暗网的通信方式及监管方法

温赵云，吴　宇，刘航午，陈奎翰，承　洋
（江苏警官学院，南京 210031）

摘要：目前大家普遍使用的互联网是一种构建在统一体系结构和通用通信协议之上的开放网络，开放、共享是现代互联网的基本特点。然而，随着互联网的快速发展，建立在传统互联网基础设施之上、采用特殊技术的暗网开始出现，并成为各类网络犯罪者使用的工具。本文针对基于洋葱路由的暗网通信，分析各国研究现状，研究分析暗网通信原理，根据其脆弱性分析提出监管技术方案。

关键词：暗网；洋葱路由；匿名通信；监管方式
doi：10.3969/J.ISSN.1672-7274.2019.07.095
中图分类号：TN918　　**文献标示码：**A　　**文章编码：**1672-7274（2019）07-0123-03

随着互联网的飞速发展，暗网也进入了公众的视野。暗网强大的匿名性保护了人们的隐私，然而匿名通信技术也是一把双刃剑，它也给网络犯罪调查与追踪带来了极大的困难和严峻的挑战，成为了犯罪分子的天堂，给社会的稳定构成了巨大的潜在危险。找到这些网站的真实 IP 址和查询到访问者的身份信息在技术上存在一定的困难，现有的技术手段在暗网监管中无法发挥有效作用。然后，在网络空间里没有绝对的“自由世界”，对暗网匿名通信规则进行监管刻不容缓。

1　暗网的特点

1.1 认识暗网

我们日常使用的搜索引擎所无法寻找到的，仅能在电脑上进行一系列特殊的操作设置或在特殊软件的辅助之下又或对本机的特殊授权之后方能进入访问的一种网络——即称之为“暗网”。“暗网”之中的数据统统是以常规手段去检索难度极大的“隐身”的方式进行传输交流，服务器地址亦是如此。此外，极高的私密性是其中用户联系彼此的一大特点，对进行拦截的手段和网络技术的要求极高，并且破译拦截后的信息也是一大难题。暗网是深网的一个分支，目前可以通过“洋葱网络”或者“I2P 网络”进行。骇人听闻的是，我们平时所能见的表层网络的域名数量仅仅占据暗网的 1/400 到 1/500。[1]

1.2 洋葱网络

“洋葱网路”这一名称抽象于一个诞生在 1996 年美军实验室的想法，该想法由在实验室进行研究的科学家提出，为实现军事上的数据保护和加密，对服务器隐藏用户身份和实时匿名将会在用户任意时间在某一系统中与 Internet 进行连接时得到保证。因此美国军事机构可以说是暗网技术的起源。洋葱路由网络的一个显而易见的特性是多层加密技术，旨在提高数据安全性。然而，由于这个特点，暗网已被有心者使用，并逐渐成为各种黑暗的聚集地，存在许多非法犯罪交易。包括比特币在内的许多数字货币已成为最受欢迎的交易方式。

1.3 暗网的主要特点

（1）接入简单。只要你掌握了基本的“过墙”技术，隐匿身份访问“暗网”只需要对电脑进行简易设置同时下载并不大的软件。此外，“暗网”开发组织还在智能手机平台上发布了访问软件，方便“暗网”访问。

（2）匿名性强。“暗网”使用分布式、多节点数据访问方法和多层数据加密来为每个数据包设计加密的 IP 地址以进行通信。要获得“暗网”在线记录，必须破解“暗网”使用的加密系统。[2]

（3）金钱往来隐蔽。“暗网”非法交易的主要支付方式是“比特币”，这是一种虚拟电子货币，由具有关联的 64 位数字网络域名组成。比特币不需要买卖双方的个人信息，在技术层面兼顾了效率与安全，在保证了交易的便捷性的同时，又能够保证交易两方的身份保密性。

（4）意识形态混乱。“暗网”本身是由一群自由派和无政府主义者组建的，其中许多人是反对非自由主义或反对政府主义的人，除此之外美国政府刻意地地推波助澜更使得“暗网”的自由倾向非常明显。

2　基于洋葱路由技术的匿名通信

Tor 是基于第一代洋葱路由的低延迟匿名系统，消除了存在于初代洋葱路由带有的匿名通信系统在设计方面的问题的机制和延迟不高，使用方便，部署容易等特点使得由 Dingledine 等人在 2004 年提出的 Tor 得以兼顾用户在性能上的优良体验和安全隐私的保护。Tor 近年来发展迅速。从数十台路由器到世界各地约莫 7000 余个受到志愿者自发进行维护的路由节点以及 300 万余名依靠 Tor 匿名交流联络的用户。Tor 在这一方面的技术不断进步因此匿名集和匿名程度节节攀升。

包含了 IP 地址及端口、公钥和带宽能力的路由描述符被 Tor 中各个洋葱路由节点创建后将会递送到最具权威的当局，网络共识文件由他们依据这些描述符信息来创建，然后打包描述符共同递送目录服务器。图 1 展示了网络在 Tor 中的架构方式。其中既包括客户端和洋葱代理与其路由节点，还有目录与网桥服务器。洋葱代理将会在诸多节点中选出三个节点以行链路中继之效，分别为入口、中间和出口。这一操作将会依据带宽权重路由的选择算法在通信链路被客户端构建时进行。

图1 Tor网络架构

（Tor user）—Tor 用户实体和（Tor node）—Tor 节点实体都属于 Tor。替用户在本地运行应用程序—洋葱代理（OP）程序所创建的通道用于该程序 TCP 数据流的接收和数据流传输。

以下为建立通道和传送消息的过程：

通过对目录服务的访问，储存于 Tor 的节点中的信息得以被 OP 获得。之后，OP 随机选择三个中继节点。只有中继节点中的入口节点知悉通信发起者的身份，通信发起者信息身份的保护及匿名程度深度便依赖于入口节点的选择。如同中介一般的中间节点可了解两方，即入口和出口节点的身份，而这一匿名通信的过程中最初的发出者和最终的接收者的身份对其而言确实不可知。而外部因特网应用层和 Tor 网络的网关以及对 Tor 网络的加密信

基金项目：江苏省高等学校大学生实践创新创业训练计划创新项目“基于洋葱路由的暗网通信及监管技术研究”，编号（201810329014Z）。
江苏省高等学校大学生实践创新创业训练计划《基于洋葱路由的暗网通信及监管技术研究》项目，项目编号：201810329014Z。

息和外部因特网未加密信息的中转传输的角色是出口节点，因此接收者的身份自然是被出口节点所知的。信道在由 OP 搭建的同时，会话密钥在各个中继节点与 OP 协商之后共享。这样的设计好处在于同时知晓信息发送者与接收者身份信息的节点是不存在的，如此一来，匿名通信的实现便达成了。[3]OP 对应用数据的传送便可在信道搭建完成时实现。当发送通信时，OP 将应用消息分成512字节的单元，每个单元依照由中继节点与 OP 共享的会话密钥中的顺序进行加密同时应满足如下顺序来进行：从出口节点到中间节点再到入口节点。数据在经过信道之后由中继节点解密，解密工具为会话密钥。解密之后传输到另一个中继节点继续进行解密。最后由出口节点以明文形式递送到接收者处。

3 基于 Tor 的暗网通信分析

3.1 基于洋葱路由的暗网犯罪案例分析

（1）暗网犯罪难以侦查

暗网平台创办者们前赴后继，暗网犯罪屡禁不止，威胁着各国的安全形势。依靠暗网的匿名服务功能，追踪犯罪者的真实 IP 十分困难，原因主要有三：一是暗网通信的匿名性，二是比特币的匿名性，三是匿名性在暗网之中被现金出现并进行普及的云服务所提高。互联秘密网络虚拟点——网桥能由云服务所运行。或两个或更多网络之间的互联设备。这一类逐渐成为数据隐藏的优良选择的网桥数量在云服务的无形中推动而递增。因此匿名网络的数量不断增加。[4]

（2）破获暗网犯罪的路径探究

与 VPN 类似，Tor 网络使用虚拟通道，但与 VPN 不同，这些通道不直接连接到客户端和服务器，Tor 客户端通过 Tor 网络中的中继站创建电路。Tor 电路具有三大重要特性：首先，所有中继站都无法识别电路端点之间的完整路径；其次，中继站之间的每个连接执行唯一的加密过程；第三，所有连接都是短暂的。由于上述特征，Tor 专用网络路径可以阻止流量分析并支持发布内容而隐匿身份或位置。

由此，我们试图从 Tor 匿名通信系统及所使用协议中寻找技术漏洞，针对其脆弱性进行分析，通过技术突破减少破获暗网犯罪的成本，为网络监管提供方向。

3.2 基于 Tor 暗网的漏洞分析

暗网的脆弱性主要体现在通信节点与通信链路两个方面。

3.2.1 暗网节点选择漏洞分析

对暗网通信的过程简单分析后便知诸如：Hidden Service—隐藏服务器、IP—引入节点和 RP—约会节点以及前文提到的 Tor 客户端、DS—目录服务器、Entry Node—入口节点、Middle Node—中间节点和 Exit Node—出口节点都是暗网实体的组成部分。图2所示展现了隐藏服务器同 Tor 客户端一起需在三跳电路的基础上才能与目录服务器进行信息交流传输。两条六跳电路则是 Tor 客户的基础条件。若需在暗网建立一条完整的通信通道，十八个洋葱路由必不可少。

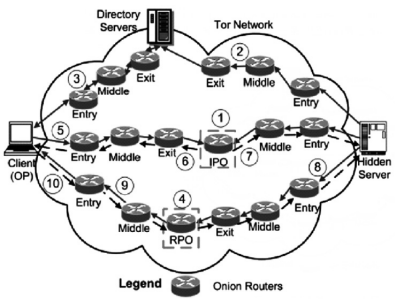

图2 暗网完整通信链路拓扑图

所有洋葱路由即十八个中的其六充当信息交流的两方通过匿名进行连接的目录服务器，另有由六个路由建造而成的通信线路将约会节点的信息发送给隐藏服务，约会节点由 Tor 客户端随机选择。引入节点 IP 由服务提供者随机选择，并且 Tor 用户对约会节点的选择具有随机性，该节点在所有洋葱路由中进行选择。约会节点身份和位置的信息需要通过发出和接收方借助引入节点的帮助来获取。剩余六个路由搭建成为以 Tor 为基础搭建的暗网中的真实数据进行传送的通道—隐藏服务和 Tor 客户端之间的通道。

通过上述分析，已知约会节点是暗网中一个完整的通信程序所必不可少的中枢。暗网之中的各种数据和庞大信息的传输通道由服务提供商联结约束节点与约会节点联结分段的通信链路客户端而构成。二者之间的连接又依赖于约会节点。实际上，用户客户端和隐藏服务的终点均为约会节点，响应于约会节点的数据信息。因此，约会节点在传输中的特殊性可能会导致暗网拓扑的某些漏洞。

3.2.2 暗网拓扑漏洞分析

基于“随机选择”机制，“有心节点”由提前以随机方式构建的形式而存在就成为必然。这和 Tor 路由算法有关，该算法主要包括三种算法：其一是简单随机选择（SRS），DS 之中提供任由 OP 选择的中继节点；其二是带宽加权的随机选择（BWRS），它也选择 DS 中的中继节点，中继节点被选中的几率正相关于自身带宽的大小。其三是调整带宽的加权随机选择（ABWRS），它与 BWRS 计算基本相同，但优先考虑出口节点的带宽。

在常规访问中，三跳访问隐藏节点的引入节点。为了保护服务提供商的匿名性，服务提供商不直接连接到 IP 以确定约会节点的身份信息。出口节点位置会与约会节点位置重合，此外，经过三次的跳转后隐藏服务中的数据信息会抵达约会节点。无论是入口节点，中间节点还是约会节点，都是根据目录服务器中的节点选择列表来选择的。这三个节点形成 Tor 客户端和约会节点之间的通信链路。中间节点掌控着约会节点身份相关信息的知悉权力，因此想要访问约会节点唯有通过这一节点才能实现。[5] 而中间节点的身份相关信息又被入口、约会节点所知，因此依照各节点之间关系，通过入口节点确定中间节点的信息，然后便可依次控制入口、中间及预约节点。取决于目录服务所提供的可选节点信息的路由算法是节点的选择的依靠。目录服务器将会收到来自该节点的最终节点信息。带宽是该算法效率和有效性高低的主导因素。由此可以布设受控入口、受控中间及受控的约会节点来控制暗网用户 Tor 客户端通信链路。

4 暗网的监管方法

4.1 改进通信链路控制方法的研究

约会节点作为整个暗网通信的核心中继节点、控制节点，同时也是存在于暗网通信链路中的脆弱节点，我们可以为易受攻击的约会节点提出一种改善控制暗网通讯链路的方法。

首先要控制住约会的节点，并通过该节点进一步更改其到服务供应商的通讯路线结构。根据入口节点选择策略，从目录服务器中的入口节点列表中直接选择洋葱路由作为暗网用户的入口节点。因为入口处节点的信息列表一段时间才更换一次，所以可以设置与用户端的入口位置信息列表相同的嗅探攻击者。如此就可以通过分析来辨别网络中存在的暗网用户所传来的请求链接。如果暗网用户只用被控制的入口节点，那么就要准备探寻下一个节点的请求链接。一旦链接到正常使用的进入节点，那么就进行重置攻击该节点，如此用户就会与其链接断开然后重新随机寻找进入的节点，如此循环往复直到选到受控制的节点。在控制了进入节点后就可以得到中间位置节点的相应信息，断开受控节点和中间的正常节点之间的链接，再连接相应受控制的约会的节点。把约会节点的相应身份讯息传达到隐藏的服务后，它将从隐藏服务接收指令。以这种方式，受控约会节点立即识别出它是暗网中的数据通信的关键节点，并且清楚地知道发送指令的 IP 地址是隐藏服务的出口节点。然后，攻击者可以对出口节点进行拒绝服务攻击，使出口位置节点不能照常使用，进而导致断路重连。控制

住出口处的节点后，可以辨别中间节点是否受控制。这样，可以完全掌握隐藏用户与隐藏服务的通信链路，暴露隐藏服务的身份信息，暗网的匿名功能消失。[6]

4.2 目录服务

洋葱路由其暗网在本质上其实是分布式的网络，那么就肯定需要组织管理以及维护其分布式中的各个节点，这些任务就要由目录服务来达成。目录服务是指使用泛洪算法来跟踪网络状态的变化。为了减少网络碎片以及降低其传输的负载程度和网络状态不一致等，利用一部分空余的节点来实时跟进其网络拓扑以及节点情况的改变。当目录服务接收到节点自签名的状态信息时，首先要检验节点自带的身份秘钥，假如标识检测通过，则将其相应的信息增加到网络状况描述符中，如果不识别，则丢弃该信息。当新节点加入网络时，新节点必须将应用程序发送到目录服务的管理员，以此确保安全性。

4.3 信任评价机制

在基于洋葱路由的暗网通信中，我们不能确定中间节点所注册的信息是否有效，也无从确定匿名的服务具体什么节点提供的更好。无法确定哪些节点更可能被恶意对手控制。基于以上的原因，应该建立一个信任评价机制。通过信任评估机制，可以对提供服务的中继节点进行排序，并且可以按照排名来选定其作为中继节点，而不只是自主注册填入信息就可以作为中继节点。所以，要防备信道选择恶意节点作为中继节点，还能支持其供给更多计算或网络等优质资源给匿名通信，更好的服务于匿名通信。

4.4 抗恶意行为机制

目前，基于洋葱路由的暗网通信恶意作为的呼应体系是一个导出的策略，它准许出口端节点配置其阻拦访问的 IP 地址和结束的范围。所以出口端节点能成功阻止用户对某些功能进行恶意的访问。该策略能在一定程度上阻止发生恶意的行为。但其效果还不够。因此，基于洋葱路由的暗网通信需要系统完整的反恶意行为机制来应对用户的恶意使用。

反恶意行为体系可以发挥出区分用户是否合法的作用，并阻拦非法用户进行访问，但是不会阻拦系统服务与 IP 地址，而是维护一个恶意行为用户的全局表，另外其中每一个中继节点都会针对性的维护一个非法用户的本地表。而匿名通道的尾节点会根据本地表和全局表进行阻拦对应用户。它将被所有节点阻止，而不是被一个或某种类型的出口节点阻止。[7]

5 结束语

伴着互联网的迅速发展，人们对网络的依赖性越来越强，由此出现的电子商务也在迅速普及。相较于普通的网络通信，商务通信需要更多地保护通讯安全，人们也愈加着重关注于通讯匿名的技术。目前备受欢迎的洋葱路由匿名通讯技术由于其容易操作部署等特点，成为了匿名通讯技术的学术界中不断被探讨的热门问题。本文主要针对基于洋葱路由的暗网通信及监管技术，首先介绍了暗网所依托的洋葱路由技术及暗网的主要特点，然后分析了基于 Tor 的匿名通信机制，分析了其网络漏洞，并对监管技术进行了探讨。洋葱路由作为应用很广泛的匿名通信技术，未来肯定会有更多的学者投身于它的研究。网络安全和信息化是涉及国家安全和国家发展的重大战略问题，关系到广大人民群众的工作生活。要维护我国网络安全，就必须重视匿名通信系统网络犯罪之威胁，并进行有效调整，及时作出相应的应对。

参考文献

[1] 陶短房 . “暗网”从未消逝 . 方圆，2017.（16）.40.
[2] 秦玉海，杨嵩，陈杰 . 针对“暗网”的监管机制研究 . 辽宁警察学院学报，2017.（5）.32.
[3] 暗网的养成：Tor（洋葱路由）的故事 . 网事焦点，2017（11）.65.
[4] 焦康武 . 总体国家安全观视域下我国暗网犯罪应对研究 . 犯罪研究，2017（6）.84-85.
[5] 何高峰，杨明，罗军舟，张璐，马媛媛 . 洋葱路由追踪技术中时间特征的建模与分析 . 计算机学报，2014（2）.369-370.
[6] 鲍凯 . 基于 tor 的暗网脆弱性分析研究 . 电子科技大学硕士学位论文 .2016.5.42.
[7] 刘鑫 . 基于 Tor 网络的匿名通信研究 . 华东师范大学博士学位论文，2011.4.78.

（上接第 122 页）目，只有这样才能实现即满足于人们喜闻乐见的播报内容的需求，又能使广播电台与新兴媒体的融合。

（2）积极寻找融合路径。广播电台应该充分利用互联网积极寻找与新兴媒体融合的路径。现今手机在人们的生活中越来越普遍，所以可以采用手机客户端与广播媒体的融合。广播电台以实用互动的模式让听着可以在手机上进行点播下载，进一步提高受众覆盖率。而且通过微信公众号平台可以收听广播电台相关内容，使听众关注公众号，提高广播电台的知名度。尤其对于在夹缝中生存的县级广播电台媒体，一方面要与新兴媒体融合发展，互利共赢，另一方面还要发挥主流媒体作用，管好新闻舆论阵地，推动广播电台和新兴媒体尽快从相“加”迈向相“融”。一是平台融合，即资源共享，联合发展；二是内容融合，即建立“中央厨房”，占领传播制高点，掌握舆论主动权，从而实现与新兴媒体的深度融合，构建符合社会潮流的主流媒体发展新格局。所以，积极寻找融合路径对于广播电台与新兴媒体融合发展是很有必要的。

4 结束语

此篇文章从广播电台与新兴媒体融合发展的必要性和目前存在的突出问题以及提出相关解决策略的角度进行思考。广播电台在与新兴媒体融合过程中可以提高信息的准确率，而且能够不断满足群众的收听需求。虽然广播电台与新兴媒体融合与发展过程中存在一些不足，但是通过不断创新广播电台原有的管理机制，积极寻找二者相融合的途径的策略使广播电台与新兴媒体完美融合与发展，促进广播电台行业蓬勃发展。

参考文献

[1] 郑伟 . 融媒体时代背景下广播的“新声势”探微 [J]. 记者摇篮，2019（02）：107-109.
[2] 扎西次仁 . 新兴媒体和广播电台的融合发展 [J]. 西部广播电视，2017（15）：77+81.
[3] 李仙芝 . 新媒体时期省级广播电台面临的危机和应对策略 [J]. 新闻爱好者，2016（07）：73-75.
[4] 郝丽婷，王菁，覃继红，邓炘炘 . 国内部分传统广播电台“互联网 + 广播”现状调研 [J]. 中国广播，2016（01）：5-18.

（上接第 78 页）改、新建等各层面，进行辅导分析。

参考文献

[1] 盛蕊 .GIS 技术在通信光缆故障定位系统的应用研究 [D]. 华北电力大学（河北），2010.
[2] 王轶锴，陈伟，杨振昊 . 光纤监测系统设计 [J]. 电子设计工程，2015，23（23）：113 － 115.
[3] 郭斌 . 通信光缆线路日常维护及管理 [J]. 中国新通信，2016，18（23）：14-15.