基于连接标识的映射通信

刘 畅,宋 飞,孙 亮,张思东
(北京交通大学电子信息工程学院 下一代互联网互联设备国家工程实验室,北京 100044)

摘 要: 本文提出了一种基于连接标识(CID)通信的方法,并添加连接标识映射服务器(CMS)来完成对连接的管理功能.CMS 将网络的核心部分与接入部分进行了分离,通过在 CMS 中建立连接标识与 IP 之间的映射,完成了映射通信的传输方式.本文将传统网络数据发送模式由基于对端地址变为基于连接标识,从而提升网络针对连接的可控可管性.本文详细讲述了这种基于连接的映射通信带来的优势,如:提高抗 DDos 攻击、防止主机身份暴露、减少核心网路由条目等.并且分析了这种映射通信对现有应用的向下兼容性,及其可能带来的新攻击方式及应对措施.最终的实现测试给出了基于连接标识映射通信的具体性能.

关键词: 连接标识; 网络架构; 映射通信; 标识映射
中图分类号: TN915 **文献标识码:** A **文章编号:** 0372-2112 (2012) 10-1920-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.10.002

A Mapping Communication Mode Based on Connection Identify

LIU Chang, SONG Fei, SUN Liang, ZHANG Si-dong
(*National Engineering Laboratory for Next Generation Internet Interconnection Devices, School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing* 100044, *China*)

Abstract: This paper proposes to use connection identify (CID) to mark the process of obtaining a service, and add connection identify mapping server (CMS) to achieve the management of connections. CMSs make the core network and access network be separated. And through the mapping between CID and IP in the CMSs, the communication is separated to three steps. This mapping communication mode makes the sending of packets be based on CID instead of IP address. Thus, the controllability and manageability of connections have gained a remarkable increasing. Moreover, this paper has particularly represented the advantages of the mapping communication, and the compatibility of current applications. In addition, we give some countermeasures aimed at the new network attacks which the mapping communication mode may bring about. At last, the experimentation results reveal the specific performances of mapping communication mode.

Key words: Connection Identify (CID); network architecture; mapping communication; identify mapping

1 引言

现有互联网架构的原始设计理念是在固定地址条件下,提供端到端通信.在现有互联网中,发送端知道接收端的 IP 地址,向指定地址发送数据包;路由工作也是将数据包按照其指定目的地址进行转发.

由于这种简单的端到端通信方式基于通信双端的地址,因此连接的概念被弱化了.一次连接虽然对应着一次传输过程这个物理实体,但是却没有一个标识来标明这个物理实体.通常我们只能通过源端 IP、源端端口号、目的 IP、目的端口号、传输协议这样的 5 元组来区分一次连接,这使得现今的互联网欠缺对连接的管理能力,基于连接的可控、可管性很差.然而,网络服务通常都是基于连接的,通过建立连接来获取某种服务,而非基于数据包或者某端地址.这种简单的端到端通信方式,还使得通信双端的地址都暴露在网络之中,带来了严重的安全隐患.如现有的 DDos 攻击就是针对指定地址的一种常见攻击形式,其产生原因就在于端到端通信将地址暴露在网络中,并且攻击者能够向指定地址发送数据包.

现在的很多研究都是针对这些端到端通信存在的问题.有些是基于间接通信的理念对传输协议进行的研究[1~3].有些是在应用层上进行针对应用程序的研究[4,5].也有些研究是利用虚拟网络实现资源的管

收稿日期:2011-06-07;修回日期:2012-04-23
基金项目:国家 973 重点基础研究发展计划(No.2007CB307100);北京市自然科学基金重点资助(No.4091003);中央高校基本科研业务费专项资金(No.2011JBM018);国家自然科学基金(No.60903150)

理[6~8].还有些研究提出了新的网络体系架构,如 I3 提出互联网间接底层设施的概念[9].但是多数研究都没有将连接的概念提炼出来,服务获取的形式仍然是以数据包为基础,而不是以连接为基础.

在本文中新提出了连接标识(CID)的概念,用于标识一次服务的获取过程.通信方式从针对 IP 地址发包,变为了针对连接 CID 发包.这种通信方式打破了原有端到端通信的传统思路,通信不再是基于地址,而是基于连接.本文设计了新的网络架构,在核心网与接入网之间加入连接标识映射服务器(CMS)设备,将核心网与接入网进行了分离,使得通信分成了 3 个部分:接入网、核心网、接入网.CMS 中 CID 到 IP 的映射工作,将通信的 3 个部分衔接在一起,最终实现通信功能.这种基于连接的通信方式使得系统对于连接的管理能力得到了大幅度增强,也使得网络的安全性得到了提升,同时使得核心路由条目大幅度削减.

2　基于连接标识的映射通信

本文提出使用连接标识(CID)标识一次服务的获取过程.属于同一次服务获取过程的数据包,将拥有同样的 CID.网络系统可以通过 CID 来区分一次连接,并且针对连接进行管理.

为了将 CID 引入到网络之中,需要在网络中添加连接标识映射服务器(CMS),如图 1 所示.本文将网络结构划分为核心网和接入网两个部分,一定区域内的终端节点经过接入网的汇聚工作,先经由本地的 CMS,通过核心节点接入到核心网之中.CMS 的主要功能就是生成、管理 CID,以及 CID 的映射工作.

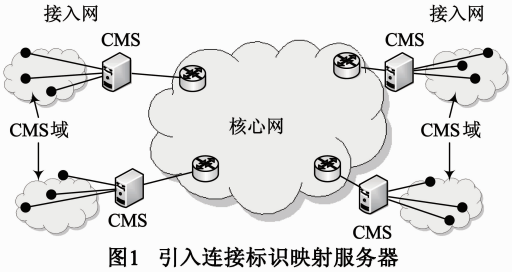

图1　引入连接标识映射服务器

首先,在连接建立之前,连接发起者的 CMS 将对终端和本次连接请求进行一系列的认证工作.连接的认证工作为网络提供了基于连接层面的安全机制.如:CMS 可以根据申请者的安全级别和其申请服务的安全级别判断认证是否通过,从而实现屏蔽指定区域的某些特定服务.

其次,在生成 CID 之后,通信双端的 CMS 将会有一个交互过程,交互内容主要包括双端可用的 CMS 地址列表.在经过交互后,CMS 将拥有通信双端的所有可用 CMS 地址列表,在此后的数据传输中,通信终端将仅仅使用 CID 和本地 CMS 地址进行通信,而非使用对端的地址.

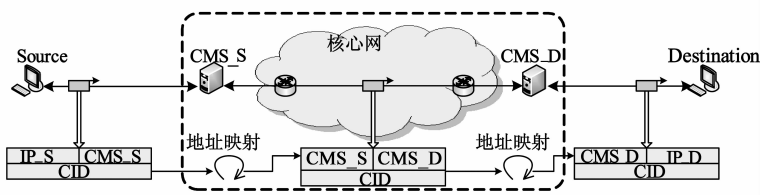

图2　映射通信

最后,在通信过程中,数据包被发送给本地 CMS,在 CMS 中将会有一次 CID 到 IP 地址的映射,从而确定数据包的目的 CMS,在通信对端 CMS 同样会做一次映射,根据 CID 将数据包转发给指定的通信终端.因此,一次通信过可以拆分成 3 个部分,如图 2 所示.第一部分是源端接入网,通信双端是源终端和源 CMS,此部分主要通过 CID 来区分不同的连接;第二部分是核心网,通信双端是源 CMS 和目的 CMS,此部分主要通过 CMS 的地址进行通信;第三部分是目的接入网,通信双端是目的 CMS 和目的终端,此部分也是主要通过 CID 来区分不同的连接.

3　连接标识的工作原理

3.1　连接标识的生成

CID 由连接发起者的 CMS 生成,根据申请的服务、申请者身份、申请时间、随机数通过生成函数最终得到,格式如图 3 所示.

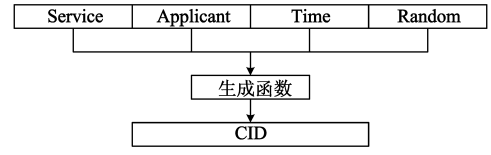

图3　连接标识的生成格式

其中,申请的服务将使用一种服务标识进行表示.申请者身份为能够标明一个申请者身份的某种标识.申请时间可以简单的理解为一个时间戳,主要用于防止 CID 冲突.随机数的引入主要也是为了防止 CID 冲突,防止攻击者使用相同身份、在同一时刻、申请相同服务从而产生的 CID 冲突攻击.

CID 生成函数要求其生成函数无法或者难以反解,同时也对冲突概率有很高的要求,因此本文选取通用 Hash 算法之一 SHA-1 作为的 CID 生成函数.

3.2　连接标识的交互

在生成 CID 之后,发起端 CMS 掌握的信息包括发起者可用 CMS 列表(由本地发起者告知)、生成的 CID、从服务查询系统(如 DNS)获得的服务提供者 CMS 地址

和 IP 地址.此时发起端 CMS 需要将这些信息告知通信对端的 CMS,并询问关于通信对端的一些信息.但是如果直接进行信息,则会将通信双端的信息完全暴露在核心网中,失去了后续通信屏蔽主机带来的安全优势.因此,CMS 之间的信息交互过程需要使用加密通信的方式.

信息交互过程如图 4 所示.CID 的生成是发生在服务发起的 A 端 CMS 中(参见 3.1 节),首先由该 CMS 将连接的相关信息①加密后发送给对端 B 的 CMS,信息包括:连接的 CID 值、申请的服务标识、发起端的所有可用 CMS 地址列表、服务提供者的 IP 地址、服务描述(一些对服务的要求).B 端 CMS 解密此交互信息后,将根据服务提供者 IP 地址和申请的服务标识,向服务提供者发送信息②询问其所有可用 CMS 地址列表.得到询问回复消息③后,B 端 CMS 将其添加到交互信息的相应位置中,加密后回复交互信息④给 A 端的 CMS.到此完成了一次 CMS 的信息交互,双方 CMS 获得了完整的连接相关信息.

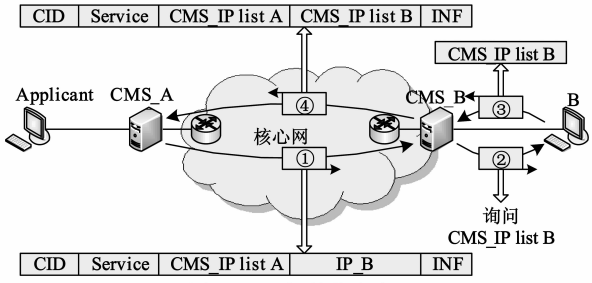

图4 CMS间的信息交互

在双方 CMS 交互连接信息完成后,还需进行一系列的信息下发工作,如图 5 所示.信息下发工作分为两个部分:向通信终端下发 CID 和向选取的 CMS 下发 CID 交互信息.两个主 CMS 需要首先向本域内此次连接的通信终端下发 CID 码,以及被选取出实际使用的 CMS 地址列表,用于通告本次连接的可用路径.此后,本次连接的两个主 CMS 还需要向被选取出的 CMS 下发连接

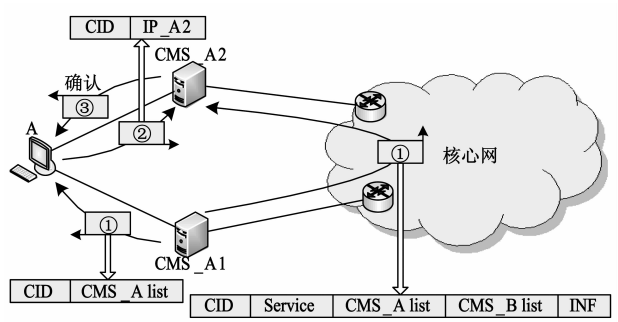

图5 CMS信息下发

相关信息,以便其完成数据传输过程中的映射工作.CMS 之间的信息下发工作同样需要使用加密传输.这两部分信息下发工作如图 5 步骤①中数据包所示.在此之后,通信终端需要确认这些 CMS 已经获得了本次连接的相关信息,终端要向本地的这些 CMS 发送确认信息②,并告知 CMS 通信终端将使用哪个 IP 地址与该 CMS 相连.CMS 收到后,将这个 IP 地址与此 CID 绑定,并回复确认消息③.

至此连接标识的信息交互过程结束.通信终端得到的为本次连接的 CID 码和本端用于建立连接的多个 CMS 地址,而用于建立连接的所有 CMS 也都得到了本次连接的完整信息.

3.3 连接标识的映射

图 6 所示的为源和目的端各自通过 2 个不同的 CMS 域,建立连接进行数据通信.为了兼容通信终端的多宿特性,因此允许终端使用不同地址通过不同的 CMS 域接入网络.

在图 6 中的接入网部分,是由终端和本地 CMS 进行数据传输,数据包的源和目的地址分别填的是终端地址和本地 CMS 地址,在 CMS 中则是通过 CID 码来区分这些数据包,对应着图 2 映射通信中的第一三部分.这种传输方式使得在接入网中完全的屏蔽了对端的身份信息,提高了通信的隐私性,同时由于目的地址只能为本地的 CMS 而避免了对域外的攻击行为.

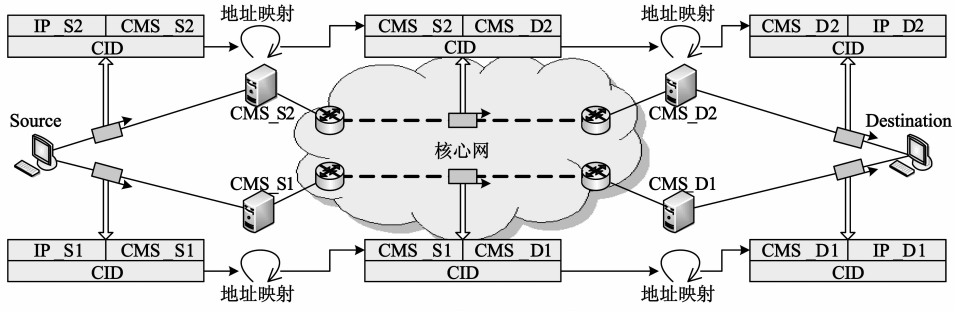

图6 CMS中CID的映射

数据包在 CMS 中将发生一次映射,根据 CID 码查找对应的 CMS 地址配对已经对端的地址,如图 6 中 CMS 的映射.在数据包进入核心网时发生一次映射,数据包的源和目的地址被替换为通信双端的 CMS 地址,

而非真正的终端地址.在数据包出核心网时再次发生映射,数据包的源和目的地址被替换为终端的 CMS 地址和终端地址,从而使得数据包成功的到底目的终端.这两次 CMS 中的映射使得网络能够针对连接进行管理,只要在 CMS 中禁止掉某个 CID 的映射,就等于切断了该连接,并且 CMS 也能够限制每台终端建立的最大连接数量.

在图 6 中的核心网部分,是由双端的 CMS 进行数据传输,数据包的源和目的地址分别填的是发送端和接收端的 CMS 地址,在 CMS 中则是依然通过 CID 码来区分这些数据包,对应着图 2 映射通信中的第二部分.这种传输方式使得在核心网中完全的屏蔽了通信双端的身份信息,并且使得核心网中路由完全变为了从 CMS 到 CMS,大幅度的减少了核心网路由条目.

4　连接标识的作用

4.1　标识一次服务获取过程

本文将连接标识(CID)定义为标识一次服务的获取过程,而非一种实际的物理连接.本文认为建立连接的根本目的是为了获取某种服务,因此连接不应该简单的被理解成多个网络节点的某种物理串联,而应该为一个逻辑连接的概念.

4.2　管理连接

如 3.3 节中提到的,CMS 拥有针对连接的管理功能.由于数据通信过程中,需要在 CMS 中生成 CID 并要根据 CID 发生映射,因此可以在 CMS 中进行基于 CID 的连接管理工作.

利用 CMS 实现切断指定连接非常简单,仅仅需要取消这次连接有关 CID 的映射条目,该连接的数据则无法在 CMS 完成映射,从而连接被切断.

利用 CMS 实现控制单个终端的连接数量也非常简单,由于 CID 的生成是在 CMS 中进行的,因此只要限制单个终端生成 CID 的数量,就可以控制其连接的数量.

4.3　减少网络攻击

如图 2 映射通信中所示,数据包在发送过程中,目的地址只能填写为本地 CMS 地址.因此攻击者的攻击目标受到了极大的限制,任何目标地址为域外地址的数据包,都无法进入核心网,针对域外的主动攻击(如 DDos 攻击)被大幅度减少.

没有填写 CID 或者 CID 非法的数据包同样会被 CMS 丢弃,这迫使攻击点必须得到一个合法的 CID,这大幅度的提高了攻击的复杂程度,简单的僵尸网络将难以完成这种复杂操作.并且在发现攻击后,只需通过取消 CID 映射关系的方式就能终止攻击.

在 CMS 中存储的连接信息是同时包括 CID 和相应终端 IP 地址的,也就意味着即使 CID 被窃听到后,攻击者还必须要成功的伪装成终端的 IP 地址,才能够有效的使用这个合法的 CID,否则 IP 地址与 CID 对应错误的数据包同样会被 CMS 丢弃,这也使得攻击的难度大幅度提升.

CMS 域内的攻击仍然是存在的,攻击者可以通过避开 CMS 的方式,直接对域内终端发起攻击,这种攻击 CMS 并没有办法阻止.但是终端可以通过仅接收 CMS 数据包的形式,快速过滤掉域内其他节点对其发送的数据包,从而避免攻击.

4.4　CMS 攻击

由于 CMS 成为了接入核心网络的必经设备,也是 CID 生成、映射的核心,同时 CMS 的地址还被所有的域内终端所知,因此 CMS 不可避免的成为了新的攻击目标.虽然 CMS 能够根据非法 CID 屏蔽掉很多形式的攻击,但是大量的 CID 生成请求或是仅仅的大量非法数包,同样会使 CMS 发生异常.这种依靠数据量的攻击形式是不可避免的,现有的网络中同样存在(如 DDos 攻击),并且难以避免.

但是本文提出的网络结构(如图 1,图 2),攻击者只能攻击本域 CMS,目标地址在域外的数据包都会被本域 CMS 丢弃.因此,如果攻击者操纵的僵尸网络较为分散,则无法集中攻击目标,只能攻击各自域内的 CMS,形成不了规模性的攻击;而如果攻击者操纵的僵尸网络较为集中,则是只能攻击僵尸网络所在域内的 CMS,使僵尸网络本域内部瘫痪.

由于 CMS 是处在核心网络的外层,CMS 发生异常仅仅带来的是域内瘫痪,对核心网和其他 CMS 域没有影响,因此这种分层方式使得核心网更加稳定,不会轻易受到攻击.

4.5　屏蔽主机

在图 2 中可以看到,如果从接入网部分截获数据包,能够得到的信息是:连接的 CID 码、本域通信终端地址和本域 CMS 地址,窃听者并不能够获取通信对端的信息,即不知道该点在与谁通信.而如果从核心网部分截获数据包,能够得到的信息是:连接的 CID 码和通信双端的 CMS 地址,窃听者不能获取任何通信终端的信息.

因此,这种映射通信实现了在接入网屏蔽对端主机,而在核心网屏蔽双端主机的功能,大大的提升了通信者的隐私性.

4.6　减少核心网路由条目

从图 2、图 6 中可以看到,在核心网传输的数据包,源和目的地址都为 CMS 的地址,而非终端主机的地址.因此核心路由器仅仅需要保存关于 CMS 的路由条目,这将大幅度削减路由条目的数量,为当前路由条目极

具膨胀的问题提供了良好的解决方案.

4.7 广播和组播的实现

图 7 所示为在本文提出的网络架构中,现有网络中广播和组播应用的实现方式.对于广播和组播服务,将服务提供者认为是该连接的发起者,由提供者域内的 CMS_S 为本次服务生成 CID,并在服务描述信息中注明为广播.服务获取者经过认证,通过 CMS 协商的方式,将自己域内的 CMS_C 地址添加到此广播 CID 对应的接收者 CMS_C 列表中,如 CMS_C1、CMS_C2、CMS_C3.

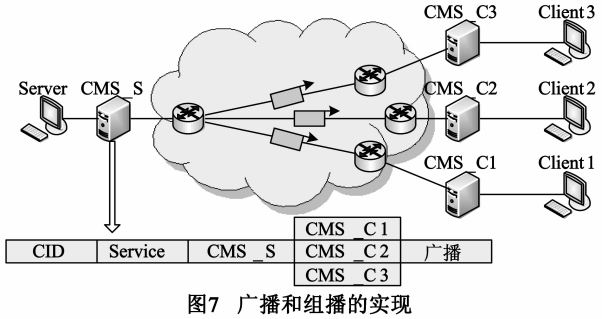

图7 广播和组播的实现

广播发送的数据包和普通数据包一样,被发送给本地的 CMS_S.但是在 CMS_S 内部,会根据服务描述中填写的广播信息,将数据包复制,分别发送给 CMS_C 列表中的每个 CMS_C,最终再由 CMS_C 转给服务获取者,从而实现了广播和组播服务.

4.8 P2P 的实现

图 8 所示为在本文提出的网络架构中,现有网络中 P2P 应用的实现方式.对于 P2P 应用,本文设计采用接收端主动索要指定数据包的形式完成传输.P2P 的接收端被认为是连接发起者,由域内的 CMS_C 为本次服务生成 CID,并在服务描述信息中注明为 P2P.CMS_C 需要维护一个服务器 CMS_S 地址列表,能够提供该服务的服务器将把他们的 CMS_S 地址经过认证添加到 CMS_S 地址列表中,如 CMS_S1、CMS_S2、CMS_S3.

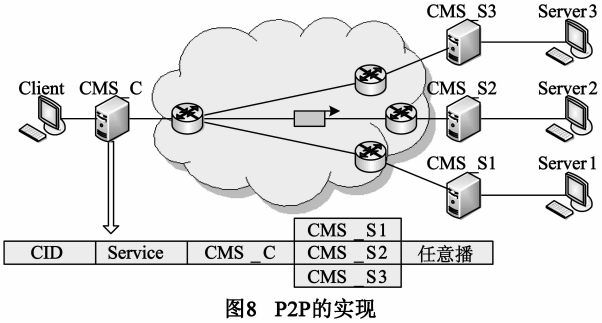

图8 P2P的实现

和普通数据包一样,接收端将索要包发送给本地的 CMS_C,其会根据服务描述中填写的 P2P 信息,采用任意播的方式,将索要包送给 CMS_S 列表中的某一个 CMS_S,再由 CMS_S 转给服务器,服务器则根据该索要包给接收端发送数据,从而实现了 P2P 服务.

4.9 CID 冲突

由于每个域拥有一个 CMS,它们分别管理域内的 CID 信息,而不是统一生成管理 CID 信息,因此存在一定可能性在域间发生 CID 的冲突.而 CMS 通过 CID 区分不同的连接,若存在相同的 CID 码,则会导致 CMS 无法区分这两个连接,出现通信错误.

首先,由于核心路由器是按照 CMS 地址进行路由的,而并不是按照 CID 码,因此域外存在相同的 CID 并不会影响到全网的正常通信.发生域内 CID 冲突可能有两种原因:通信对端 CMS 生成的 CID 在本域内已存在;服务迁移将相同的 CID 迁移进入本域内.对于第一种情况,只需要求对方重新生成 CID 就可以解决.由于连接还处在协商的状态并没有完全建立,重新生成 CID 并不会导致传输的异常,只是增加了建立连接的耗时.对于第二种情况,只能依靠拒绝本次服务迁移来处理.

其次,CID 的冲突概率非常低.由于本文定义的 CID 为一个经过 Hash 的 160 位码,理论上讲 CID 冲突概率约为 2^{-80}(小于 10^{-24}).这样低的冲突概率,在单个 CMS 域中是可以忽略不计的.

5 映射通信性能测试

基于连接标识映射通信的实现工作是在一体化标识网络中进行的.该体系中使用服务标识(SID)标注一个具体服务,使用接入标识(AID)标注一个接入地址,本文提出的连接标识(CID)用于标注一次服务的获取过程.在初步实现的原型系统中,本文对基于连接标识的映射通信进行了主要性能的测试工作.

5.1 新增 CID 延时测试

在连接建立过程中,CMS 在接收到新 CID 的信息交互包后,需要首先在本地 CID 列表中进行比对,如果确认没有该 CID 的相关信息,则可以将其添加到本地 CID 列表之中.此新增 CID 过程的耗时,取决于本地已有 CID 列表的长度.图 9 所示为新增 CID 延时随 CID 列表长度的变化.分析图 9 可知,添加延时和 CID 数量基本呈线性关系;且绝大部分(约 90%,图下侧稠密区域)分布较为稳定,但有小量可能性(约 10%,图中上侧散点区域)会出现延时较大的情况.

5.2 数据包映射延时测试

在数据通信过程中,每个数据包会根据其所属的 CID,在 CMS 中发生一次映射,替换源目的地址,CID 映射的耗时也将取决于本地已有 CID 列表的长度.图 10 所示为数据包根据其 CID 在 CMS 中发生映射的延时.分析图 10 可知,映射延时和 CID 数量基本也呈线性关系;相同数量 CID 条件下,映射延时基本呈现均匀分布

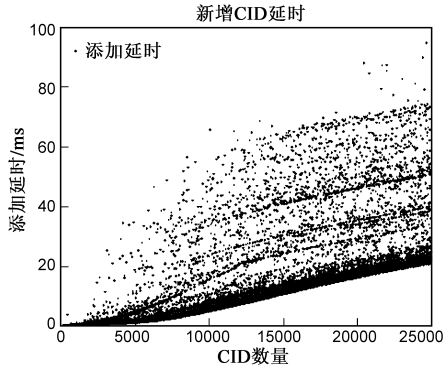

图9　新增CID延时测试结果

(对于相同横坐标,除个别点以外,数据点纵向较为均匀的分布于上下限之间),其说明映射延时主要取决于该 CID 在列表中的位置;有极少数情况(小于 1%)会出现较大延时的情况.

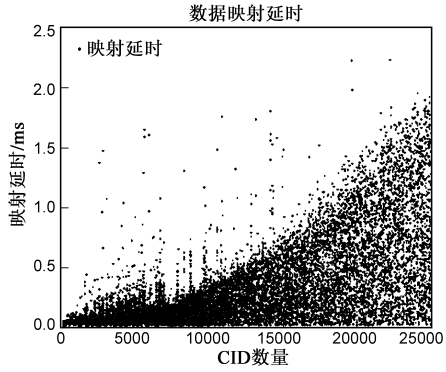

图10　数据包映射延时测试结果

5.3　攻击包丢弃延时测试

CMS 能够根据数据包中的 CID 信息,确定是否该转发该数据包,从而在核心网之前屏蔽 CID 错误的攻击数据.图 11 所示为判断数据包 CID 信息错误并丢弃该包的耗时.

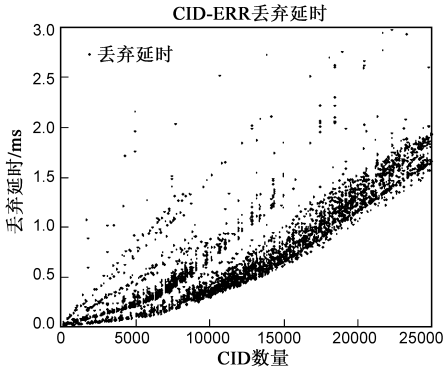

图11　攻击包丢弃延时测试结果

测试过程中,100% 的攻击包都被 CMS 丢弃,没有攻击包进入核心网络.而相比之下,在传统的互联网中是很难在网络中屏蔽这些攻击包的.

5.4　删除 CID 延时测试

在连接传输完成后,CMS 将会收到 CID 删除信息包,将指定 CID 从 CID 映射列表之中删除.图 12 所示为删除 CID 延时随 CID 列表长度的变化.分析图 12 可知,删除延时和 CID 数量呈线性关系;相同数量 CID 条件下,删除延时基本呈现均匀分布(对于相同横坐标,数据点纵向较为均匀的分布于上下限之间),其说明删除延时主要取决于该 CID 在列表中的位置.

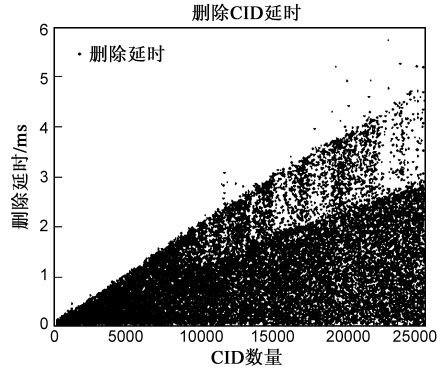

图12　删除CID延时测试结果

5.5　CID 冲突概率测试

若在 CMS 中存在相同的 CID 条目,将会导致该 CID 数据包不能正确映射的错误.本部分主要测试 CID 码的长度对冲突概率的影响.表 1 所示为不同长度的 CID 码对应的冲突概率测试.根据 Hash 函数的特性,即使生成过程中使用相同的服务标识和身份标识,最终生成 CID 的冲突概率也是基本相同的,其冲突仅取决于 CID 码的最终长度.分析表 1 可知,在 CID 码达到 64 位时,其冲突概率已小于 10^{-8},因此选择使用 160 位的 CID 码,完全可以不考虑其发生 CID 冲突.

表 1　CID 冲突测试结果

位数	160 位	128 位	64 位	32 位
算法	SHA-1	MD5	CRC64	CRC32
理论概率	2^{-80} 8×10^{-25}	2^{-64} 5×10^{-20}	2^{-32} 2.3×10^{-10}	2^{-16} 1.5×10^{-5}
测试概率	10^8 无冲突	10^8 无冲突	10^8 无冲突	1.3×10^{-4}

6　结论

本文提出使用连接标识来标志一次服务的获取过程,这使得通信过程变为了基于连接,从而大幅度提升了网络针对连接的可控、可管性.本文利用连接标识将通信分为了三个步骤,实现了接入网屏蔽对端主机,核心网屏蔽双端主机的功能,使得核心网路由条目得到了大幅度削减,也同时为网络提供了更好的安全性能.

映射通信对广播、P2P 等现有应用也具备兼容性,并且使得终端的实现更加简单.针对新网络结构可能带来的新攻击方式,文章也给出了相应的分析和应对措施.

参考文献

[1] S E Terry, A Chandra. Method and System for Implementing H-ARQ-Assisted ARQ Operation [P]. US: US20070168826, 2007-07-19.

[2] X J Tang, R H Liu, P Spasojevic, H V Poor. On the throughput of secure hybrid-ARQ protocols for gaussian block-fading channels [J]. IEEE Transactions on Information Theory, 2009, 55(4): 1575 – 1591.

[3] E Exposito, C Chassot, M Diaz. New generation of transport protocols for autonomous systems [A]. IEEE GLOBECOM Workshops (GC Wkshps) [C]. USA: IEEE Press, 2010. 1617 – 1621.

[4] Y H Chu, S G Rao, S Seshan, H Zhang. A case for end system multicast [J]. Selected Areas in Communications, 2002, 20(8): 1456 – 1471.

[5] J Jannotti, D K Gifford, K L Johnson, M F Kaashoek. Overcast: Reliable multicasting with an overlay network [A]. Proceedings of OSDI [C]. USA, 2000. 197 – 212.

[6] A T Campbell, J Vicente, D A Villela. Virtuosity: Performing virtual network resource management [A]. Seventh International Workshop on Quality of Service [C]. USA: IEEE Press, 1999. 65 – 76.

[7] C C Marquezan, J C Nobre, L Z Granville, G Nunzi, D Dudkowski, M Brunner. Distributed reallocation scheme for virtual network resources [A]. IEEE International Conference on Communications [C]. USA: IEEE Press, 2009. 1 – 5.

[8] B Agrawal, T Sherwood. High-bandwidth network memory system through virtual pipelines [J]. Networking, 2009, 17(4): 1029 – 1041.

[9] I Stoica, D Adkins, S Zhuang, S Shenker, S Surana. Internet indirection infrastructure [J]. Networking, 2004, 12(2): 205 – 218.

[10] 张宏科,苏伟.新网络体系基础研究——一体化网络与普适服务 [J].电子学报,2007,35(4):593 – 598.
ZHANG Hong-ke, SU We. Fundamental research on the architecture of new network——universal network and pervasive service [J]. Acta Electronica Sinica, 2007, 35(4): 593 – 598. (in Chinese)

[11] 杨冬,周华春,张宏科.基于一体化网络的普适服务研究 [J].电子学报,2007,35(4):607 – 613.
Research on pervasive services based on universal network [J]. Acta Electronica Sinica, 2007, 35(4): 607 – 613. (in Chinese)

作者简介

刘 畅 男,1986 年 5 月出生于北京,北京交通大学电子信息工程学院博士研究生,主要研究方向为下一代互联网体系架构.
E-mail: deathsmile522@gmail.com

宋 飞 男,1983 年 4 月出生于河北,博士,讲师,硕士生导师.主要研究方向为下一代互联网体系架构、网络协议分析与优化.
E-mail: fsong@bjtu.edu.cn