基于物联网的 DDOS 攻击与防范技术研究

周泓锦 唐宾徽

四川大学锦城学院 计算机与软件学院 四川 成都 610000

【摘 要】物联网在今天的发展取得了了巨大的成功，在各行各业得到了实践应用，它解决了传统设备之间不能通信与管理不方便的问题，并且物联网利用了传感器技术、射频技术、定位系统、嵌入式传感器、无线通信等各种先进的设备和技术，让物与物，物与人之间的交互变得简单可行，可以实时的获取所有联网设备的各种信息，实现了彼此之间的智能感知，沟通和识别。物联网以互联网作为信息传输和通信的载体，随着联网设备的增加构建出庞大的物理网络。但是物联网面临的主要安全威胁也日益严重，根据 DDOS 攻击情况研究报告指出，物联网设备的泛滥导致联网设备的安全性保证不到位，易受到攻击者的恶意攻击。在另一方面物联网的爆发式发展给攻击者提供了便利。本文对物联网遭受到的 DDOS 攻击为例，提出了相关防范技术。

【关键词】物联网 DDOS 攻击

引言：自从美国最重要的 DNS 服务提供商 dyn 遭受大规模 DDoS 攻击以来，twitter、Netflix、CNN 和《华尔街日报》等多家网站都无法正常访问。造成巨大的经济损失，很多媒体称此次攻击为美国“史上遭受最严重的 DDoS 攻击”，此次 DDOS 攻击产生了巨大的影响，值得让人深思的是，在这次网络攻击中，黑客利用了大量物联网设备的安全漏洞对目标发起攻击。经过此次 DDOS 攻击，让分布式拒绝服务攻击真正意义上进入大众的视野。面对日益泛滥的 DDOS 攻击，如何有效的防范成为重中之重。因此本文在分析 DDOS 在物联网当中的攻击原理，提出了将区块链技术，蜜罐部署运用到物联网当中。

1 DDOS 攻击的相关理论

1.1 DDOS 攻击简介

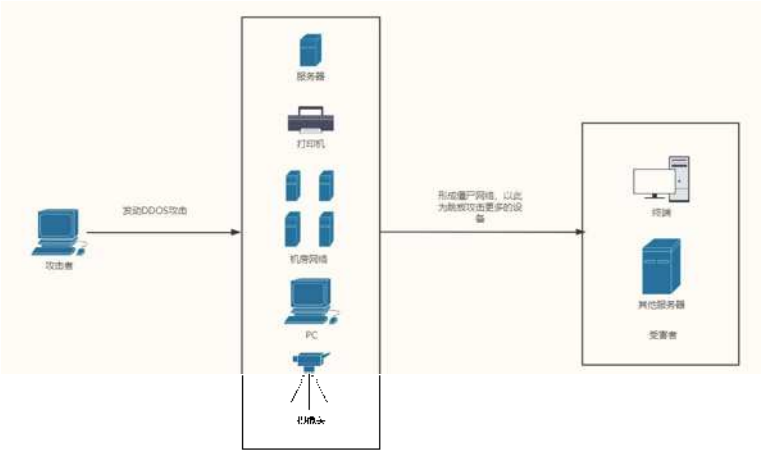
攻击者发起 DDoS 攻击就是利用大量合法的计算机对目标发送访问请求，占用目标服务器的带宽，，使服务器无法正常的向合法用户无法获得服务。通常而言就是利用网络节点的相关资源如：个人计算机，智能联网设备，摄像头，网络打印机等等对攻击目标发起大量访问请求，从而导致被攻击者的链路拥塞或者服务器资源枯竭，从而无法对合法用户提供所需的服务。

1.2 DDOS 攻击原理

DDoS 攻击要求攻击者必须对联网的设备进行攻击，控制联网计算机之后，根据被攻击计算机的路由信息选择最近的其他设备进行攻击。计算机或其他物联网设备遭受攻击之后，会将每台被攻击的计算机变成僵尸。然后攻击者可以远程控制被攻击的设备，进而实现对外辐射。

如果僵尸网络建立起来后，攻击可以以远程控制的方式对僵尸网络中的计算机发送操作指令。让僵尸网络中的计算机执行相关命令对另外的目标实施攻击。当知道需要攻击对象的 ip 地址时，每个僵尸网络当中的设备都会对攻击的目标发送访问请求，导致目标服务器容量溢出，从而无法对其他计算机提供服务，并且每个僵尸网络中的设备都是合法的正常互联网设备，因此很难将恶意的攻击流量与正常流量划分开来。物联网设备在受到 DDoS 攻击时表现为有大量等待 TCP 连接，网络中基本全是无用的数据包，占用网络带宽，进而使设备资源枯竭。无法与外界进行通信和提供服务。

1.3 DDOS 攻击步骤



图一：DDOS 攻击示意图

当前通信网络的发展速度都是很快的，得益于通信技术和处理器的发展，计算机的通信和处理能力得到了很大的提高,即便是家用宽带都能轻易达到千兆级别，因此使用少量的攻击机对物联网当中的设备进行 DDOS 攻击可能不再起到显著的作用，但是如果攻击者采用成百上千的攻击机对物联网设备进行 DDOS 攻击时，很显然攻击者会成功。DDOS 的攻击步骤大概如下：首先攻击者对服务器，机房网络，摄像头等实施 DDOS 攻击，然后被攻陷的设备成为僵尸网络被恶意攻击者控制向外辐射攻击其他设备，如图一所示

1.4 DDOS 攻击的分类

1.4.1 资源耗尽类攻击

资源消耗类是比较典型的 DDoS 攻击，通过制造高流量的无用数据和大量 TCP 连接请求将目标主机的带宽占满和耗尽设备处理资源的能力，从而达到无法提供服务的目的。

1.4.2 服务消耗性攻击

对于服务消耗性攻击而言，不需要巨大的恶意流量，该类攻击主要是针对服务器的特点，实施多对一的精确攻击，如针对 WEB 服务器的访问，FTP 服务器的上传与下载等。通常不是为了占用带宽和拥塞通道作为攻击的目的，它们是为了让服务端始终保持处理高消耗型业务的状态，进而无法对正常用户对服务器的合法访问进行响应。

1.4.3 反射型攻击

反射攻击也被称之为放大攻击，这类攻击依托与 UDP 协议，攻击者不是直接的对目标 ip 地址发起攻击。而是通过一些手段伪装 ip 地址，然后将请求信息通过伪装的 ip 地址发送给服务器，使得服务器用多出请求信息好几倍的数据发送给被攻击的 ip 地址。从而让攻击者的网络带宽被大流量拥塞，导致被攻击者的业务无法正常响应。

2 区块链技术

2.1 区块链技术简介

区块链是一个分布式共享的分类账和数据库，它是去中心化的、不可更改的、可追踪的、集体维护的、高度开放的。区块链是由随机哈希算法生成的一系列区块连接而成。每个块都记录相关事务，不同的块之间按顺序连接，形成一个链式结构。这些特点保证了区块链的公开和透明，为不同的区块之间建立信任关系奠定了基础，实现了多区块间的共同信任和协同行动。

2.2 区块链的分类

2.2.1 公有链

是一个非常开放的，全世界所有人都可读取、发送交易，并且交易能获得有效确认的、也可以参与其中共识过程的区块链，从属于所有联网用户的一种去中心化分布式账本。

2.2.2 私有链

私有链是指一个区块链的写入权限在一个组织或者是公司手里，只能在独立个体的内部进行使用，并且对其读取权限进行了限制。

2.2.3 联盟链

区块链技术的应用在未来既不会是去中心化也不可能是完全集中化的，因为去中心化以为着用户与用户以及设备与设备之间有着绝对的信任关系。但是在实际运用中不可能绝对去中心化，所以联盟链应运而生，其结合了私有链和公有链的相关特点，更符合目前大多数行业发展的实际需求，对面适当的开放了部分权限，即有利于公平公正，也受到了来自于社会的监督。

3 蜜罐

蜜罐是一种对攻击行为进行诱骗的技术，通过布置一些漏洞，诱饵主机等等，引诱攻击者对其进行攻击，并且当蜜罐引诱攻击者入侵成功后时，你就可以分析黑客的攻击数据，针对攻击者的攻击行为安全防护，从而极大的降低了正常设备被恶意攻击的风险。

3.1 蜜罐的分类

3.1.1 低交互蜜罐

低交互蜜罐只是对操作系统一些简单服务的模拟，所以蜜罐获取的信息十分有限，对攻击者的行为进行简单的应答。并且与攻击者之间的交互行为很少，因此获取到攻击者的相关信息非常有限，很难对攻击者进行有效的分析

3.1.2 中交互蜜罐

中交互蜜罐是对真实存在的操作系统的各种行为进行模拟，提供了比低交互蜜罐更多的交互行为，可以从攻击者的攻击行为中获取到更多的信息。

3.1.3 高交互蜜罐

高交互蜜罐提供了一个真实存在的操作系统去与攻击者进行交互，可以将攻击者的更多行为记录下来，但是高交互蜜罐有着一个致命的缺点就是被攻击的可能性非常高，一旦高交互蜜罐被攻击，那么攻击者很可能以此为跳板对更多设备进行攻击。

4 物联网遭受 DDOS 攻击的防范技术

4.1 区块链技术运用到物联网中

在现有的模式中，物联网是由中心节点的服务器对所有联网设备进行管理的，这不仅需要该服务器需要具有强大的运行和处理任务的能力。而且，随着物联网设备呈指数级增长，一旦遭受安全攻击，服务器的维护成本也将大大增加，中小型企业难以维持这么巨大的开销。在另一方面中心化的服务器容易受到 DDOS 攻击，一旦中心服务器被攻击者攻破，那么将会以此被攻破的服务器为跳板，使连入该服务器的物联网遭受攻击，进而辐射到更多设备。因此提出了将区块链的相关技术运用到物联网中，因为区块链有着去中心化的特点，基于这一特点，区块链本身就能够抵御 DDOS 攻击，因为即使区块链当中的一个区块遭受到 DDOS 攻击时，其他区块也不会终端服务，而是会继续进行当前的工作，并且每个区块之间是公开透明，相互备份的，以为着一个区块的所有数据在另一个区块中都能看到，所以即使一个区块被攻破停止服务也不影响其他设备的正常运行。

4.2 在物联网数据中心服务上部署蜜罐

物联网设备大都使用同一的协议栈，并且物联网技术往往是离不开一个中心化的服务器，而且当前许多物联网设备的安全性较低，这就以为者一旦中心化的服务器遭受到 DDOS 攻击时，容易依托安全性低的其他设备将攻击辐射出去从而导致更多的物联网设备被攻击，因此在无法改变物联网中心化的本质上面，如何抵御日益泛滥的攻击，提出了将蜜罐部署在中心化的服务器和安全性较低的物联网设备上，通过蜜罐模拟操作系统，开放端口和服务去与攻击者进行交互，对攻击者的数据进行分析，进而获取攻击者采用的攻击方式。连接端口等等，最后根据攻击行为进行有效的应对。

结语

DDOS 攻击是当下网络发展当中面临的主要威胁，传统的网络安全防御技术研究不能用于抵抗 DDOS 的攻击，DDOS 攻击使系统中出现大量高流量的无用数据，占用带宽，消耗设备资源。区块链作为一种新兴技术，得益于区块链去中心化的本质，可以有效抵御 DDOS 攻击。另一方面在无法改变物联网设备具有中心化服务器的前提下可以通过部署蜜罐来防御 DDOS 攻击。蜜罐技术能够有效的诱骗攻击者进行攻击，并能通过与攻击者交互行为分析攻击者的相关数据，从而进行安全防护。因此，本文基于区块链技术和蜜罐部署，对物联网设备遭受 DDOS 攻击给出了有效的防御方法。并在未来的研究中解决好物联网发展的安全问题。

【参考文献】

[1] 谢欣岳，孙长江．区块链技术在工业物联网中的应用 [J]. 电子技术与软件工程 ,2020(17):173-174.

[2] 瞿少凯 .5G 技术促进区块链在物联网中的应用 [J]. 中国新通信 ,2020,22(06):100.

[3] 汤辉，付康，胡少文．一种基于分布式蜜罐技术防御监测 DDoS 攻击的方法 [J]. 江西通信科技 ,2020(03):33-35.

[4] 厉章忠． 基于蜜罐技术的 DDoS 防御模型研究 [D]. 东华大学 ,2009.

[5] 林美玉，韩海庭．物联网安全：核心问题与缓释策略 [J]. 中国电信业 ,2020(06):66-70.