面向未来互联网的基于Capabilities的DDoS防御体系研究

张洪豪 王劲松 黄 玮 赵祥麟
(天津理工大学计算机视觉与系统教育部重点实验室 天津 300384)

摘 要 介绍了面向未来互联网的防御DDoS攻击的Capabilities机制的原理及其关键技术,阐述了当前基于Capabilities机制的几个典型方案。研究了基于Capabilities机制的DDoS防御体系的全局框架,并探讨了该框架所包含的流分类、执行、Capabilities管理这3部分在未来互联网中可行的实现方案。建立了Capabilities机制框架下的流量模型,从理论上分析并论证了Capabilities机制框架下的安全性与效率等问题。通过仿真实验,比较了在不同场景下各种Capabilities方案的性能及效率。

关键词 网络安全,分布式拒绝服务攻击,Capabilities机制,未来互联网
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.07.044

Capabilities-based DDoS Defense Architecture for Future Internet

ZHANG Hong-hao WANG Jin-song HUANG Wei ZHAO Xiang-lin
(Key Laboratory of Computer Vision and System, Ministry of Education, Tianjin University of Technology, Tianjin 300384, China)

Abstract Firstly, this paper introduced the theory and key technologies of Capabilities mechanism for future Internet and expounded and compared the typical programs based on Capabilities mechanism about their performance and reliability by simulation experiment in dissimilar scenarios. Secondly, we researched on the DDoS defense architecture based on capabilities mechanism, and discussed the viable implementation of the three parts (the flow classification, enforcement, Capabilities management) contained in the architecture in future network. Furthermore, we designed a simple traffic modeling under the Capabilities framework and analyzed the security and efficiency of the Capabilities framework theoretically. Finally, the paper analyzed the shortcomings and inadequacies of several solutions based on Capabilities mechanism and compared their performance and efficiency of in different scenarios through simulation experiments

Keywords Network security, DDoS, Capabilities mechanism, Future internet

1 引言

随着互联网的迅速发展,网络攻击也层出不穷,其中拒绝服务攻击(Denial of Service, DoS)尤其是分布式拒绝服务攻击(Distributed Denial of Service, DDoS)已成为最严重的威胁之一。2013年2月,Arbor网络公司发布的调查报告显示DDoS攻击的规模连续3年突破60Gbps[1]。一般来说,网络攻击根据产生的后果可分为两类:一类是通过非法入侵受害者系统,对受害者的软硬件进行破坏,使其不能正常工作,或者盗取受害者的重要信息(如:账号或密码等);另一类是通过大量消耗受害者的资源(如:内存、存储处理能力、带宽等)使其无法正常工作。DDoS攻击则通常是将这两种攻击结合起来,先通过非法入侵大量其他主机达到控制这些主机的目的,再利用这些受控主机组成"僵尸网络"对受害机进行资源消耗型攻击。这种攻击由于不需要进行源地址欺骗,只需通过控制僵尸网络中的真实主机向受害机或其所在的瓶颈链路发送少量的数据包就能达到攻击目的,而且每一台主机发送的数据流量和正常合法流量没有明显区别,因此容易躲避DDoS防御系统的检测。互联网设计之初主要考虑可达性,而对安全性考虑得较少。根据美国计算机应急和响应中心(U. S. Computer Emergency Readiness and Response Center)的报告,现阶段只有修改TCP/IP内核才能从根本上解决DDoS攻击问题。鉴于此,研究者提出了以安全性为首要目标的下一代安全互联网(Next Generation Secure Internet, NGSI)架构[2]。在此架构下,华盛顿大学的Anderson提出的防御DDoS攻击的网络Capabilities机制很可能被未来互联网所采纳[3]。本文主要针对面向未来互联网的基于Capabilities机制的DDoS防御体系进行研究。Capabilities机制属于基于"白名单"的DDoS攻击缓解方案,不同于传统的类似于打补丁的增量式改进,它需要改变当前互联网条件下终端主机彼此进行通信的方式(由当前互联网default-on模式转变为default-off模式)。在默认状态下某一台主机到其他任何主机都是不可达的,即某台主机不能直接向另一台主机发送数据,发送者必须首先获得接收端所授予的发送信息的权限。另

到稿日期:2013-09-16 返修日期:2014-01-18 本文受国家自然科学基金(60904063,61301140),天津市教委科技项目(20120703)资助。
张洪豪(1984—),男,硕士,工程师,CCF会员,主要研究领域为未来互联网、网络安全,E-mail:zhanghonghao@tjut.edu.cn;王劲松(1970—),男,博士,研究员,主要研究领域为网络安全、网络管理;黄 玮(1981—),男,博士,副教授,主要研究领域为复杂网络、信息安全等;赵祥麟(1992—),男,主要研究领域为计算机网络等。

外，Capabilities 机制具有良好的激励作用，并产生了一个“滚雪球”式的效应：随着越来越多的终端系统和自治系统部署了该机制，已经部署的终端或 AS 能够更好地预防 DDoS 洪泛攻击，这促使越来越多的系统部署该机制。因而 Capabilities 方案对于日益重视安全性的未来互联网显得十分重要。

2 Capabilities 机制及其典型方案

2.1 Capabilities 机制的原理

Capabilities 机制的主要原理是：发送者先与目标主机建立连接以获得授权。发送者先发送 Capabilities 请求包，沿路各路由器在包中依序插入各自的特征标记，目标主机收到后，如果允许该发送者继续向其发送数据，则将完整的标记序列（即 Capabilities）回传给发送者。发送者随后将该 Capabilities 植入将要发送的后续数据包中，以接受沿路各个路由器核查并优先通过，如图 1 所示。

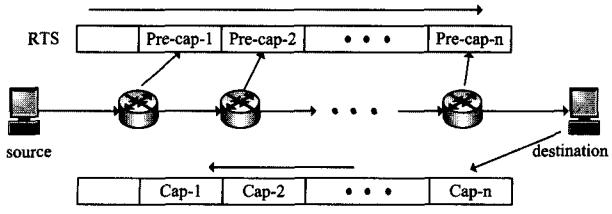


图 1 Capabilities 获取的过程

Capabilities 机制所压成的 Capabilities 应当具备以下特征：Capabilities 必须由接收者授予、Capabilities 不可伪造、时效性（Capabilities 机制采取非永久有效的策略，根据链路传输状态阶段性地更新输入密钥，要求发送方阶段性申请更新 Capabilities，尽管可能会影响数据传输效率，但从安全性上讲是必须的）、不可欺骗性以及高效性（即 Capabilities 不能给网络造成太大的负担）等。相对于其他策略中描述表身份的信息，Capabilities 具有更大的优势，它不需要复杂的推理、计算，攻击者不能伪造，并且不受端到端编码的限制。

2.2 基于 Capabilities 机制的防御 DDoS 攻击的典型方案

SIFF[4] 是 Capabilities 机制的首个方案，接收者通过数据包的控制策略来重新设计防御 DDoS 洪泛攻击的系统。它将所有的互联网流分成有特权的和没有特权的两类，客户端在其发往服务器的数据包中添加 Capabilities。沿路的每一个路由器对 Capabilities 进行验证，并给予通过验证的特权数据包更高的优先级。TVA 架构[5] 通过修改 TCP/IP 协议，在 IP 层和 TCP 层之间插入一个中间层来存放 Capabilities 信息。在整个通信过程中，先建立发送者和接收者之间的授权连接，然后进行正常数据传输。该过程包括两种数据包：Capabilities 请求（Request To Send，RTS）包和 Capabilities 授权数据包。它将计算与处理 Capabilities 所需要的状态进行绑定，并实现增量部署，有效减少了路由器处理 Capabilities 所需保存的状态。Capabilities 中包含接收者授予的有效期 T 和通信量上限 N，以及沿路路由器在 RTS 包中插入的 Pre-Capabilities 信息。之后，发送者即可发送含有 Capabilities 的授权数据包，沿路的各路由器将检查到达的授权包是否同时满足授权、限时和限量等要求。

与此同时，TVA 方案同时也引入了一种新的攻击即拒绝 Capabilities 攻击（Denial of Capabilities，DoC）[6]，攻击者通过发送大量的 Capabilities 请求包来洪泛请求通道（仅占 5%带宽），使得合法用户与攻击者共同竞争请求通道，由于路由器无法鉴别数据包的合法好坏，只能按比例进行包丢失，在攻击者大量发送数据包的情况下，合法新用户将需要较长的时间才能得到授权。Walfish 等提出用 speak-up 方案来防御 DoC 攻击[7]，其基本思想是：当链路发生拥塞时，合法用户通过提高数据包的发送速率，接收方通过数据包流量大小来给予相应的优先权。然而，这种方案用在 DoC 攻击防御中无疑会对网络造成严重的负担。Parno 提出了基于猜谜机制的 Portcullis 方案来应对 DoC 攻击[8]，其基本思想是：用户在获得服务器的服务前必须先求解谜题，求解的过程中所耗费的资源由某个难度系数来决定。用户必须在一定的时间内提交正确的答案，否则将终止其服务请求，服务器端一旦验证了答案的正确性，就根据其难度系数为客户端提供相应优先级的服务。采用 Portcullis 方案能够将工作负担转嫁至发送者，确保了在请求包泛滥的情况下，合法用户能经过有限次数尝试或在一定时间内获得 Capabilities，避免了合法用户长时间无法获取 Capabilities 的局面，提高了 Capabilities 机制的安全性和健壮性。但是，采用此法对于当今繁忙的服务器或者手持式移动硬件设备来说需要消耗大量的计算资源，因此该方案存在一定的瓶颈。TVA+是在 TVA 的基础上采用 StopIt 方案[9] 中用于防止源地址欺骗的发送端鉴别体系，并在请求通道中采用分级排队机制（先基于 source-AS 再基于 source-IP 地址）来缓解请求包的洪泛攻击，当接收者将 Capabilities 授予攻击流量（相勾结串通的情形）时，使用基于接收者的公平排队策略来缓解授权包的泛洪攻击。此外，NetFence[10] 的核心是安全的拥塞控制反馈机制，确保在网络内部对流量进行拥塞控制。NetFence 将反馈信息与控制策略放在网络内部或者网络与终端系统之间的可信边界区域而不是任何终端系统。

3 Capabilities 机制的框架研究

对于防御 DDoS 攻击的 Capabilities 机制，尽管到目前为止已经提出了一些重要的解决方案，但就 Capabilities 机制而言缺乏一个基础性的框架。因而有必要从全局的角度定义 Capabilities 机制的框架，这有助于安全的未来互联网的构建。Capabilities 机制框架的依据主要应该考虑以下几个方面：接收者所需要的 Capabilities 类型、Capabilities 传输策略、网络中 Capabilities 机制的执行策略、接收端与网络的其他部分之间的通信以及 Capabilities 的交换、更新等。图 2 是构建的基于 Capabilities 机制的 DDoS 防御体系的示意图，该框架包括 3 个重要组成部分：流量分类、执行策略以及 Capabilities 的管理。值得指出的是，由于没有哪一种设计适用于所有的情况，毕竟策略和业务需求各不相同，因此在阐述其具体实现时只是给出一些可选的方案，而不是“唯一正确的”答案。

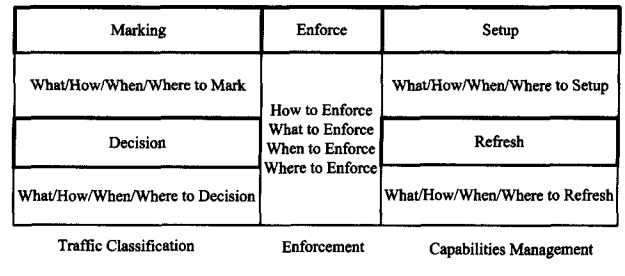


图 2 基于 Capabilities 的 DDoS 防御框架示意图

3.1 流量的分类

不同的架构尽管可以选择不同的组织形式，但应该包括3个最基本的流类：想要的、不想要的、未进行分类处理的。Capabilities架构需要区分想要的和不想要的数据流，但有时候接收者没有足够的信息来进行分类（如：来自于新客户的数据包或者不是DDoS攻击时，这两种情况下接收者不必对该数据流进行分类）。进行流量分类时，首先需要确立进行分类的决策者（Decider）的位置。一般来说，接收端主机（Destination Host）是比较好的选择，因为它拥有的资源信息较多，并且其可以实施的策略也较多。然而，若采用接收端主机来安装进行流量分类的组件，则只使得一台主机受益。若将Decider安装在接收者所在自治系统的边界路由器（DBR，Destination Border Router）上，那么处于该DBR下游的主机都将受益。此外，由于DBR较终端主机拥有更多的中间网络信息（如：瓶颈链路的状态等），使得Decider在进行流量分类时会更加准确。另外，决策过程对资源的消耗与到达决策者或者由决策者转发出去的流量数目成正比。DBR由于要向多个接收者转发流量，因此较单个接收者会消耗更多的资源。

如何进行决策呢？主要有3种途径：(1)完全基于本地化的策略；(2)基于分布式实体的协作策略；(3)基于全局策略的第三方系统。对于基于本地化的系统，决策者可能为用户保存有一个声誉值或者是不良用户的黑名单列表。对于基于分布式实体的协作策略，需要结合内部和外部节点甚至其他决策者的信息来进行决策。然而，对于分布式网络的不同节点，由于其侧重点不同，需要解决各部分的可靠性、安全性、一致性等问题；对于基于全局策略的第三方系统，决策者可能倚赖于某个全局的系统进行决策，如：一个全局的信誉系统或者全局的不良行为的黑名单列表等。

何时进行决策呢？通常情况下，可以根据情况将决策时机分为3种状态：(1)总是，随时待命状态；(2)当受到攻击时；(3)需要做出决策时。很明显，后两种方式在未遭受持续攻击的情形下能够有效地减少开销，但同时也会引入新的挑战（如：决策者对攻击的反应迟缓等问题）。关于数据包标记方面，同样需要研究标记的位置、时机以及标记的方法等问题。由于标记越靠近接收端，执行策略时有效性会越低，因此标记时一般遵守“标记应该离发送者越近越好”的原则。此外，与标记位置的确定相关联的一个很重要因素是激励机制，即：为什么要进行标记？或者标记能给自身带来什么好处？由于“谁标记谁受益”，因此发送者很乐意做这件事情。在所有现存的Capabilities方案中在处理数据包标记问题时基本上都采取了在“Source”进行标记的办法。

3.2 Capabilities的执行策略

由于在3.1节研究标记策略时所针对的对象是数据包，为了保证一致性，实施执行策略的对象也应该是数据包。下面主要探讨“执行者”如何根据数据包中所携带的Capabilities来实施转发策略。类似于3.1节中的决策过程，在实施执行阶段首先要确立实施的位置。同样地，执行者离发送端越近越好，但不可能是“Destination Host”，因为尽早地移除不想要的流量可以避免其占用网络资源，尤其是宝贵的瓶颈链路的资源。基于该思想，建议将执行者放置在发送端的边界路由器（SBR，Source Border Router）中，而不考虑在DBR或目的端主机中。接着需要解决如何执行的问题？通常可以实施以下3种方式：(1)丢弃数据包；(2)转发数据包；(3)将数据包进行降级处理。执行者首先对数据包中所携带的Capabilities进行校验，验证通过则给予转发，否则直接进行丢弃或者速率限制处理。

3.3 Capabilities的管理

如图2所示，关于Capabilities的管理可以从两个方面进行讨论，即Capabilities的安装和Capabilities的更新。

(I)Capabilities的安装。Capabilities的类型一般来说有两种，一种是限时，另一种是限量。前者即指拥有该Capabilities的有效期限（T），后者指的是使用该Capabilities允许发送的数据包的数量（N）。这两个参数的设置十分重要，若T值设置得太大，一旦Capabilities被窃取或者合法用户转变为非法用户，其产生的危害甚大，若设置得过小，经常地更新势必会增加资源的开销。同理，N值的设定亦是如此。在现有的方案中，有的方案中只使用了其中的一种Capabilities，如SIFF方案；有的方案则兼具两种类型，如TVA架构。那么怎样进行Capabilities的安装呢？一般有两种方案：一种是类似于三次握手原理，如2.1节所阐述的那样按照“申请=>判定=>授予”的程序进行安装；而另一种则是借助第三方（如DNS）定期地向发送端发送Capabilities，而且采用此法不用担心像上一种方法那样遭受DoC攻击。

(II)Capabilities的更新机制。首先明确为什么Capabilities需要更新机制？主要基于以下原因：(1)决策过程本身不是静态的，而是随着时间不断变化。譬如：由于路径的改变导致标记者或者执行者发生变化，为了适应这种变化，Capabilities必须进行更新。(2)某个发送端者原先是合法用户，但是它后来变成了恶意的攻击者，很显然，这时决策需要发生改变。那么，如何进行更新呢？一般可以遵循“行为良好的用户拥有更大的N和T值”的原则。至于具体是增加抑或减少的策略，需要权衡效率、公平、可扩展等因素，这方面的内容在第4节重点阐述。

4 Capabilities机制下流量控制机制与效率研究

Capabilities机制的流量控制方案采用了和式增加积式减少（AIMD，Additive Increase Multiplicative Decrease）算法[11]，为了解释方便，图3示出了简化了的流量模型。

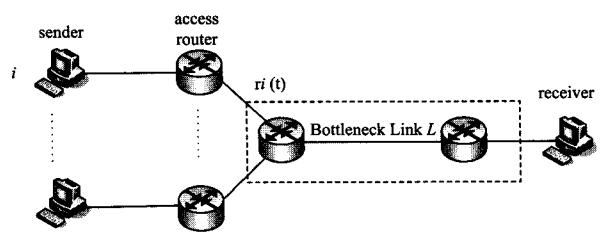


图3 Capabilities机制框架下简单的流模型

假设某条链路由K个同步流共享，所有的流具有相同的RTT值（T）。对于任意数据流i，使用以下规则来更新其发送速率：

$$\mathrm{AI}: x_i(t+T)=x_i(t)+\alpha$$

$$\mathrm{MD}: x_i(t+\varphi)=x_i(t)\cdot\beta$$

其中，$\alpha>0$，$\beta\in(0,1)$，$\varphi>0$ 且 $\varphi\to 0$。

当链路未被充分利用时，流量更新会一直实施 AI，总的速率将会增加，直到某一时刻链路过载而实施 MD 操作，导致总速率下降，链路利用不充分。这是因为：

$$\sum_i x_i(t+T)=\sum_i x_i(t)+KT>\sum_i x_i(t)$$

$$\sum_i x_i(t+\varphi)=\sum_i[x_i(t)\cdot\beta]=\beta\cdot\sum_i x_i(t)<\sum_i x_i(t)$$

这样，总流量将围绕在链路被充分利用的附近进行震荡。而当 $\alpha\to 0$ 且 $\beta\to 1$ 时，可获得效率收敛。为简便起见，不考虑时延（即发送者任何速率的改变都将对瓶颈链路产生影响）。下面给出几个重要定义和定理及其相关论证。

定义 1 对于任意主机 i，假设 $r_i^i(t)$ 为主机 i 在时刻 t 的发送速率，$r_i^a(t)$ 为接入路由器在某一段控制期间 $[t_0,t_0+\Delta t)$ 所允许的最大速率限制。在接入路由器的输出链路上，针对主机 i 的输出速率 $r_i(t)=\min(r_i^i(t),r_i^a)$。

定义 2 若某台主机能够尽力而为地最大限度地进行数据发送，且不会受到稳健的速率控制算法的处罚，该主机可认定为拥有了“充分需求”。

定义 3 在任意一个控制期间 Δt，对于给定的某个速率限制 r_i^a，速率限制利用率记为 $u_i=\bar{r}_i/r_i^a$，其中 $\bar{r}_i$ 为出口速率的平均值，且 $\bar{r}_i=\frac{1}{\Delta t}\int_{t_0}^{t_0+\Delta t} r_i(t)\mathrm{d}t$。

由于

$$\bar{r}_i=\frac{1}{\Delta t}\int_{t_0}^{t_0+\Delta t} r_i(t)\mathrm{d}t\leqslant\frac{1}{\Delta t}\int_{t_0}^{t_0+\Delta t} r_i^a\,\mathrm{d}t$$

$$=\frac{1}{\Delta t}[(t_0+\Delta t)-t_0]\times r_i^a=r_i^a$$

因此：

$$u_i=\bar{r}_i/r_i^a\leqslant 1$$

假设 1 拥塞检测的指标为当且仅当通过瓶颈链路的总需求超过瓶颈带宽，即 $\sum_i\bar{r}_i\geqslant C$。假设的现实基础：由于基于负载的检测方案依据“流量的平均值达到或超过某一高负载阈值”来评判是否发生拥塞，因此基于负载的检测方案，该假设通常成立。基于排队理论的拥塞检测方案对流量的变化十分敏感，即使链路的平均利用率较低，突发的流量也可能被误判为拥塞。然而，在 Capabilities 框架下，由于每一个发送者的流量在其进入瓶颈链路之前都会被速率限制器进行“重构”，这样极大地限制了总的输入流量的峰值速率，使得上述假设也能够很好地满足。

定理 1 对于任何拥有充分需求的主机 H，其速率限制为所有其他主机速率限制中最高的，即 $S_H=\max_i(r_i^a)$。

证明：根据所设计的 Capabilities 框架下采用的流量控制算法 AIMD 的特性可知，AI 使得公平性增加，而 MD 保持其不变；每当执行一次 MD，其后面至少会执行一次 AI。这是因为如果只存在 MD，总的速率最终会变得非常小，这样瓶颈链路将不存在拥塞，必将导致执行 AI。因此，随着时间的推移，速率限制的公平性会增加，最终导致所有主机均会得到相同的 r_i^a。对于那些不满足充分要求的主机，流量控制机制则通过不增加甚至减少其速率限制来惩罚它，这必将导致不满足充分需求的主机比符合充分需求的主机得到更低的速率限制。

定理 2 假定发送端拥有 M 个合法用户、N 个恶意用户，它们共享带宽为 C 的瓶颈链路，不管攻击策略如何，任何一个拥有充分需求的合法者 m 最终都将获得一个公平的带宽份额 $\bar{r}_m\geqslant\frac{u_mC}{M+N}$。

证明：依据前面的假设 1 可得：

$$C\leqslant\sum_i\bar{r}_i$$

又由于

$$\sum_i\bar{r}_i\leqslant\sum_i r_i^a$$

由定理 1 可得：

$$\sum_i r_i^a\leqslant\sum_i\max_i(r_i^a)$$

又由于

$$\sum_i\max_i(r_i^a)=r_m^a(M+N)$$

因此有

$$r_m^a\geqslant\frac{C}{M+N}$$

由定义 3 可知：

$$\bar{r}_m=u_m\cdot r_m^a$$

于是有：

$$\bar{r}_m\geqslant\frac{u_mC}{M+N}$$

5 Capabilities 机制的典型方案的比较研究

基于 Capabilities 机制的防御 DDoS 攻击解决方案的简单比较结果如表 1 所列。表 1 对 SIFF，TVA，TVA+，Portcullis，NetFence 等方案就部署的位置、部署的难易程度以及是否对流进行分类等方面进行比较。

表 1 基于 Capabilities 机制的防御 DDoS 攻击解决方案的简单比较

方案	部署位置	部署难度	流分类
SIFF[5]	Router	Hard	√
TVA[6]	Router	Hard	√
TVA+[10]	Border Router	Modest	√
Portcullis[9]	Victim Host	Easy	×
NetFence[11]	Internet	Middle	√

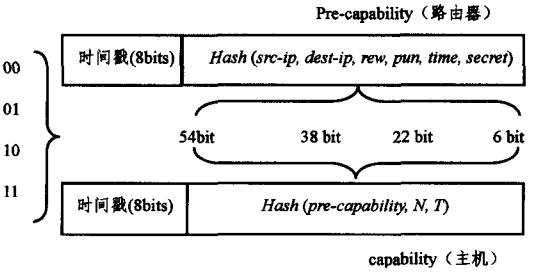


图 4 多尺度的 Capabilities 结构

为了体现仿真实验的可信度，笔者从互联网数据分析协会（Cooperative Association for Internet Data Analysis，CAIDA）网站上获得了互联网路由器和 AS 拓扑数据[12]，并通过数据集的分析与处理得到实验时所需要的数据。在通信协议内核设计方面，Capabilities 机制做了如下大胆的创新：在 IP 层和上层协议之间插入一个“夹层”，对于部署该机制的发送者和接收者，在传输过程中数据包采取在头部“先插入后剥离”的策略。对于传统的路由器可以忽略添加的头部而使用 IP 头部进行转发，但需要对瓶颈链路上的路由器和 AS 中的

边界路由器进行升级，在实际部署时可采取嵌入式设计的方法强制将某些特定的功能内置于需要升级的路由器中。在仿真实验时，所设计的夹层的结构如图 4 所示。

鉴于路由器的处理能力的差异性，设计了 4 种类型的 Capabilities 结构，其原则是：路由器处理能力越强，Capabilities 的尺寸越长；路由器处理能力越弱，Capabilities 的尺寸越短。在 Capabilities 结构中，前两位用来表示路由器的处理能力，同时对应着不同的 Capabilities 长度，即在请求包到达接收端的过程中，沿途路由器根据自身的处理能力生成相应尺寸的 Capabilities。为了更具参考性，还对公平排队策略 FQ (Fair Queuing)进行了仿真实验，该方案旨在将攻击流量限制在不超过链路的公平带宽份额。使用 NS-2[13] 仿真软件设计了两类仿真实验场景来比较 SIFF、FQ、TVA、NetFence、Portcullis、TVA+等方案的性能及其可靠性。仿真实验的拓扑图如图 5 所示。

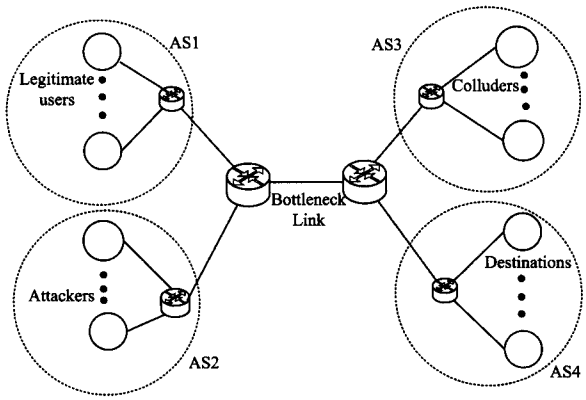


图 5　仿真实验的拓扑图

在仿真实验中，对流量分类采用 3.1 节所探讨的分类方法，将数据包分为请求包(RTS)、规则包(Regular packet)和普通包(Normal packet) 3 种，并对这 3 种不同的数据包给予不同的优先级。为确保源地址的真实性，建立了一条路径标识来进行源定位，在边界路由器上给每个数据包进行唯一的标记，该标记作为对上游路径的身份标识，部署了 Capabilities 机制的路由器对接收到的数据包采用多层次的路径标识公平排队策略进行甄别与归类，如图 6 所示。

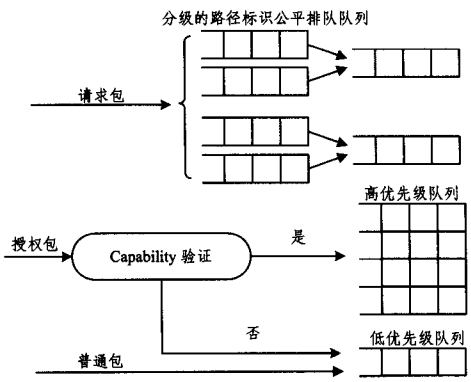


图 6　路由器上进行流量分类的队列管理机制

场景 1　单向链路洪泛攻击，即攻击者直接对受害机节点进行洪泛攻击，当发送至受害机的流量被阻止时，它们则将流量发往与受害机在瓶颈链路的同一侧的其他节点上。图 7 是单向链路洪泛攻击下，文件传输时间与数据包传输的成功率随着攻击者数量增加而变化的曲线。

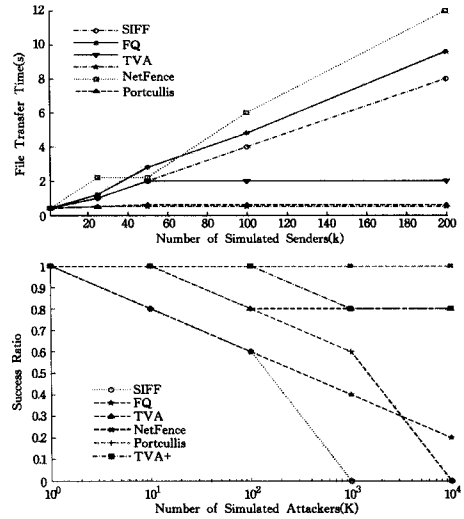


图 7　单向链路洪泛攻击下各种防御方案性能比较

场景 2　双向链路洪泛攻击，即与受害机位于瓶颈链路同一侧的攻击者视为“同伙”或者“串通攻击者”。实验时限定左侧攻击者数量的上限是 10M，“同伙”的数量从 1k 到 10M，图 8 是双链路洪泛攻击下，文件传输时间与数包传输的成功率随着攻击者数量增加而变化的曲线。

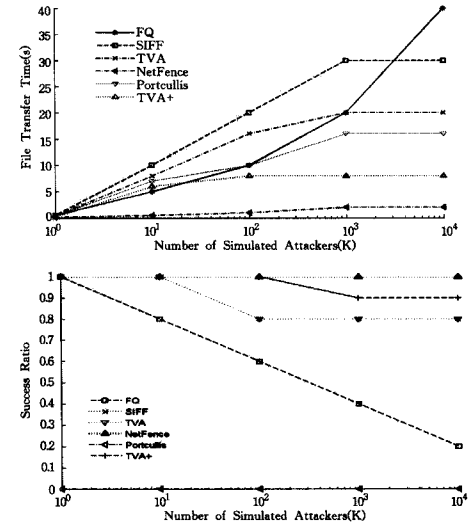


图 8　双向链路洪泛攻击下各种防御方案性能比较

值得说明的是，假设右侧有 m 个“串通攻击者”，左侧有 n 个攻击者，按照基于目的端的公平排队理论，目的端受害机所获得的瓶颈链路带宽份额不超过 $1/m$，而该带宽资源将由所有的合法用户以及 n 个攻击者竞争共享，按照基于源端的公平排队理论，则源端的每一个用户所拥有的瓶颈链路带宽份额将不超过 $1/(mn)$。通过上述两个不同场景的仿真实验，结合实验数据不难看出，对于 TVA+和 NetFence 方案，攻击者数量的增加对文件传输时间以及数据包到达接收端的成功率影响不大，而对其他方案的性能会产生较大影响。

结束语　本文详细阐述了防御 DDoS 攻击的 Capabilities 机制的原理及其典型方案。研究了面向未来互联网的 DDoS 防御方案的整体框架及其组成部分，分析并论证了 Capabilities 机制框架下的安全性与效率，并通过仿真实验比较了这些方案的性能以及可靠性。

参 考 文 献

[1] Worldwide Infrastructure Security Report [OL]. http://www.arbornetworks.com/research/infrastructure-security-report,2013

[2] Bellovin S,Clark D,Perrig A,et al. A Clean-Slate Design for the Next-Generation Secure Internet[C]//National Science Foundation Workshop on Next-Generation Secure Internet. CMU,GENI Design Document,2005

[3] Anderson T,Roscoe T,Wetherall D. Preventing Internet Denial-of-Service with Capabilities [J]. Computer Communication Review,2004,34(1):39-44

[4] Yaar A,Perrig A,Song D. SIFF:A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks[C]//Proceedings of IEEE Symposium on Security and Privacy. May 2004

[5] Yang X,Wetherall D,Anderson T. A DoS limiting Architecture [C]//Proceedings of ACM SIGCOMM. 2005:241-252

[6] Argyraki K,Cheriton D. Network Capabilities:The Good,the Bad and the Ugly[C]//Proceedings of ACM HotNets IV. College Park,Maryland,2005

[7] Walfish M,Vutukuru M,Balakrishnan H,et al. DDoS defense by offense[J]. Proceedings of ACM SIGCOMM,2006,36(4):303-314

[8] Parno B,Wendlandt D,Shi E,et al. Portcullis:Protecting Connection Setup from Denial-of-Capability Attacks [J]. Proceedings of ACM SIGCOMM,2007,37(4):289-300

[9] Liu X,Yang X,Lu Y. To Filter or to Authorize:Network-Layer DoS Defense Against Multimillion-node Botnets[J]. Proceedings of ACM SIGCOMM,2008,38(4):195-206

[10] Liu X,Yang X,Xia Y. NetFence:Preventing internet denial of service from inside out[C]//Proceedings of the ACM SIGCOMM. 2010:255-266

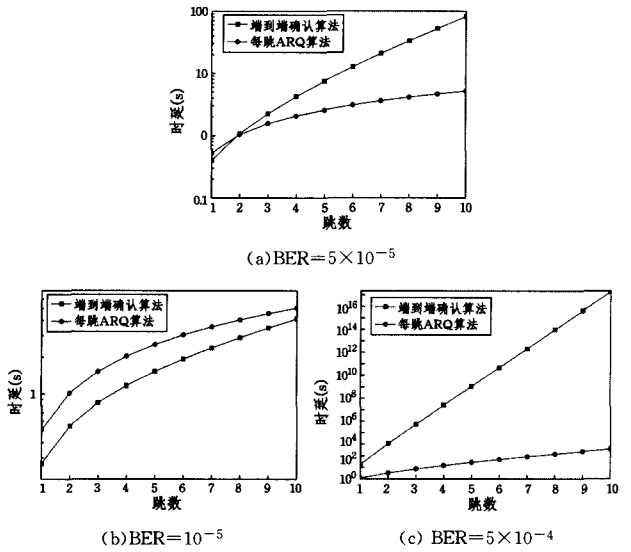
[11] Van Jacobson. Congestion avoidance and control [C]// Proceedings of ACM SIGCOMM'88. 1988

[12] CAIDA[OL]. http://www.caida.org/home/

[13] The Network Simulator NS2[OL]. http:// www.isi.edu/nsnam/ns/

(上接第 180 页)

ARQ 的分片重组算法;当误码率较低(见图 15(b))时,端到端确认算法的时延要小于带有每跳 ARQ 的算法;当误码率较高(见图 15(c))时,端到端确认算法的时延要高于带有每跳 ARQ 的算法。由以上分析可知,如果适当地选取自适应算法框架及算法门限值,可以在动态的通信环境中提高网络通信效率和性能。



(a)BER=5×10^{-5}

(b)BER=10^{-5} (c) BER=5×10^{-4}

图 15 跳数对时延产生的影响

结束语 对 6LoWPAN 的 IPv6 适配层分片与重组算法的分析研究有助于了解 IPv6 协议在低功耗物联网感知层网络中的传输效率和性能,可为后续的上层协议向物联网感知层网络移植提供能耗、时延等方面的量化预测分析,因此对分片与重组算法进行数学建模及数据仿真是十分必要的。根据对分片与重组算法及其端到端确认算法、带有每跳 ARQ 的算法的数据仿真,提出了将网络通信环境即误码率的高低作为判别条件的自适应分片与重组算法,它可以使通信节点在网络环境发生变化时自动调整分片与重组算法,以达到网络的最优性能。

参 考 文 献

[1] Amardeo C, Sarma J G. Identities in the Future Internet of Things [J]. Wireless Pers Commun,2009,49:353-363

[2] Kushalnagar N,Montenegro G,Schumacher C. IPv6 over Low-Power Wireless Personal Area Networks(6LoWPANs)[C]//Overview, Assumptions, Problem Statement, and Goals. RFC 4919,IETF,2007

[3] IEEE Computer Society. IEEE Standard for Information technology— Local and metropolitan area networks — Specific requirements — Part 15. 4: Wireless Medium Access Control (MAC) and Physical Layer(PHY) Specifications for Low Rate Wireless Personal Area Networks(WPANs)[S]. IEEE Std 802.15.4-2006,October 2006:1-320

[4] Montenegro G, Kushalnagar N, Hui J, et al. Transmission of IPv6 Packets over IEEE 802.15.4 Networks[S]. RFC 4944, IETF,September 2007:6-13

[5] Hui J,Corporation A R,Thubert P,et al. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks[S]. RFC6282,IETF,September 2011:5-20

[6] Thubert P,Cisco E,Hui C J,et al. LoWPAN fragment Forwarding and Recovery,Internet Draft draft-thubert-6lowpan-simple-fragment-recovery-07[S]. IETF draft,Dec 2010:1-17

[7] Thubert P,Hui J. LLN Fragment Forwarding and Recovery,Internet Draft draft-thubert-roll-forwarding-frags-01 [S]. IETF draft,February 25,2013:1-16

[8] Ayadi A,Maille P,Ros D,et al. Energy-Effcient Fragment Recovery Techniques for Low-Power and Lossy Networks[C]// Wireless Communications and Mobile Computing Conference (IWCMC),2011,7th International,IEEE. July 2011:601-606

[9] 黄仁,郜辉,任军华. 非时隙 CSMA/CA 性能分析与研究[J]. 计算机工程与应用,2009,45(7):108-110,118

[10] Shuaib A H,Mahmoodi T,Aghvami A H. A Timed Petri Net Model For The IEEE 802.15.4 CSMA-CA Process[C]//PIMRC. Sept. 2009:1204-1210