基于区块链技术的网络 DDoS 联合防御方法研究

◆陈　旭

（国网四川省电力公司信息通信公司　四川　610041）

摘要：由于不安全的移动及固定设备的快速增加，以及网络流量的指数级增长，导致分布式拒绝服务攻击(DDoS)成为威胁计算机网络的重大威胁。孤立的防御方法难以应对大规模的 DDoS 攻击，因此，跨组织的联合防御成为了解决 DDoS 问题的有效手段。为了方便跨组织的 DDoS 防御，本文提出了基于区块链技术的网络 DDoS 联合防御方法。在公有区块链以太坊(Ethereum)基础上，设计智能合约，授权用户可以更新 DDoS 攻击者名单，所有用户可以查询 DDoS 攻击者名单。由于利用了以太坊的基础设施，本方法无需修改现有网络设施，从根本上解决了跨组织联合防御的实施难题。由于区块链的不可篡改性，攻击者无法干扰本方法的运行。由于智能合约的可编程性，本方法具有很强的扩展性。

关键词：DDoS 攻击；联合防御；区块链；智能合约

0　引言

近年来，分布式拒绝服务(DDoS)呈现上升的趋势[1]，其主要任务是中断或中止网络服务。DDoS 动机五花八门，包括：商业竞争、勒索钱财甚至政治目的[2]。除了攻击频率上升以外，DDoS 攻击的攻击强度和持续时间也呈现上升的趋势，导致 DDoS 攻击更加危险和难以防御。DDoS 攻击增强的一个原因是攻击者可以获得更多的反射器(reflector)，例如安全性较差的 IoT 设备和家用网关[3]。DDoS 会导致许多危害，轻则降低网络服务吞吐量、降低用户体验，重则带来严重的经济损失。

为了应对 DDoS 攻击，学术界和工业界提出了大量的方法从 4 个层面上开展对 DDoS 攻击的防御，分别是：攻击防护、攻击检测、攻击溯源和攻击清理[4]。遗憾的是，任何单个组织都无法应对大规模的全网性 DDoS 攻击。例如：DDoS 攻击源离检测点非常远，基本检测点能够检测到 DDoS 攻击，也很难进行有效防御。因此，最近有一些研究工作指出需要跨组织的合作，实现对 DDoS 攻击的有效防治。其主要思想是：多个组织对自己区域内的网络实施 DDoS 攻击检测和防御，检测到 DDoS 攻击后，将攻击者信息共享给其他组织，这样一来，其他组织可以在 DDoS 攻击到来之前提前准备并展开防御。但是，现有跨组织联合防御方法存在一些缺陷，导致其不能很好的实施和部署。这些缺陷包括：需要修改现有网络基础设施、需要设计新的网络协议、资金耗费高等[5-9]。

为了方便跨组织合作，本文提出基于区块链技术的 DDoS 跨组织联合防御方法。本方法的核心思想是：设计专门的智能合约，实现跨组织的攻击者名单更新和查询。本方法部署在公有区块链以太坊(Ethereum)上，因此不需要修改现有的网络基础设施。由于区块链的不可篡改性，因此本方法部署后是相对安全的，攻击者无法影响本方法的运行。由于智能合约的可编程性，可以随时增删黑名单列表，也可以随时增删授权用户。因此，本方法能够很好的解决跨组织合作难以实施和部署成本高的问题。

本文第一部分介绍区块链、以太坊和智能合约相关背景知识；第二部分回顾相关工作；第三部分介绍本方法的设计；第四部分介绍关于本方法的具体实现；第五部分总结全文。

1　背景知识

区块链的概念是在 2008 年被正式提出，第一个区块链系统是作为比特币的核心组件，其功能是公开的交易账本[10]。从概念上讲，区块链是一个不断增长的记录列表，这些记录被存放在一个个的区块中，这些区块用指针链接起来，形成一个区块的链条。一个区块通常包含一个指向前一个区块的指针，一个时间戳，零个或者多个交易。区块链的底层结构是一个 P2P 网络，所有矿工(miner)和验证者(Validator)都通过这个 P2P 网络相连。一旦交易被记录在了区块链中，相关的数据就无法修改，除非攻击者拥有了超过 50%的区块链计算能力。因此，区块链从设计上保证了数据防篡改。

以太坊是仅次于比特币的第二大区块链，同时也是支持智能合约的最大的区块链(比特币不支持智能合约)。如果没有特殊说明，下文中提及的区块链指以太坊，智能合约指运行在以太坊上的智能合约。智能合约是一种由程序员编写并部署，由普通用户调用的特殊程序，其部署在区块链上并在区块链上的所有节点(矿工+验证者)上运行。智能合约由高级语言，如：Solidity 编写，并编译成为 EVM 字节码，并运行在节点上的 EVM 虚拟机内。开发人员通过发送目标地址为 0 的交易部署智能合约，交易的数据域存放了智能合约的的 EVM 字节码。用户同样通过发送交易的方式调用智能合约，交易的目标地址是被调用合约的地址，数据域指明了被调用的函数以及给出了函数的参数。EVM 虚拟机是一个图灵完备(Turing-complete)的运行环境，所以通过编写智能合约能够实现各种各样的应用。本文就是设计了一个智能合约，用于联合不同组织。

2　现有研究

有一些工作提出将不同的组织联合起来共同对抗 DDoS 攻击。IETF (Internet Engineering Task Force)设计了一个新协议，叫做 DOTS (DDoS Open Threat Signaling)，涵盖了组织内部以及跨组织协作抵御 DDoS 攻击[5]。该协议由多个代理协作实现，代理包含了 DOTS 服务器和 DOTS 客户端，并能够在中心化和分布式环境中发布黑名单以及白名单信息。一个 DOTS 客户端首先向一个 DOTS 服务器注册。DOTS 协议用来协调 DDoS 防护服务。Steinberger 等人提出了类似的方案，但他们使用的协议是基于 FLEX (FLow-based Event eXchange)格式的，这种协议格式有助于简化该方法的整合与部署，同时有助于不同域之间的通信[7]。

Rashidi 等人提出基于网络功能虚拟化(Virtual Network Functions: VNF)的联合防御策略[6]。该方法通过 VNF 重定向和重构过量的网络流量到其他的联合的域中做过滤处理。Zhang 和 Parashar 提出基于 gossip 通信机制用以在独立的检测点之间交换攻击信息，从而汇聚关于攻击的所有信息[9]。该方法使用 P2P 网络来分发攻击信息。Velauthapillai 等人提出了相似的办法，同样是通过基于 gossip 的协议在网络上通过中间路由器可交换信息[8]。

Sahay 等人提出的方法有所不同，他们提出了一个联合框架，允许用户从自治系统(AS)请求 DDoS 防御。综上，现有的方法需要修改网络基础设施，设计新的网络通信协议，并且会产生高昂的费用。因此，现有方法在实施和部署上存在困难。

3 方法设计

本文提出基于区块链技术的 DDoS 攻击联合防御方法，其目标是克服跨组织联合的难度，降低方法实现和部署方面的开销。因此，本方法设计了专用的智能合约用以存储攻击者黑名单、提供增删黑名单功能、增删认证用户功能以及查询黑名单功能。其中，只有合约的开发者才能够增删认证用户，而通过认证的用户都可以增删黑名单，而所有的区块链用户都可以查询黑名单。需要注意的是，合约开发者对用户的认证过程是在线下进行的，合约开发者可以在网络上公布自己的联系方式，希望成为认证用户的组织则可以在线下联系合约开发者，通过开发者的审核后，则会成为认证用户。因此，本文假设开发者已经拥有了认证用户名单。图 1 是本方法的整体结构。

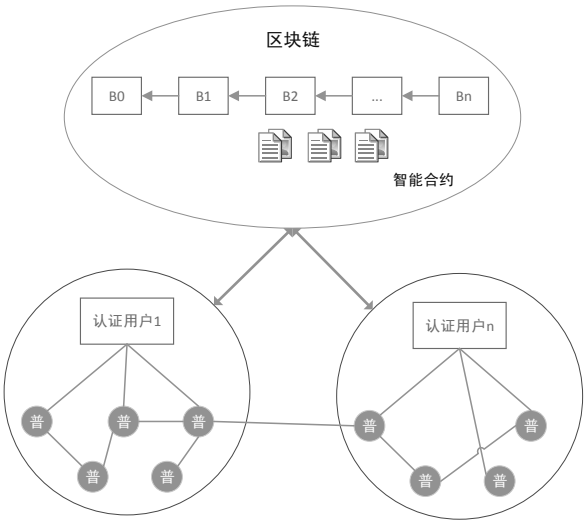

图 1 本方法架构示意图

智能合约部署在区块链上，认证用户发送交易到智能合约增删攻击者黑名单，而普通用户也可以发送交易到智能合约查询攻击者黑名单。认证用户之间，普通用户之间均不直接进行通信，所有的增删查改过程全部通过区块链进行，这就保证了各个用户的黑名单的一致性。此外，所有的操作都经过区块链，攻击者无法篡改和取消黑名单的增删查改操作，攻击者也无法篡改黑名单。

4 方法实现

图 2 给出了智能合约的简单实现，需要注意的是，图 2 仅展示了实现黑名单增删查改核心功能代码。第 1 行指明编译器是 Solidity 0.4.0，从第二行开始是智能合约代码，命名为 DDoS。第 3 行定义了一个 owner 变量，用以存放合约作者的地址。第 4 行和第 5 行分别定义了两个数组，存放所有的认证用户和攻击者地址。第 7 行是智能合约的构造函数，当智能合约被创建的时候执行，它把合约开发者记录下来，同时将合约开发者设置为认证用户，从而合约开发者也可以增删攻击者黑名单。

addAuth 函数用以增加认证用户，只有合约作者才可以增加认证用户，所以第 14 行对交易发送者的身份进行了验证，如果不是合约作者就抛出异常。随后，第 15 行添加认证用户。deleteAuth 的流程和 addAuth 类似，不同的是在第 21 行用一个循环查找认证用户，如果找到则删除。addAttacker 函数的功能是增加攻击者黑名单，首先通过一个循环判断交易发起者是否是认证用户，如果不是则抛出异常。通过认证以后才将新的攻击者信息添加到 attackers 数组。deleteAttacker 函数在通过验证后，用一个循环查找是否存在交易制定的攻击者，如果存在则从黑名单中删除。queryAttackers 函数的功能是查询所有的攻击者黑名单，所以直接返回 attackers 数组。由于所有用户都可以查询攻击者黑名单，所以 queryAttackers 不需要身份验证。

```
1  pragma solidity ^0.4.0;
2  contract DDoS {
3      address owner;
4      address[] auth_users;
5      uint32[] attackers;
6
7      function DDoS() {
8          owner = msg.sender;
9          auth_users.push(owner);
10     }
11
12     function addAuth(address auth_addr)
13     {
14         if(msg.sender != owner) throw;
15         auth_users.push(auth_addr);
16     }
17
18     function deleteAuth(address auth_addr)
19     {
20         if(msg.sender != owner) throw;
21         for(uint j = 0; j < auth_users.length; j++)
22             if(auth_users[j] == auth_addr) delete auth_users[j];
23     }
24
25     function addAttacker(uint32 attacker_addr)
26     {
27         uint i;
28         for(i = 0; i < auth_users.length; i++)
29             if(auth_users[i] == msg.sender)break;
30         attackers.push(attacker_addr);
31     }
32
33     function deleteAttacker(uint32 attacker_addr)
34     {
35         uint i;
36         uint j;
37         for(i = 0; i < auth_users.length; i++)
38             if(auth_users[i] == msg.sender)break;
39         if(i == auth_users.length) throw;
40         for(j = 0; j < attackers.length; j++)
41             if(attackers[j] == attacker_addr) delete attackers[j];
42     }
43
44     function queryAttackers() returns (uint32[])
45     {
46         return attackers;
47     }
```

图 2 智能合约核心代码

5 结语

DDoS 攻击是计算机网络的重大威胁，孤立的防御方法无法对大规模全网络的 DDoS 攻击进行有效防御，而现有的跨组织方法存在各种缺陷，导致这些方法事实和部署困难。为了解决跨组织 DDoS 防御实施困难的问题，本文提出了基于区块链技术的 DDoS 联合防御方法。在以太坊上开发智能合约，用以维护认证用户与攻击者黑名单，认证用户可以增删黑名单而任何参与者都可以查询黑名单，从而实现了跨组织的信息共享。由于利用了以太坊，本方法不需要修改网络基础设置，也不需要设计新的网络协议，也不需要大量的资金投入，因此解决了联合 DDoS 防御部署困难的问题。此外，以太坊的防篡改特性使得攻击者难以干扰本方法的运行。同时，由于智能合约的可编程性，本方法具有很好的扩展性。

参考文献：

[1]Akamai: How to Protect Against DDoS Attacks – Stop Denial of Service (2016).https://www.akamai.com/us/en/re-Sources/protect-against-ddos-attacks.jsp.Accessed 10 Jan ,2017.

（下转第 39 页）

与去使能等功能，但是这些功能的实现要重定义 ONU 设备和 OLT 设备之间的管理方法，很难升级那些在网运行的相关设备，部署难度比较大。归纳起来，通过 TMS 系统和 PON 网关二者的结合，可以更好地进行 HGU 设备远程管理工作，或者可以说其可以有效解决 HGU 设备未来一段时间的全面远程管理工作。

2.2 PON 网络终端未来发展趋势展望

随着我国通信技术的进一步发展，未来宽带接入网会以 PON 接入为主，ONU 设备会作为光纤网络在家庭中的最后节点，相应的终端功能会进一步得到丰富，且不同终端设备生产厂家的 ONU 设备与 OLT 设备可以实现互通组网。当前我国运营商已经开始逐步采用 HGU 设备来替代最初的“ONU+HG”组网结构，可以使上网用户在家庭网络中实现多种网络业务，比如 IPTV 业务、可视电话业务与基本的上网业务。但是为了实现 IPTV 业务，除了确保电视和 HGU 设备相互连接之外，还要将其串接上机顶盒设备，如天猫魔盒等。未来有望将机顶盒设备的功能也集成在 ONU 设备中，真正使其满足家庭上网的各项业务需求，减少家庭中网络终端设备的数量，进一步降低网络终端设备的能耗。另外，随着移动物联网的飞速发展，未来有望实现家庭内各种“智能”设备之间的相互连接，进而可以智能化管理家庭中的各种设备。另外，如果在管理 HGU 设备的时候仅仅采用 PON 网管，由于 GPON 协议或 EPON 协议标准中没有对 PON 网管配置 HGU 设备的三层相关业务进行明确定义，所以这可能会不同厂家对 PON 网管配置 HGU 设备中的机制出现差异，影响 ONU 设备和 OLT 设备之间的互通，所以未来的发展中这个方面问题需要及时加以解决，力求可以充分利用 PON 技术的发展来全面推动我国互联网行业的稳步发展。

3 结语

总之，伴随着我国互联网技术的发展，PON 技术标准化进程得到了进一步推进，同时运营商和网络终端生产厂家的共同努力促使我国 PON 网管配置 HGU 的规范更加趋于标准化，比如不同生产厂家的 OLT 和 ONU 可以实现互通。但是在考虑组网便利性的同时，要注意考虑设备的兼容性，避免因设备兼容问题影响使用功能的正常发挥。

（上接第 26 页）

属综合的体系，而且还存在自身的独特特征，比如多层次防御，同时，还存在立体纵深特征，基于发展层面来说，虚拟技术在今后将会具有更为宽广的发展空间，这就需要从以下方面着手：第一，基于现状来啊看，虚拟网络技术发挥其中的作用性，显现良好的使用效果，在未来发展中需要保持现阶段的发展特征，逐步向稳定性、安全性，还有可靠性方面迈进，从发展层面分析，虚拟网络技术在实际应用中要注意，不断完善其网络应用技术，特别是在可靠性方面，这样才能保障数据传输的准确性，所以在未来研究中，必须要将高效传输系统作为基础，发挥虚拟网络的功能性，这样才能为计算机网络的安全性提供保障。其次，计算机网络依靠虚拟网络技术自身的功能性特点，借助其自身的优势性保障网络的安全性，在今后的发展中，虚拟网络技术还存在诸多需要完善的部分，消除很多制约因素，将虚拟网络技术应用到计算机网络安全保障之中，能够提升整体的工作性能，彰显安全性与有效性。最后，随着科学及信息技术的不断发展，智能化已经是未来发展的主体趋势，这对于计算机虚拟网络技术的应用可以说提供良好的契机，需要融合现代化的技术，同时优化智能化技术，从而获取最满意数据传输结果，多种技术联合使用必然能够发挥最大的效能，研究出最智能化的方法。

5 结语

计算机网络安全在现阶段的重视度越来越高，如何突显计算机的安全性能则是目前研究的课题，有研究显示，采取虚拟网络技术能够保障计算机网络的安全性，确保数据准确传输，提升网络的安全性能。

参考文献：

[1]宋福.计算机网络安全中虚拟网络技术的作用效果[J].电脑迷，2017.

[2]李斯祺.计算机网络安全中虚拟网络技术的作用效果[J].科技展望，2017.

[3]罗驿庭.计算机网络安全中虚拟网络技术的作用效果[J].中国新通信，2017.

[4]吴巧雪.简析计算机网络安全中虚拟网络技术的作用效果[J].四川水泥，2016.

[5]唐卫国.简析计算机网络安全中虚拟网络技术的作用效果[J/OL].电子技术与软件工程，2016.

[6]郑振谦，王伟.简析计算机网络安全中虚拟网络技术的作用效果[J].价值工程，2014.

（上接第 30 页）

[2] Mansfield-Devine,S.:The growth and evolution of DDoS.Netw.Secur.10,2015.

[3] The Associated Press: Hackers Used ‘Internet of Things’ Devices to Cause Friday’s Massive DDoS Cyberattack. http://www.cbc.ca/news/technology/hackers-ddos-attacks-1.3817392. Accessed 10 Jan 2017.

[4] Peng,T.,Leckie,C.,Ramamohanarao,K.: Survey of network-based defense mechanisms countering the DoS and DDOS problems.ACM Comput. Surv. (CSUR) 39(1),2007.

[5]Nishizuka,K.,Xia,L.,Xia,J.,Zhan,D.,Fang,L., Gray,C.: Inter-organization cooperative DDOS protection mechanism. Draft.https://tools.ietf.org/html/draft-nishizuka-dots-inter-domain-mechanism-02.

[6] Rashidi,B.,Fung,C.: CoFence: a collaborative DDOS defence using network function virtualization.In:12th International Conference on Network and Service Management (CNSM 16),October 2016.

[7]Steinberger,J.,Kuhnert,B.,Sperotto,A.,Baier,H.,Pras,A.:Collaborative DDOS defense using flow-based security event information.In:NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium,pp.516-522,April 2016.

[8]Velauthapillai,T.,Harwood,A.,Karunasekera,S.:Global detection of floodingbased DDOS attacks using a cooperative overlay network.In:Network and System Security (NSS),pp.357 - 364.IEEE 2010.

[9] Zhang,G.,Parashar,M.:Cooperative defence against DDoS attacks. J. Res. Pract. Inf. Technol,2006.

[10]S.Nakamoto.(2008)Bitcoin:A peer-to-peer electronic cash system. [Online].Available: https://people.eecs.htberkeley.edu/raluca/cs261-f15/readings/bitcoin.pdf.