网络隐蔽信道实现机制及检测技术研究

董丽鹏 陈性元 杨英杰 石 旺
(解放军信息工程大学 郑州 450004)

摘 要 网络隐蔽信道利用正常网络协议传递隐蔽信息,能够为木马、间谍软件等恶意通信规避安全检测提供载体。针对现有隐蔽信道数量众多、特征繁杂、检测不便等问题,在分析其通信模型及应用模式的基础上,提出了一种基于实现机制的分类方法,从协议和字段的根本特点出发研究了隐蔽信道的异常特征,分析了现有检测方法及其缺陷,给出了下一步的研究方向。

关键词 网络隐蔽信道,实现机制,异常特征,检测技术

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.047

Implementation and Detection of Network Covert Channel

DONG Li-peng CHEN Xing-yuan YANG Ying-jie SHI Wang
(PLA Information Engineering University, Zhengzhou 450004, China)

Abstract Network covert channel uses normal network protocols to pass hidden information, which can provide carriers for Trojan, spyware etc. to circumvent security detection. Aiming at the problems that number of convert channels is large, the features are complicated and the detection is inconvenient, we analysed the communication model and application model, proposed a classification method based implementation mechanisms and abnormal features of network covert channel according to the basic features of protocols and fields, analysed existing detection methods and their weaknesses. And the future research direction was given.

Keywords Network covert channel, Implementation mechanism, Abnormal features, Detection techniques

1 引言

网络隐蔽信道概念由系统隐蔽信道[1]引申而来。1987年,Girling[2]首先发现了3种局域网上的隐蔽信道,开启了对计算机网络中隐蔽信道的研究,并将网络隐蔽信道定义为"在现代网络通信中存在的危害网络安全的通信信道"。现实中,不法攻击者主要通过对合法用户通信数据的协议字段、时间间隔、通信行为等进行非法篡改利用来实现隐蔽通信。进入21世纪,计算机网络技术得到了飞速发展,以Web、P2P、流媒体、云计算为代表的网络应用得到了极大丰富,网络带宽呈指数增长,网络中高速流动的数据和大量的不同类型的协议为网络隐蔽信道[3-5]提供了足够的传输载体。同时,隐蔽信道容量也得到了极大提升。如果每个数据包中仅携带1bit的隐蔽数据,那么一个大型网站每年能够为此传输超过26GB的数据[6]。

网络隐蔽信道由于操作简单、隐蔽性强、载体丰富等特点,备受攻击者的青睐。攻击者将恶意通信数据(如木马、间谍软件或恶意程序与控制端的通信)隐蔽在用户的正常通信数据中[7,8],极大地增强了通讯行为的隐蔽性,同时也进一步加剧了隐蔽信道对信息安全的威胁。用户浏览网页,就可能通过JavaScript等小程序引入木马等恶意和间谍代码。用户安装未经安全检测的第三方软件也可能引入间谍或恶意程序,这些代码和程序通过网络隐蔽信道将搜集到的机密信息传输出去,可以轻易地绕开防火墙或IDS的检测,造成信息泄漏。网络隐蔽信道与病毒、木马等间谍技术的结合,严重威胁着网络信息的安全[9]。

从网络隐蔽信道的通信模型及应用模式入手,系统分析了网络隐蔽信道的实现机制,给出了新分类方法与传统OSI模型分类方法的对应关系,说明了时间隐蔽信道的实现情形,根据协议与字段特点,结合实例研究了网络隐蔽信道存在的异常特征,并从技术和产品两个层面分析了现有的网络隐蔽信道检测技术及其存在的不足,指出了下一步研究方向和需要突破的技术。

2 通信模型及应用模式

网络隐蔽信道的经典通信模型即"囚犯模型"由Simmons[10]提出,并由Handel等[11]引入计算机网络。如图1所示,Alice与Bob是监狱中的两名囚犯,需要进行通信协商其越狱计划,而Wendy是监狱的管理者或称监狱长,能够监听甚至更改Alice与Bob之间的所有通信。因此,如何在Wendy

到稿日期:2014-08-05 返修日期:2014-10-29 本文受国家973计划项目(2011CB311801),河南省科技创新人才计划项目(114200510001)资助。
董丽鹏(1987-),男,硕士生,工程师,主要研究方向为信息安全、入侵检测,E-mail:dolipe@sina.com;陈性元(1963-),男,博士,教授,主要研究方向为信息安全、分布式操作系统;杨英杰(1971-),男,博士,副教授,主要研究方向为信息安全、入侵检测;石 旺(1987-),男,硕士生,助理工程师,主要研究方向为信息安全。

的监听下传递隐蔽信息，实现秘密共享，成为 Alice 与 Bob 越狱是否成功的关键。

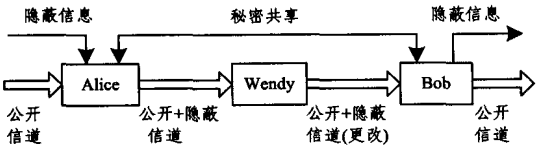

图 1　网络隐蔽信道通信模型

通常情况下，隐蔽信道的发送者和接收者并不一定都是公开信道的发送者和接收者，如图 2 所示。其应用模式主要分为中间人模式和直接通信模式。隐蔽信道的发送者和接收者可以部署在公开信道发送者与接收者之间的路由器或网关上(要求该路由器或网关靠近公开信道一方网络的边缘)，也可以部署在该相同物理设备中更低层网络协议栈中。应用场景的不同决定了隐蔽信道实施的时机、方法、信道容量及安全程度等。

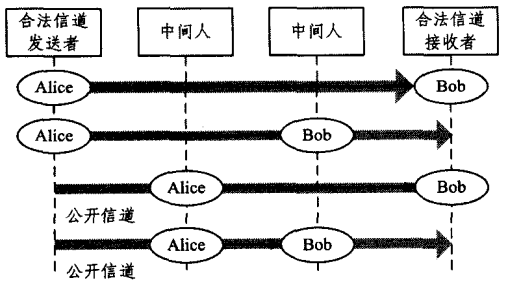

图 2　网络隐蔽信道应用模式

3　隐蔽信道实现机制

传统上，与系统隐蔽信道类似，将网络隐蔽信道分为存储隐蔽信道和时间隐蔽信道两种[12]，2005 年 Llamas 等[13]总结描述了 TCP/IP 协议中公布的网络时间和存储隐蔽信道。存储隐蔽信道主要是在各种协议的数据包字段或应用层编码[14]中隐蔽信息。网络时间隐蔽信道则一般利用网络中传输数据包的时间特性来表示信息，这些时间特性包括数据包的发送/到达时刻、间隔时间[9,15,16]等。也有基于网络 OSI 模型划分的，将其分为物理层、网络层、传输层和应用层的隐蔽信道等，相对而言，上层协议丰富，信息隐蔽更加灵活，难以发现，而有些信道则存在于多个层次之间，使用相同的机制进行隐蔽传输，比如基于地址修改的隐蔽传输可对应于物理层的 MAC 地址隐蔽、网络层的 IP 地址隐蔽和传输层的 UDP/TCP 端口号等。2007 年 Zander 等[8]将出现的隐蔽信道进行了全面细致的描述；Cai 等[17]提出了一种基于熵的分类方法；2014 年 Wendzel 等[18]将网络隐蔽信道划分为 11 种模式，并使用模式语言标识语言 PLML 进行了描述。

因此，本文采用分层模型与隐蔽机制相结合的混合分类方式，对网络隐蔽信道分类，结果如表 1 所列。

表 1　网络隐蔽信道分类

分层 \ 机制	协议首部	报文格式	报文内容	重传机制	封包操作	协议操作
物理层	—	—	—	√	—	—
网络层	√	√	√	—	√	√
传输层	√	—	—	√	√	—
应用层	—	√	√	—	—	√

(1)基于协议首部字段的隐蔽信道

网络隐蔽信道通常使用网络数据包的协议控制部分或扩展数据部分加载信息，包括以下机制：

a)将信息附加在首部的未用字段，包括未用的 IP 首部字段，如 DF[19]、TOS[11]字段，TCP 首部的紧急 URG[20]和复位 RST[6]标志位等。

b)将信息附加在首部扩展或填充字段，包括 IP 首部的选项[21]和填充字段[22]、IPv6 首部目的选项[23]、安全扩展首部[24]、IP 首部路由记录选项[25]等。

c)将信息附加在首部常用字段，如 IP 标识符[26,43]、碎片偏移[27]、生存时间(TTL)字段[28]、TCP 初始化序列号[26,29]和时间戳[11]等。

d)通过改变首部某些选项的位置或数量来编码隐蔽信息，如改变 IPv4 选项列表中选项位置、IPv6 扩展头部中选项位置或原始 IP 包产生的分片数量[44]等。

(2)基于报文格式的隐蔽信道

应用层协议种类繁多、设计灵活，其隐蔽信道的隐蔽方式也更为灵活，通常使用应用层报文格式中没有严格定义的部分。

a)通过改变报文中某些部分的序列来隐蔽信息，如 HTTP 协议头部域的序列[30]、动态主机配置 DHCP 协议中的选项序列[31]及文件传输 FTP 协议中的命令序列[32]等。

b)通过对字段位置的修改来编码隐蔽信息，如使用 DHCP 协议选项列表中的选项位置[31]。

(3)基于报文内容修改的隐蔽信道

通常认为直接对报文内容进行修改的信道不具有通信行为及内容的隐蔽性，应将其归属为隐写信道或加密信道，不属于隐蔽信道研究范畴。但一些特殊协议的报文内容也能够用于传输隐蔽信息。

a)利用网际控制报文 ICMP 协议回显请求与应答报文[33,34]的数据部分传递隐蔽信息，利用安全防护设备通常不检测 ICMP 数据的特点实现隐蔽。

b)利用域名解析协议 DNS 回答报文的资源记录数据传递隐蔽信息[33,35]，基于不同实现方式可分为基于域名和基于域名服务器两种。

c)在规定了首部的报文中增加额外的域或字节来传输隐蔽信息，例如在 HTTP[30]首部、简单邮件传输协议 SMTP[36]首部、可扩展通讯和表示协议 XMPP 报文[37]增加域，在加密的 SSH 报文[38]增加字节等。

(4)基于重传机制的隐蔽信道

重传机制广泛应用于物理层帧传输和传输层 TCP 协议中，用于确保数据包的正确送达。

a)在 MAC 层使用重传机制，MAC 层采用载波监听多点接入/碰撞检测(CSMA/CD)机制来协调总线上各计算机上帧的传输。Handel 等人[11]通过设置退避时间为 0 或者最大值向接收者传送 0 或 1。

b)在无线网络中使用重传机制。Kratzer 等人[39]在802.11 协议中通过帧重放来传输隐蔽信息。

c)在传输层 TCP 协议使用重传机制。TCP 协议采用超时重传、快重传和快恢复、选择确认等机制来确保面向连接的可靠交付。Mazurczyk 等人[41]提出了基于 TCP 协议的重传隐蔽 RSTEG 方法。

(5)基于封包操作的隐蔽信道

网络封包是指在网络中以指定协议传输的数据包,或者称数据包的打包发送为封包。

a)通过对封包进行丢失和排序操作实现隐蔽信息传输。封包丢失通过在发送端人工操作丢失数据包,此处要求每个数据包有一个序列号,这样接收端能通过跳过的序列号来接收隐蔽信息。对于一串相连的 n 个数据包,能够有 $n!$ 种排列方式,通过重排序最大可传输 $\log_2 n!$ 比特。发送者通过修改数据包对应序列号或者目的地址编码实现隐蔽信道,如使用 TCP 序列号[41]、IPSec 协议的 AH(Authentication Header)[42]或者 ESP(Encapsulating Security Payload)序列号等。

b)通过改变网络封包大小来编码隐蔽信息,如 IP 分片大小[43,44]、IPSec 封包大小[45]及其他网络封包的消息长度[46]等。

c)通过改变封包发送时间来编码隐蔽信息,主要用于产生时间隐蔽信道,如基于 Web 服务器响应的隐蔽时间信道[20]。

(6)基于协议操作的隐蔽信道

通过网络中流量控制协议的使用来改变数据包传输的速率或者时间间隔,因此可以构造基于时间的隐蔽信道[47]。

a)在无线网络中使用控制协议。Handel 等[11]提出了一种基于无线网络协议中清除发送/请求发送(Clear to send/Ready to send,CTS/RTS)信号修改的隐蔽信道。

b)在计算机网络中使用控制协议,使用 ICMP 协议的源抑制消息[48]来控制消息传输的速率。

4 隐蔽特征分析

针对纷繁多样的隐蔽信道,检测者们几乎为每种信道都提取了相关字段、数据包和连接的多种特征用于模式匹配、机器学习和检测,这些方法检测准确性较高,但由于很多特征基于统计方法获得,时效性略显不足。下面以网络存储隐蔽信道为研究重点,根据协议和数据包特点,从字段特性、字段关系和协议行为等方面分析了隐蔽信道的特征。

(1)常量字段的跳跃(波动)特征

网络数据流中,可用于隐蔽信息传输的字段根据其在网络协议实现中的取值特性分为两种:常量字段和随机字段。常量字段指那些在网络数据包实现中字段取值相对固定、取值范围为有限个(≤255)的字段,其中,协议版本号和标志位最为典型,协议版本号通常为固定 1 个取值,而标志位则只有 0 或 1 两个取值。另外,我们认为 IP 协议的 TTL 值也是常量字段,因为对于相同通信双方、相同协议之间的通信,其到达网络同一节点的 TTL 值也应该是相对固定的,或者说差异较小。

常量字段的跳跃特征以基于 TTL 值的隐蔽信道为典型,主要分为 3 种类型:

a) 直接编码:直接将隐蔽信息 bits 放入 TTL 字段中;

b) 映射编码:将指定的 TTL 值映射为隐蔽信息编码;

c) 差别编码:将连续 TTL 值的变化用于编码隐蔽信息。

基于 TTL 值的隐蔽信道有以下几种:Qu04-1[49]使用映射编码放置隐蔽信息位,原始的 TTL 值代表 0,将 TTL 值增加一个整数 Δ 代表 1;Qu04-2 则将隐蔽信息直接存放在 TTL 值的最低 bit;Lucena 的 Lu05 隐蔽信道[50]利用 IPv6 协议中的跳数限制字段(等同于 IPv4 中的 TTL),将 TTL 值增加一个整数 Δ 代表 1,降低一个整数 Δ 代表 0;Zander 设计的 Za06 信道[28]仅对 TTL 执行降值操作,而不违背 IP 标准,它使用原始 TTL 值代表 0,将 TTL 值减去 Δ 代表 1;而 Sebastian Zander 的 Scheme1 信道[51]与 Qu04-2 类似,将隐蔽信道值直接编码到 TTL 值中,以 TTL 的变化来代表 0 或 1;Scheme2 信道采用与信号交替反转编码(Alternate Mark Inversion,AMI)类似的差分编码方式隐蔽信息,保证了 TTL 值不会增加,而且其变化值不会超过 1。各种实现方式的跳跃特性如图 3 所示。

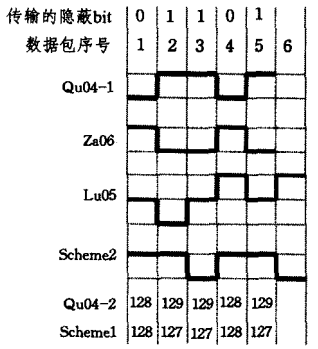

图 3 TTL 隐蔽信道的跳跃特征

由图 3 可以看出,通过增加 TTL 值的方式隐蔽信息会导致 TTL 值轻微地高于正常的初始 TTL 值;而 Lu05 没有对 TTL 值修改设定上限,则一长串的 0,1 序列会导致 TTL 值出现较大的上下波动。但通常情况下,固定通信双方之间出现两个不同的 TTL 值的情况在正常数据流中是极其少见的,因此可以通过其变化特性检测 TTL 隐蔽信道的存在。

另外,对于 TCP 协议,如果其序列号、IP 地址、端口地址存在跳跃特征,则可能存在隐蔽信道,而如果数据包延迟时间存在规律性的跳跃特征,也可能是存在基于时间间隔的隐蔽信道。

同样,对于 HTTP、ftp 等应用层传输协议,如果其命令或者参数序列发生了规律性的跳跃,则可能存在隐蔽信道。对于 ICMP 协议,若协议选项或命令类型存在跳跃关系,则也极有可能存在着隐蔽信道。

(2)随机字段的规律性特征

随机字段是指字段取值不确定,由协议本身根据需要随机生成的;或者是取值内容随机的字段。最为典型的是协议负载字段,由于其使用空间大,每次传输数据不相同,可认为其是随机字段;另外数据包首部中的 TCP ISN 字段等由操作系统随机生成,也属于随机字段。随机字段在经过人为修改后会体现出一定的规律或特征,通过统计或判断可以检测其中存在的隐蔽信道。

TCP ISN 字段最早被用于隐蔽信道传输,初期的 TCP ISN 隐蔽直接将隐蔽信道的每个字节乘以 2563 作为 ISN 传输,但其只是将要传输的隐蔽信息直接替换掉原来的 ISN,并不符合 ISN 值不重叠和唯一性的要求,容易被检测出。NUSHU 是一种典型的 TCP ISN 隐蔽信道,它在将隐蔽数据放入 ISN 之前会首先对其进行加密,这就会导致其不同于 Linux 下正常模式生成的 ISN 的分布。其数据隐蔽方式如图 4 所示,首先对数据进行加密(使其看起来更像是伪随机过程),然后放入 ISN 域中。加密机制是采用一个 NUSHU 使用者与读取者共享的私钥对(源端口⊕目的端口 ‖ 源 IP 地址

⊕目的 IP 地址)进行 DES 加密,将前 32 位值与根据 CC 协议生成的 32 位 ISN 值进行异或,用作最终的 ISN 值传输。当 TCP ISN 冲突发生时,可以对 ISN 进行异或来移除关键字流,由于这是两个明文的异或,因此结果也同样是明文。如果这些明文是相同的,且此时没有数据传输,则结果应当等于 0,否则说明该 ISN 域被人为编码了。

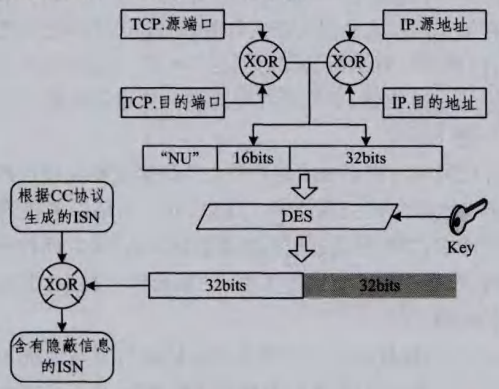

图 4 NUSHU 隐蔽信道

另外,在低速的网络连接中,时间戳的低阶位会体现出一定的随机性,因此对于 devcc 信道实现的 TCP 时间戳隐蔽信道,若低有效位出现一定的规律性,则说明隐蔽信道存在。对于高带宽 TCP 连接,监听者可以计算时间戳值的数量占开始和结束时间戳值之间不同的比率,如果接近 0.75,说明 devcc 隐蔽信道存在,如果接近于 1,则没有。

此外,隐蔽信道的开发者经常会使用编码映射方式对隐蔽信息进行传输,这样会使得随机字段的取值或字节值重复出现,打破原有字段的随机性。

(3)关联字段间的约束关系异常

每个网络协议都是一个有机的整体,实现网络中特定的数据交换。协议的语法规定了协议中数据和控制信息的结构及格式,协议各字段间存在着千丝万缕的联系。有的属强关联关系,相互之间互为补充或者互相排斥,如 ICMP 协议中的消息类型字段与其传输负载、数据包首部与校验和字段都是互相补充说明的关系,而 IP 协议首部中 DF 和 MF 字段则为互斥关系,二者不能同时为 1 或者 0。有些则属于弱关联关系,如 TCP 选项的顺序、HTTP 协议中字段的顺序,协议规范中并没有完全设定其出现顺序,但在具体的协议实现时其会以固定的顺序出现。

```
⊟ Hypertext Transfer Protocol
  ⊞ GET / HTTP/1.1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:29.0) Gecko/20100101 Firefox
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\
    Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Referer: http://www.baidu.com/\r\n
    Host: www.smzdm.com\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.smzdm.com/]
    [HTTP request 1/41]
    [Next request in frame: 100]

Hypertext Transfer Protocol
⊞ GET /wp-content/themes/smzdm_two_year/style.css?v=201405141500 HTTP/1.1\r\
  User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:29.0) Gecko/20100101 Firefox/2
  Accept: text/css,*/*;q=0.1\r\n
  Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Referer: http://www.smzdm.com/\r\n
  Host: www.smzdm.com\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://www.smzdm.com/wp-content/themes/smzdm_two_year/s
  [HTTP request 1/25]
  [Next request in frame: 141]
```

图 5 利用字段顺序隐蔽信息

基于字段位置的隐蔽信道常被用于设计较为开放的协议,如 IPv4 选项中的字段顺序、IPv6 扩展首部顺序等。HTTP 协议首部字段的排序也是常用的隐蔽方法,具体实现见图 5,通过改变 Host 字段和 Connection 字段的顺序分别代表 0 或 1。

同样,ICMP 隐蔽信道会将回显应答报文(报文类型字段值为 0x0)的负载(通常为延时及路由器地址等信息)用以传输隐蔽信息,对其检测时只需将报文类型字段值与负载信息进行关联检测即可。

(4)通信行为的异常特征

协议是控制两个对等实体进行通信的规则的集合,对等实体进行信息传递的过程就称为通信行为,此处实体是指任何能够发送或接收信息的硬件或软件进程。在特定网络环境下,通信协议双方会表现出某些具有固定特征的通信行为,如流量特征、统计特征和连接特征等。对于非中间人场景下的网络隐蔽信道,使用者往往会最大程度地利用自身通信自主的优点,但与此同时,也会使其表现出异于寻常的通信行为特征。

重传机制广泛应用于物理层帧传输和传输层 TCP 协议中,用于确保数据包的正确送达。MAC 层采用载波监听多点接入/碰撞检测(CSMA/CD)机制来协调总线上各计算机上帧的传输,Handel 等人[11]通过设置退避时间为 0 或者最大值向接收者传送 0 或 1。Kratzer 等人[52]在 802.11 协议中通过帧重放来传输隐蔽信息。TCP 协议中采用超时重传、快重传和快恢复、选择确认等机制来确保面向连接的可靠交付,Mazurczyk 等人[40]提出 TCP 协议的 RSTEG 方法(Retransmission Steganography),通过人为控制超时,并在重传数据包的负载中携带隐蔽信息实现隐蔽传输。利用超时重传进行隐蔽信息传输的机理如图 6 所示。但事实上,在相对稳定的网络中,数据包的重传概率也是相对稳定的,应用程序利用重传机制进行隐蔽信息传输会大大增加重传概率,这样便很容易被检测到。

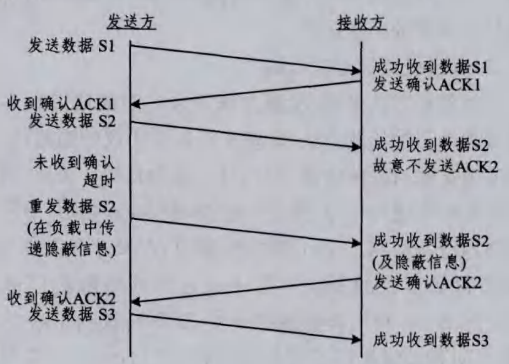

图 6 基于超时的重传隐蔽信道

另外,基于 DNS 协议及 ICMP 协议的隐蔽信息传输都需要通信双方相互配合进行信息传输,但正常操作中要求通信的发起方为内网实体,由内网实体向外网实体发出请求报文,并由外网实体发送应答报文。这样,根据通信发起方的不同,将隐蔽通信分为两种模式。当外网实体需要首先发起隐蔽通信时,其需要直接伪装回答报文发送给内网实体,这就造成了通信行为的不完整,可以根据通信连接的完整性检测出一些此类的隐蔽信道。

此外，为提高传输效率，某些隐蔽信道会人为增加传输载体的频率，如大多数基于 TCP ISN 的连接只能在每个连接中传输 16bits 甚至 1bit 的隐蔽信息，如果网络中出现大量频繁的异常 TCP 连接，则可能是 TCP ISN 隐蔽传输。

5 隐蔽信道检测技术分析

网络隐蔽信道检测技术可根据其对数据的获取和处理方式不同，分为网络隐蔽信道审计(Auditing)技术和识别(Identification)技术[8]。而鉴于隐蔽信道的特殊性，目前大多数检测技术都属于对网络流数据集的审计技术，即通过一个被动的监控者进行数据采集，根据某隐蔽信道的特点对数据集进行特征匹配、统计分析或机器训练与识别等，以检测其中可能存在的隐蔽信道。

(1)基于特征匹配的检测

基于特征匹配的检测技术适用于实现简单、具有明显特征的单一方式隐蔽信道，如基于 TCP/IP 数据首部字段的隐蔽信道。文献[43]中给出了 IP ID、TCP ISN 等隐蔽字段的特性，并提出了 NUSHU 信道、TCP 时间戳信道的检测方法，但其缺点是只能对单一方式的隐蔽信道进行检测，且检测阈值不易确定。

(2)基于统计分析的检测

基于统计分析的检测技术则更适用于具有明显统计特征的隐蔽信道，如对多主机、多软件协同工作的隐蔽信道统计其通信链路长度，对符合泊松分布的局域网流量实施流量统计分析等。华元彬等[53]针对 Active Port Forward、Covert Channel Tunneling Tool 等软件的隐蔽特点，采用基于链路长度统计的分析方法；薛晋康等[54]针对局域网系统中的流量特性采用了基于流量统计的分析方法；对于采用编码方式传输信息的隐蔽信道，同一个字段值可能会在网络数据包中重复出现，对此钱玉文[55]采用了基于模糊 Petri 网的已知隐蔽信道检测和基于密度聚类的未知隐蔽信道检测方法。但此方法的缺点是仅从宏观角度分析网络流量特征，准确率低，不能判断是什么类型的隐蔽信道。

(3)基于机器学习的检测

针对隐蔽方式多样、检测方法复杂的隐蔽信道则多采取基于机器学习的检测方法，如基于应用层协议的隐蔽信道等。其方法是首先对隐蔽信道进行分析，提取其特征属性，通过大量的训练样本进行学习，建立判断规则和检测模型，最后对待识别样本进行检测。Sohn 等提出利用 SVM 来检测 IP 的 ID 字段和 TCP 协议的 ISN 字段中潜在的网络隐蔽信道的方法[56]；Tumoian 利用神经网络研究 TCP 协议的 ISN 的检测问题，并对相关结果进行可靠性分析[57,58]；Borders 等利用基于相似的方法研究并开发了一个工具用来检测 HTTP 协议中的网络隐蔽信道[59]；章思宇等[60]利用 J48 决策树、朴素贝叶斯(Naive Bayes)和逻辑回归(Logistic Regression，LR)算法对基于 DNS 的隐蔽信道进行了检测，取得了良好的效果，但其缺点是对检测样本的数量要求较高，时效性较差。

网络隐蔽信道的在线检测与识别是进行隐蔽信道限制与阻断的前提，但当前的安全防护系统(主要是入侵检测系统)并未提供全面的网络隐蔽信道检测服务，大多数仅支持对基于静态数据段修改或具有简单数据行为特征的隐蔽信道进行预警，如 SNORT 系统[61]的 icmp_id、icmp_seq 检测或 Enterasys NIDS[62,63]的 ICMP 负载隐蔽信道检测等，存在可检测种类少、检测方式单一等问题。

离开了网络，隐蔽信道的检测便失去了一半的价值。在线检测与识别需要优先考虑时效性和准确率。高速网络环境中，数据流的处理必须面临两个问题，即少量的扫描次数和有限的存储空间。这是因为在实际环境中，软硬件处理性能的限制，使得海量数据流的实时到达不允许安全软件对网络数据包进行多次扫描，更无法在硬盘空间中进行大量存储实现复杂的统计分析。

在线检测与识别技术需要首先对海量数据流进行概要信息提取及数据流的关联处理。这里，面对网络隐蔽信道检测的特殊需求，对哪些信息进行概要数据提取、采取何种概要提取算法，对哪些数据流进行关联、关联到哪个层次，都是需要解决的问题。

同时，高速数据流下的网络隐蔽信道检测与传统入侵检测方法也有很大不同，不仅需要深度包解析，更需要多数据流的关联查询，在线及存档数据的结合利用，数据包检测引擎与网络异常行为检测引擎的综合决策。因此网络隐蔽信道事件模式如何定义，检测引擎如何设计与优化，都是实现网络隐蔽信道在线检测需要突破的关键技术。

结束语 在过去的二三十年，随着网络技术的飞速发展，各式各样的网络隐蔽信道也逐渐泛滥起来，它们隐藏在网络中的各个角落，让人防不胜防。其与病毒、木马、间谍软件等恶意程序的结合为网络安全带来了诸多隐患。

当前的隐蔽信道检测技术存在针对面窄、时效性弱等问题，本文着眼于高速网络环境中的隐蔽信道发现问题，从通信模型、应用模式、实现机制、隐蔽特征等方面层层递进地进行了分析，同时结合隐蔽信道检测技术的现状及不足提出了下一步研究思路和目标。

参 考 文 献

[1] Lampson B W. A note on the confinement problem[J]. Communications of the ACM, 1973, 16(10): 613-615

[2] Girling C G. Covert Channels in LAN's[J]. IEEE Transactions on Software Engineering, 1987(2): 292-296

[3] Kratzer C, Dittmann J, Vogel T, et al. Design and Evaluation of Steganography for Voice-over-IP [C] // Proceedings of 2006 IEEE International Symposium on Circuits and System (ISCAS 2006). IEEE, 2006

[4] Bates A, Mood B, Pletcher J, et al. On detecting co-resident cloud instances using network flow watermarking techniques [J]. International Journal of Information Security, 2014, 13(2): 171-189

[5] Ranjith P, Priya C, Shalini K. On covert channels between virtual machines[J]. Journal in Computer Virology, 2012, 8(3): 85-97

[6] Fisk G, Fisk M, Papadopoulos C, et al. Eliminating steganography in Internet traffic with active wardens[C] // Petitcolas F A P, ed. Information Hiding: 5th International Workshop, IH 2002. Springer Berlin Heidelberg, 2003: 18-35

[7] Lucena N B, Lewandowski G, Chapin S J. Covert channels in IPv6[C] // Danezis G, Martin D, eds. Privacy Enhancing Technologies: 5th International Workshop, PET 2005. Springer Ber-

lin Heidelberg,2006:147-166

[8] Zander S, Armitage G J, Branch P. A survey of covert channels and countermeasures in computer network protocols[J]. IEEE Communications Surveys and Tutorials, 2007, 9(1-4): 44-57

[9] Gianvecchio S, Wang H. Detecting covert timing channels: an entropy-based approach[C]// Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007: 307-316

[10] Simmons G J. The prisoners' problem and the subliminal channel[C]// Advances in Cryptology. Springer US, 1984: 51-67

[11] Handel T G, Sandford II M T. Hiding data in the OSI network model[C] // Information Hiding. Springer Berlin Heidelberg, 1996: 23-38

[12] 王永吉,吴敬征,曾海涛,等. 隐蔽信道研究[J]. 软件学报, 2010, 21(9): 2262-2288
Wang Yong-ji, Wu Jing-zheng, Zeng Hai-tao, et al. Covert Channel Research[J]. Journal of Software, 2010, 21(9): 2262-2288

[13] Llamas D, Allison C, Miller A. Covert channels in internet protocols: A survey[C]// Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, PGNET 2005. 2005

[14] Sun Xing-ming, Huang Hua-jun, Wang Bao-wei, et al. An algorithm of webpage information hiding based on equal tag[J]. Journal of Computer Research and Development, 2007, 44(5): 756-760

[15] Cabuk S, Brodley C E, Shields C. IP covert timing channels: design and detection[C]// Proceedings of the 11th ACM Conference on Computer and Communications Security. ACM, 2004: 178-187

[16] Berk V, Giani A, Cybenko G, et al. Detection of covert channel encoding in network packet delays, Technique Report TR536 [R]. de lUniversité de Dartmouth, 2005: 35-43

[17] Cai Zhi-yong, Zhang Yong. Entropy based taxonomy of network convert channels[C] // 2009 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS). IEEE, 2009: 451-455

[18] Wendzel S, Zander S, Fechner B, et al. A Pattern-based Survey and Categorization of Network Covert Channel Techniques[J]. ACM Computing Surverys, 2015, 47(3): 1-26

[19] Kundur D, Ahsan K. Practical Internet steganography: data hiding in IP[C]// Proceedings of the Texas Workshop on Security of Information Systems. 2003

[20] Hintz A. Covert channels in TCP and IP headers[Z]. DEFCON, 2002

[21] Trabelsi Z, Jawhar I. Covert file transfer protocol based on the IP record route option[J]. Information Assurance and Security, 2010, 5: 64-73

[22] Wolf M. Covert channels in LAN protocols[M]// Berson T A, Beth T, eds. Local Area Network Security. Springer Berlin Heidelberg, 1989: 89-101

[23] Graf T. Messaging over IPv6 destination options[EB/OL]. http://grayworld.net/papers/messip6.txt

[24] Lucena N B, Lewandowski G, Chapin S J. Covert channels in IPv6[C] // Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2006: 147-166

[25] Trabelsi Z, El-Sayed H, Frikha L, et al. Traceroute based IP channel for sending hidden short messages[M]// Advances in Information and Computer Security. Springer Berlin Heidelberg, 2006: 421-436

[26] Rowland C H. Covert channels in the TCP/IP protocol suite[J]. First Monday, 1997, 2(5): 42-51

[27] Cauich E, Cárdenas R G, Watanabe R. Data hiding in identification and offset IP fields[M]// Advanced Distributed Systems. Springer Berlin Heidelberg, 2005: 118-125

[28] Zander S, Armitage G, Branch P. Covert channels in the IP time to live field[C]// Proceedings of Australian Telecommunication Networks and Applications Conference (ATNAC). 2006

[29] Rutkowska J. The implementation of passive covert channels in the Linux kernel[C]// Chaos Communication Congress, Chaos Computer Club eV. 2004

[30] Dyatlov A, Castro S. Exploitation of data streams authorized by a network access control system for arbitrary data transfers: tunneling and covert channels over the HTTP protocol[EB/OL]. http://grayworld.net/projects/papers/html/covertpaper.html. 2003

[31] Rios R, Onieva J A, Lopez J. HIDE_DHCP: Covert Communications through Network Configuration Messages[M]// Information Security and Privacy Research. Springer Berlin Heidelberg, 2012: 162-173

[32] Zou X, Li Q, Sun S H, et al. The research on information hiding based on command sequence of FTP protocol[C]// Knowledge-Based Intelligent Information and Engineering Systems. Springer Berlin Heidelberg, 2005: 1079-1085

[33] Smeets M, Koot M. Research report: Covert channels[R]. Holland: University of Amsterdam, 2006

[34] Stødle D. Ping Tunnel: For those times when everything else is blocked[EB/OL]. http://www.cs.uit.no/~daniels/PingTunnel, 2009

[35] Kaminsky D. Black Ops of DNS[Z]. Black Hat Briefings, 2004

[36] Getchell A. RE: For those interested in covert channels [EB/OL]. http://www.security-focus.com/archive/101/499640. 2008

[37] Patuck R, Hernandez-Castro J. Steganography using the Extensible Messaging and Presence Protocol (XMPP)[J]. arXiv preprint arXiv: 1310.0524, 2013

[38] Lucena N B, Pease J, Yadollahpour P, et al. Syntax and semantics-preserving application-layer protocol steganography[C]// Information Hiding. Springer Berlin Heidelberg, 2005: 164-179

[39] Krätzer C, Dittmann J, Lang A, et al. WLAN steganography: a first practical review[C] //Proceedings of the 8th Workshop on Multimedia and Security. ACM, 2006: 17-22

[40] Mazurczyk W, Smolarczyk M, Szczypiorski K. Hiding information in retransmissions[J]. arXiv preprint arXiv: 0905.0363, 2009

[41] Luo X, Chan E W W, Chang R K C. Cloak: A ten-fold way for reliable covert communications[M]// Computer Security-ESORICS 2007. Springer Berlin Heidelberg, 2007: 283-298

[42] Ahsan K, Kundur D. Practical data hiding in TCP/IP[C]// Proc. ACM Workshop on Multimedia Security, 2002. 2002

(下转第 244 页)

481-490

[6] Leung Wai-ting, Lee D L, Lee W-C. Personalized Web search with location preferences[C]// Proc. of ICDE'2010. 2010:701-712

[7] Lu Yu-mao, Peng Fu-chun, Wei Xing, et al. Personalize Web search results with user's location[C]// Proc. of SIGIR'2010. 2010:763-764

[8] Leon R A D, Yang Bin, Christian S J. Towards context-aware search and analysis on social media data[C]// Proc. of EDBT 2013. 2013:137-142

[9] Alonso O, Strogen J, Baeza-Yates R, et al. Temporal information retrieval:chanllenges and opportunities[C]// Proc. of TempWeb workshop. 2011:1-8

[10] Zhang R, Chang Y, Zheng Z, et al. Search result re-ranking by feedback control adjustment for time-sensitive query[C]// Proc. of NAACL. 2009:165-168

[11] Alonso O, Baeza-Yates R, Gertz M. Effectiveness of temporal snippets[C]// Proc. of WWW'. 2009

[12] Jones R, Diaz F. Temporal profiles of queries [J]. ACM Transactions on Information System, 2007, 25(3)

[13] Metzler D, Jones R, Peng F, et al. Improving search relevance for implicitly temporal queries[C]// Proc. of SIGIR. 2009:700-701

[14] Alonso O, Strotgen J, Baeza-Yates R, et al. Temporal information retrieval: challenges and opportunities [C] // Proc. of TWAW. 2011:1-8

[15] Kanhabua N, Novag K. Determining time of queries for re-ranking search results[C]// Proc. of European Conference on Digital Libraries(ECDL). 2010:261-272

[16] Kulkarni A, Teevan J, Svore K M, et al. Understanding temporal query dynamics[C]// Proc. of WSDM. 2011:167-176

[17] Gey F C, Kando N, Larson R R. The crucial Role of semantic discovery and markup in Geo-temporal search[C] // Proc. of CIKM. 2010:5-6

[18] Kamath K, Caverlee J, Lee K, et al. Spatio-Temporal Dynamics of Global Social Media[C]// Proc. of WWW. 2013

[19] Liu Ye-feng, Alexandrova T, Nakajima T. Using Stranger as Sensors: Temporal and Geo-sensitive Q&A via Social Media[C]// Proc. of WWW'. 2013

[20] Strotgen J, Gertz M. Proximity2-aware ranking for textual, temporal, and geographic queries[C]// Proc. of CIKM. 2013

(上接第 221 页)

[43] Murdoch S J, Lewis S. Embedding covert channels into TCP/IP [C] // Information Hiding. Springer Berlin Heidelberg, 2005: 247-261

[44] Mazurczyk W, Szczypiorski K. Evaluation of steganographic methods for oversized IP packets[J]. Telecommunication Systems, 2012, 49(2):207-217

[45] Sadeghi A R, Schulz S, Varadharajan V. The Silence of the LANs: Efficient Leakage Resilience for IPsec VPNs[M]// Computer Security-ESORICS 2012. Springer Berlin Heidelberg, 2012:253-270

[46] Ji L, Liang H, Song Y, et al. A normal-traffic network covert channel [C] // 2009 Computational Intelligence and Security (CIS'09). IEEE, 2009:499-503

[47] Wendzel S, Keller J. Systematic engineering of control protocols for covert channels[C]// Communications and Multimedia Security. Springer Berlin Heidelberg, 2012:131-144

[48] Postel J. RFC 792: Internet control message protocol[Z]. 1981

[49] Qu H, Su P, Feng D. A typical noisy covert channel in the IP protocol[C]// 38th Annual 2004 International Carnahan Conference on Security Technology. IEEE, 2004:189-192

[50] Lucena N B, Lewandowski G, Chapin S J. Covert channels in IPv6 [C] // Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2006:147-166

[51] Zander S, Armitage G, Branch P. An empirical evaluation of IP Time To Live covert channels [C] // 15th IEEE International Conference on Networks(ICON 2007). IEEE, 2007:42-47

[52] Krätzer C, Dittmann J, Lang A, et al. WLAN steganography: a first practical review[C]// Proceedings of the 8th Workshop on Multimedia and Security. ACM, 2006:17-22

[53] 华元彬,蒋建春,卿斯汉. 基于链路分析法的复合隐蔽通道检测[J]. 计算机应用,2006,26(1):81-83
Hua Yuan-bin, Jiang Jian-chun, Qing Si-han. Complex covert channel detection based on chain analysis methodology[J]. Computer Applications, 2006, 26(1):81-83

[54] 薛晋康,许士博. 基于流量分析的网络隐蔽通道检测模型[J]. 计算机工程,2002,28(12):46-48
Xue Jin-kang, Xu Shi-bo. A network covert channel detecting model based on traffic analysis [J]. Computer Engineering, 2002, 28(12):46-48

[55] Yuwen Q, Huaju S, Chao S, et al. Network covert channel detection with cluster based on hierarchy and density[J]. Procedia Engineering, 2012, 29:4175-4180

[56] Sohn T, Seo J T, Moon J. A study on the covert channel detection of TCP/IP header using support vector machine[M]// Information and Communications Security. Springer Berlin Heidelberg, 2003:313-324

[57] Tumoian E, Anikeev M. Detecting NUSHU covert channels using neural networks[EB/OL]. http://www.ouah.org/neural_networks_vs_NUSHU.pdf, 2005

[58] Tumoian E, Anikeev M. Network based detection of passive covert channels in TCP/IP[C]// The 30th Anniversary IEEE Conference on Local Computer Networks, 2005. IEEE, 2005: 802-809

[59] Borders K, Prakash A. Web tap: detecting covert web traffic [C] // Proceedings of the 11th ACM conferenceon Computer and communications security. ACM, 2004:110-120

[60] 章思宇,邹福泰,王鲁华,等. 基于 DNS 的隐蔽通道流量检测[J]. 通信学报,2013,34(5):143-151
Zhang Si-yu, Zou Fu-tai, Wang Lu-hua, et al. Detecting DNS-based covert channel on live traffic[J]. Journal on Communications, 2013, 34(5):143-151

[61] Team S. Snort Users Manual 2.9.5[Z]. 2013

[62] Cisco Systems, Inc. User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x[Z]. 2014

[63] Marleau G, Hebert A, Roy R. A User Guide for DRAGON Version5[Z]. 2014