对比特币矿池的 DoS 攻击

18308045 谷正阳

1 DoS 攻击

1.1 简介

DoS 攻击即拒绝服务攻击，是一种用于破坏用户合法访问目标网络和网络资源的攻击。一般来说，它是通过用大量的流量或恶意请求令目标（网络服务器通常是网络服务器）过载，使目标服务器故障甚至完全失灵。首例有记载的 DoS 攻击发生于 2000 年 2 月，由一个 15 岁的加拿大黑客对 Amazon 和 eBay 的网络服务器发起。自此以后，越来越多的人利用 DoS 攻击来破坏许多行业的目标。

1.2 种类

由于不是所有的设备和网络都易受同一种方法的危害，那些造成危害的攻击经常是可以巧妙地运用漏洞进行。以下是几种常见的 DoS 攻击种类。

1.2.1 缓冲区溢出攻击

缓冲区溢出攻击是最常用的攻击，它通过发送比目标设计能够处理流量更多的流量来实现。这种攻击可以使目标进程崩溃。

1.2.2 ICMP flood 攻击

ICMP flood 攻击在目标网络错误地配置一台设备，强制其对每个节点发送伪造包，使网络过载。

1.2.3 SYN flood 攻击

SYN flood 攻击发送请求连接目标网络服务器，但不完成完整的连接认证，然后继续对目标的每个剩余的开放的端口重复上述操作直至致使目标服务器崩溃。

1.3 区块链对 BDoS 攻击的防御机制

1.3.1 去中心化

区块链的去中心化机制为其抵御 DoS 攻击和 DDoS 攻击提供了强大的支撑。即使是许多节点无法通信或下线，整个区块链仍可以继续运行并验证交易。当那些崩溃的节点可以重新恢复工作时，它们又可以重新同步并获得那些没受攻击的节点提供的数据，重新跟上最近的数据进度。区块链可以抵御这些攻击的程度与网络的节点数和哈希率有关，对于最老最大的加密货币比特币而言，它被认为是最安全且最不易受攻击的区块链。这意味着 DoS 攻击和 DDoS 攻击更不容易对其造成崩溃。

1.3.2 工作量证明

工作量证明机制使得对比特币的许多攻击十分昂贵。矿工只能证明他们在系统外花费了计算能力来创建区块。仅当系统中的大部分计算能力运行正常时，才能维护区块链的安全。因此，攻击者要进行攻击，其拥有的计算能力就要比其他参与者的总和都要高，即 51% 攻击。对于主要的加密货币来说，51% 攻击的代价对于大多数实体而言都是难以承担的。

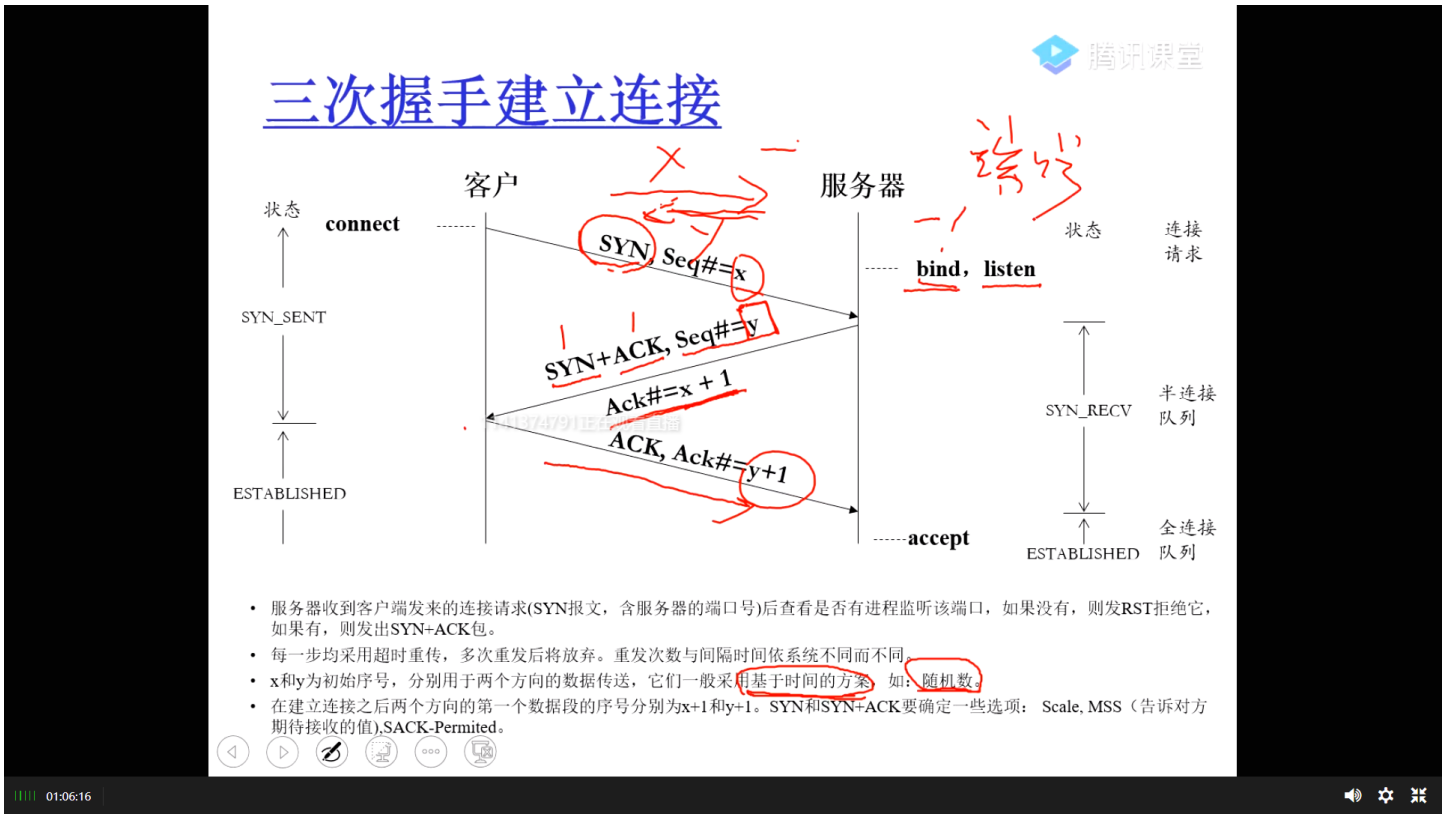
2 对比特币矿池的 DoS 攻击

2.1 比特币矿池

由于比特币全网的运算水准在不断的呈指数级别上涨，单个算力微弱的矿工难以获得收益，于是就出现了多个矿工联合算力挖矿，挖出的比特币奖励按贡献度分享，这便是矿池。大多数矿池都是“托管矿池”，即公司或者个人运营着矿池服务器。矿池服务器运行着专用的软件，根据矿池挖矿协议来协调矿工们的工作。其他机器自然知道其公网 ip 及开放端口，可以利用此来进行 SYN flood 攻击令矿池服务器瘫痪进而达到攻击整个矿池的目的。

2.2 具体实现

TCP 协议是进程与进程之间建立，要建立连接，会先进行三次握手：



而这个流程有一个缺陷：在第二次握手在接受服务器发送的 SYN+ACK 报文后不发送 ACK，服务器会等待对方放入半连接队列，并等待 ACK，超时重传 SYN+ACK，直至超过重复次数才会释放连接。默认重试次数为 5 次，重试的间隔时间从 1s 开始每次都番倍，分别为 1s + 2s + 4s + 8s +16s = 31s, 第 5 次发出后还要等 32s 才知道第 5 次也超时了，所以一共是 31 + 32 = 63s。这个时间非常长。另外由于

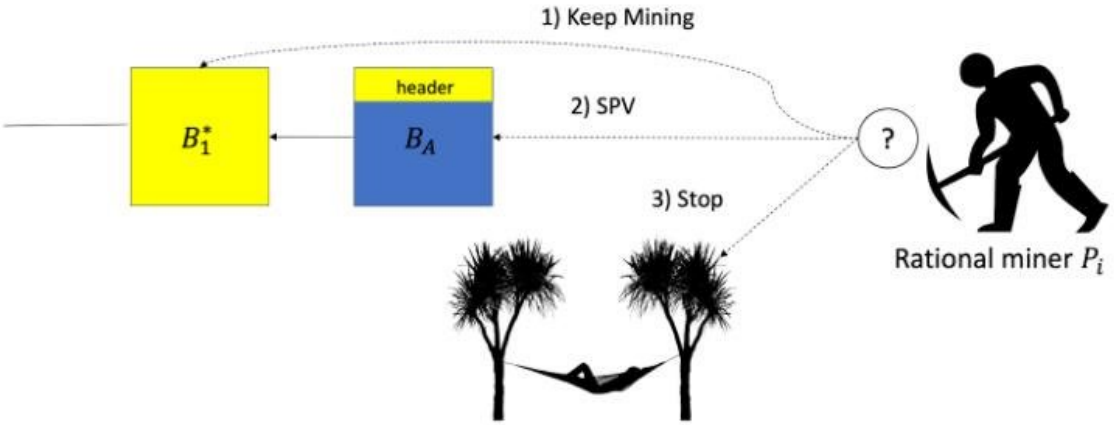
半连接队列是有长度限制的，默认是 1024，如果攻击者在这个时间内不断对目标服务器开放的端口发送 SYN 报文，且收到 SYN+ACK 后不发送 ACK。这样服务器的半连接队列会被大量占用以至占满，这样就无法再处理新的连接请求也就无法继续协调矿工工作，这样整个矿池就崩溃了。

3 对基于 PBFT 共识的区块链的 DoS 攻击

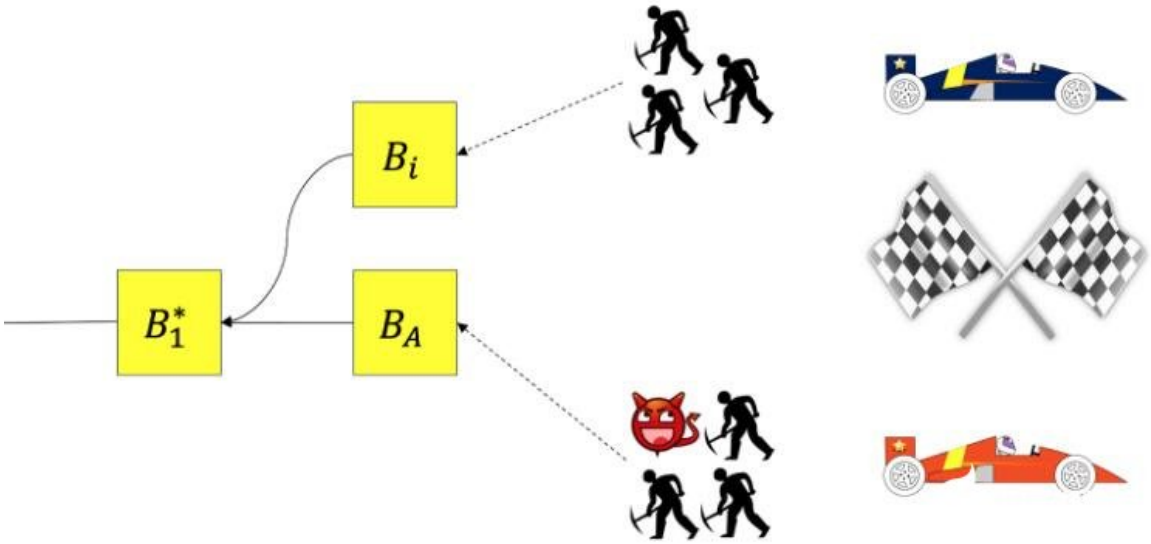
上述方法是对矿池进行攻击，而对整个比特币社区，这种攻击无法奏效，因为整个社区是去中心化的，没有中心服务器。想要成功需要针对比特币社区的漏洞来进行特别的攻击。在区块链中，奖励机制促使矿工挖矿，但是一旦激励机制不能够促进良好行为时，区块链就会处于危险之中。BDoS 攻击就是利用这一点，会使得整个网络处于一种状态，使得理性矿工最佳的行动是停止挖掘。

3.1 具体实现

攻击者挖出一个块，然后只公布区块头。这时候矿工有三个选择：其可以延长主链，然后忽略区块头；其可以扩展这个区块头（SPV 挖矿）；其可以停止挖矿，既不消耗算力，也不赢得奖励。



如果理性矿工选择扩展主链，找到并广播一个新的区块，那么攻击者矿工将那么攻击者就快速广播与区块头对应的完整块（攻击块）。因为点对点网络里每个节点的网络连通性不一致，有的节点会先收到攻击块，有的节点会先收到防守块，这会导致两组矿工之间的竞争。



在一定概率下，该理性矿工会输掉比赛，使得区块 Bi 最终不被包含在主链当中。因而这种情况下在最后一个完整区块上挖矿的预期回报会低于一般情况。如果理性矿工遵循选择扩展这个区块头 BA，则攻击者就不会发布完整的区块 BA。这导致这个区块不会上主链，从而导致该区块的预期回报为零。由于挖矿还需付出大量计算，一定情况下关机不继续挖矿成为预期净回报最高的选择，因而就使得奖励机制无法鼓励矿工继续挖矿，进而无人记录交易，进而使整个网络瘫痪。

3.2 影响

3.2.1 规则的共识

规则即确保交易、区块有效的机制，保证了比特币参与者能够进行最基本的交互。而 BDoS 攻击可能会破坏奖励机制，导致理性的矿工最优的策略是不挖矿，这样相当于破坏了规则共识的一环。

3.2.2 历史记录的共识

记录即已发生的被记录在区块链串接的 Merkle Tree 上的交易，保证了去中心化的 UTXO 的正常运行。规则中如最长链原则，大家优先相信最长的账本，因而规则的共识促成了历史记录的共识。而 BDoS 攻击一旦破坏规则共识，没有人继续挖矿或保有账本，因而也破坏了交易记录的分布式存储的一致性，导致破坏了历史纪录的共识。

3.2.3 比特币价值的共识

价值共识即与现实货币的汇率，保证所有人想要比特币，所有人可以用比特币交易。历史纪录的共识保证了人们对比特币的信任。然而 BDoS 一旦破坏了历史纪录的共识，会令人们丧失对比特币的信任，进而降低对比特币的购买意愿，进而比特币贬值，又会导致一部分人抛售比特币，进而加速了比特币的贬值，最终破坏了比特币价值的共识。