两表至少有一表摘要结果为 1 的期望值

$$E=OutPut\times\left(1-\left(1-\frac{1}{HSize}\right)^{InputNum}\right)=833\,010.$$

此时任一输出分组以耦合方式通过匹配校验的最大概率为 833 010/1 G=0.077 58%，即检测系统对攻击分组做出假阴性判断的最高概率不超过 0.077 58%，此时假阴性判断分组个数为 0.077 58%×833 010=647 个.

综合上述理论分析，当 $Output=10$ Gbps，$\rho=0.5$ s，$Hsize=1$ Gbits 时，本文设计的范式检测系统可以 100%判断合法分组，并可识别不低于 99.92%的流量窃听分组. 为验证该判断的准确性，本文利用 X86 系统仿真范式模型的工作流程，并利用实际环境中的真实流量进行范式检测功能评估.

仿真系统采用 MD5 作为 hash 算法，并选择特征三元组摘要值的第 65 到第 94 字节作为摘要结果. 我们从实际网络环境中获取 1 250 450 个分组，实验结果显示，前 833 333 个分组全部通过范式验证. 我们基于该仿真系统实施两种攻击，第 1 种攻击把前 833 333 个分组的目的 IP 地址篡改为 10 个随机 IP 地址，第 2 种攻击在第 1 种攻击的基础上，把所有载荷按字节取反. 图 8 给出两种攻击中窃听分组通过范式检测的数量. 注意实验中错误通过检测分组的平均数量为 626，低于理论值 647. 经统计，实验数据的前 833 333 个分组通过系统后，两张摘要结果表去重后的输入分组记录表中摘要值为 1 的数量为 818 773，此时攻击分组理论通过范式检测的数量为 635，因此实验结果符合理论值.

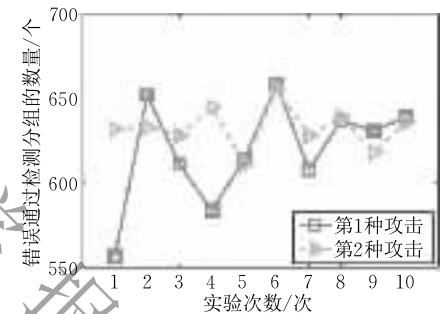

图 8 模拟窃听分组通过范式检测的数量

6.2 范式体系的性能评估

如图 9 所示，路由交换设备的工作效率与其处理单分组的时间周期 T 成反比，T 主要包括传统路由交换时间 $T1$ 和范式检测时间 $T2$. 在固定传统设备和分组长度前提下，$T1$ 固定，因此 $T2$ 直接决定范式设备的工作效率.

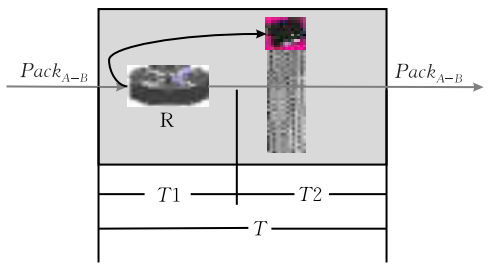

图 9 路由交换设备处理单分组的时间周期

我们利用范式检测系统和真实流量进行范式检测效率评估. 实验过程中实际获取分组 4 897 900

个，其中长度为 1500 字节的分组 4010903 个，占总量的 81.9%. 图 10 给出 $T2$ 的 10 次实验测试结果，由于 $T2$ 可能受分组长度影响，这 10 次实验的分组长度分别为 64、200、400、600、800、1000、1200、1400、1500 和全部实验分组.

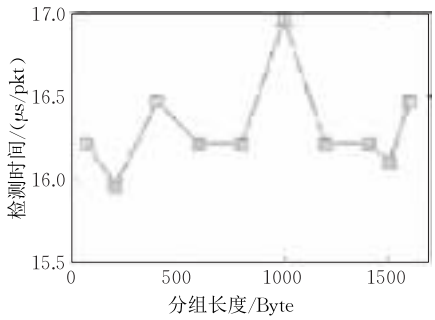

图 10　不同长度分组对应的范式检测周期

实验结果显示，在不超过 1500 字节的前提下，分组长度对 $T2$ 的影响不明显. 图 10 的时间单位为 μs，以均值 16.30μs 作为检测周期，系统范式检测效率随分组长度的不同在 31.4 Mbps 到 736.2 Mbps 之间波动，该结果与 10 Gbps 的期望值差距较大.

当路由交换设备吞吐率为 10 Gbps 时，单分组路由交换周期为 $(1500\times8)/10^{10}=1.2\,\mu s$. 考虑到本实验基于 X86 系统实现，我们进一步利用本实验系统对相同数据的传统路由交换周期 $T1$ 进行仿真，10 次实验结果的平均值为 11.23 μs，实验结果显示对比 $T1$，范式检测周期 $T2$ 的增加比例不明显. $T1$ 实验结果(11.23 μs)与期望值(1.2 μs)同样差距明显，我们认为其原因在于当前汇聚层网络路由设备都采用专用芯片，基于硬件实现路由转发，其工作效率远大于本实验采用的基于通用处理器实现的软件平台[20]，因此在实际应用环境中，利用专用芯片和 FPGA 完成范式检测，有望大幅度提升范式检测效率. 实验所用的 X86 平台的处理器为 Intel i5-2410 双核处理器，RAM 容量 4 G，不低于该配置的检测系统可开发，因此范式路由交换设备的工作效率可满足当前网络需求.

6.3　路由交换范式体系实现关键技术

利用路由交换范式体系实现数据窃听攻击的防御目标，其关键技术主要包括路由交换设备范式检测设备模型设计、输入输出分组特征三元组快速匹配以及漏洞路由交换设备和窃听分组接收主机识别与定位等. 本文已经基于范式体系设计范式检测设备模型，并基于部分摘要表查找给出输入分组特征三元组快速匹配算法，但部分摘要表的使用将导致 0.07758%的假阴性检测结果，这里首先对特征三元组快速匹配算法进行优化，之后给出漏洞路由交换设备和窃听分组接收主机识别与定位技术.

网络分组传输过程中通常要经过多级转发，理想状况下特征三元组一次假阴性匹配输出分组将在后续路由转发过程中被范式检测设备识别与约束，但各次检测的 hash 算法输入参数均为相同的特征三元组，因此后续范式检测结果与首次结果一致，需要对原始匹配算法进行优化.

一种快捷安全的解决方案是在 hash 算法输入参数中加入随机数，随机数同样每隔 2ρ 时间周期进行变化，范式检测设备记录先后两次随机数，并计算相应的两个部分摘要结果，若二者之一能够在摘要表中找到匹配，则认为输出分组存在匹配输入.

经上述优化，假阴性分组被逐级检测，当分组传输路径长度为 n 时，其被判定为数据窃听分组的概率为 0.0007758^n.

由于范式选择〈源 IP，目的 IP，载荷〉作为检测特征，范式检测设备在识别窃听分组后仅需记录特征三元组内容，即可实现漏洞路由交换设备和窃听分组接收主机识别与定位，并了解攻击者试图窃听分组的内容. 若输出分组违反规则 R1，其特征三元组为〈源 IP，Eve，载荷〉，则可判定首次输出该分组的路由交换设备执行了数据窃听操作，窃听分组的接收主机为 Eve，其试图窃听内容即为特征三元组中的载荷部分. 类似地，若输出分组违反规则 R2，其特征三元组为〈路由交换设备 IP，Eve，载荷〉，则可判定数据窃听操作为该路由交换设备，窃听分组的接收主机和试图窃听内容与 R1 情形一致. 若输出分组违反规则 R3，则受检测路由交换设备为漏洞设备，窃听分组的接收主机为路由交换设备将分组转发端口指向的主机. 因此实现漏洞路由交换设备和窃听分组接收主机识别与定位的关键在于窃听分组特征三元组的记录问题，该问题可在核心网络中增设专用存储服务器实现，一旦识别窃听分组，范式检测设备把受检测路由交换设备的 IP 地址以及窃听分组特征三元组发送到专用存储服务器.

7　结论和下一步的工作

针对当前利用设备漏洞窃听用户流量攻击不易被识别和约束的现状，本文提出理论完备的路由交换范式，设计相应的范式设备检测模型，并通过对范

式通用性和可实现性进行优化,给出一种现实可行的利用设备漏洞窃听用户流量攻击的防御方案.本文在理论上证明了本方案的完备性,并通过仿真实验评估了范式检测能力和效率.

为提高应用性,本文所提范式体系尚需在以下方面进行深入研究.首先范式设备在核心网络中的全局部署将增加网络的部署成本和运行开销,拟设计相应的部分部署机制.其次,作为本领域尝试性探索,本文提出一种基于行为结果检测的静态范式,为提高范式的检测效率和应用范围,下一步拟基于动作编码设计基本操作层面的动态范式.最后,除数据窃听攻击外,漏洞路由交换设备还可通过篡改输出分组源地址向目标网络设备发动 DDoS 攻击,危害网络运行安全,需设计面向分组源地址欺骗攻击的路由交换范式体系.

致 谢 感谢"八六三"项目"地址驱动网络关键技术和验证"和清华大学信息科学与技术国家实验室对本项研究工作的资助!

参 考 文 献

[1] Xu Ke, Shen Meng, Chen Wen-Long, et al. Building secure and trusted networks based on routing and switching paradigm. Communications of the CCF, 2015, 11(1): 29-35 (in Chinese)
(徐恪, 沈蒙, 陈文龙等. 基于路由交换范式构建安全可信网络. 中国计算机学会通讯, 2015, 11(1): 29-35)

[2] Xu Ke, Chen Wenlong, Lin Chuang, et al. Toward a practical reconfigurable router: A software component development approach. IEEE Network, 2014, 28(5): 74-80

[3] Dobrescu M, Argyraki K. Software dataplane verication// Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI'14). Seattle, USA. 2014: 101-114

[4] Kothari N, Mahajan R, Millstein T, et al. Finding protocol manipulation attacks//Proceedings of the ACM SIGCOMM 2011 Conference (SigComm 2011). New York, USA, 2011: 26-37

[5] Challener D, Yoder K, Catherman R, et al. A Practical Guide to Trusted Computing. 1st Edition. Indianapolis, USA: IBM Press, 2007

[6] Zhang Huan-Guo, Luo Jie, Jin Gang, et al. Development of trusted computing research. Journal of Wuhan University, 2006, 52(5): 513-518(in Chinese)
(张焕国, 罗捷, 金刚等. 可信计算研究进展. 武汉大学学报, 2006, 52(5): 513-518)

[7] Chen P M, Noble B D. When virtual is better than real// Proceedings of the 8th Workshop on Hot Topic in Operating Systems (HOTOS-VIII). Elmau, Germany, 2001: 133

[8] Garfinkel T, Mendel R. When virtual is harder than real: Security challenges in virtual machine based computing environments//Proceedings of the 10th Workshop on Hot Topics in Operating Systems. Berkeley, USA, 2005: 210-217

[9] Wu Jiang-Xing, Zhang Fan, Luo Xing-Guo, et al. Mimic computing and mimic security defense. Communications of the CCF, 2015, 11(1): 8-13(in Chinese)
(邬江兴, 张帆, 罗兴国等. 拟态计算与拟态安全防御. 中国计算机学会通讯, 2015, 11(1): 8-13)

[10] Xu Ke, Zhu Min, Lin Chuang. Internet architecture evaluation models, mechanisms and methods. Chinese Journal of Computers, 2012, 35(10): 1985-2006(in Chinese)
(徐恪, 朱敏, 林闯. 互联网体系结构评估模型、机制及方法研究综述. 计算机学报, 2012, 35(10): 1985-2006)

[11] Zhang Huan-Guo, Chen Lu, Zhang Li-Qiang. Research on trusted network connection. Chinese Journal of Computers, 2010, 33(1): 706-717(in Chinese)
(张焕国, 陈璐, 张立强. 可信网络连接研究. 计算机学报, 2010, 33(1): 706-717)

[12] Kim T H, Basescu C, Jia L, et al. Lightweight source authentication and path validation//Proceedings of the ACM SIGCOMM 2014 Conference (SigComm'14). Chicago, USA, 2014: 271-282

[13] Ehrenkranz T, Li Jun. On the state of IP spoofing defense. ACM Transactions on Internet Technology, 2009, 9(2): Article 6

[14] Xu Ke, Zhu Liang, Zhu Min. Architecture and key technologies of Internet address security. Journal of Software, 2014, 25(1): 78-97(in Chinese)
(徐恪, 朱亮, 朱敏. 互联网地址安全体系与关键技术. 软件学报, 2014, 25(1): 78-97)

[15] Lin Chuang, Peng Xue-Hai. Study on trustworthy network. Chinese Journal of Computers, 2005, 28(5): 751-758(in Chinese)
(林闯, 彭学海. 可信网络研究. 计算机学报, 2005, 28(5): 751-758)

[16] Meenakshi S P, Raghavan S V. Impact of IPSec overhead on Web application servers//Proceedings of the 2006 International Conference on Advanced Computing and Communications (ADCOM2006). Mangalore, India, 2006: 652-657

[17] Xu Ke, Xu Ming-Wei, Chen Wen-Long, et al. Advanced Computer Networks. Beijing: Tsinghua University Press, 2012(in Chinese)
(徐恪, 徐明伟, 陈文龙等. 高级计算机网络. 北京: 清华大学出版社, 2012)

[18] Kuhn T S. The Structure of Scientific Revolutions. Chicago, USA: The University of Chicago Press, 1962

[19] ISO/IEC. International Standard ISO/IEC 27000. 3rd Edition. 2014

[20] Deepakumara J, Heys H M, Venkatesan R. FPGA implementation of MD5 hahs algorithm//Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE'2001). Toronto, Canada, 2001: 919-924

XU Ke, born in 1974, Ph. D., professor, Ph.D. supervisor. His research interests include network architecture, network security etc.

ZHAO Yu-Dong, born in 1973, Ph. D. candidate. His research interest is network security.

CHEN Wen-Long, born in 1976, Ph. D., associate professor. His research interests include network architecture, routing and switching technology etc.

SHEN Meng, born in 1988, Ph. D., assistant professor. His research interests include network traffic engineering, network virtualization etc.

XU Lei, born in 1982, Ph. D. candidate. His research interest is network security.

Background

This paper aims at defending data interception attacks (DIAs). With such attacks, non-target users take advantage of vulnerabilities embedded in routers and switches to monitor and acquire legitimate users' traffic within core networks.

Because DIAs have characters of low cost, stubborn, concealed and being able to create highly damage, researchers have been paying more and more attentions in defending them. Most current solutions can be broadly categorized in four areas: recognizing and restraining intercepting behaviors routers output, designing secure routers, designing secure networks and encrypting traffic. All these solutions have the ability in preventing or mitigating DIAs, however, it is our humble opinion that current solutions are either only fit for specific core networks and specific types of DIAs, or are difficult to implement. To the best of our knowledge, there are still no security complete, universal and easily implementable mechanisms for defending DIAs.

Based on analyzing all possible abnormal behaviors that vulnerability routers and switches perform, this paper designs and implements a static paradigm-based routing and switching system and the model of paradigm-violation output-packets detector. We prove that the paradigm-based routing and switching system is security complete to data interception attacks. Also all rules of the paradigm are universal applicable to TCP/IP networks, the detector is designable, and the paradigm violations are detectable. Based on simulations, we show that not only 100% of normal packets can pass through the paradigm-based detector, but also about 99.92% of intercepting ones would be caught. In addition, the throughout put of the detected routers/switches can reach Gbps level.

The proposed work of this paper is one of the component of National 863 Project Key Technology and Validation of Address Driven Network (ADN). In order to solve the security challenges that Chinese Internet is facing, this project tries to design dynamic and trusted ADN-based network architecture, addressing and routing system. Trusted routing and switching system can contribute much to these systems.

In order to defending DIAs, we present in [1] the definition of routing and switching paradigm, and proposes to design paradigm-based system to detect and restrain abnormal behaviors routers and switches output. Also [1] analyzes the validation mode and difficulties in design routing and switching paradigm.