一种区块链网络的 DDoS 攻击模型

刘昌平 刘 海 李 威
(广东科学技术职业学院计算机工程技术学院 广东 广州 510640)

摘 要 攻击区块链及应用的手段非常多。提出一种分布式拒绝服务攻击(Distributed Denied of Service, DDoS)攻击模型,建立 2 个指标衡量 DDoS 攻击对区块链网络性能的影响。以 Hyperledger Fabric 为环境,在 6 组实验中设置不同数量的 DDoS 攻击节点,仿真 DDoS 攻击事件,设置 1 组实验仿真 DDoS 攻击全过程。实验表明,区块链网络存在 DDoS 攻击的安全隐患,区块链对等节点可以成为 DDoS 攻击节点,攻击节点数量较少(占比低于 33% 或 51%)时能发起 DDoS 攻击,DDoS 攻击对区块链的破坏性主要是延长交易的结束时间,造成网络吞吐量及服务性能下降。

关键词 区块链 网络安全 攻击 共识 拒绝服务 对等节点

中图分类号 TP302.7 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.11.050

A DDoS ATTACK MODEL FOR BLOCKCHAIN NETWORK

Liu Changping Liu Hai Li Wei
(*Computer Engineering Technical College, Guangdong Polytechnic of Science and Technology, Guangzhou 510640, Guangdong, China*)

Abstract There are many ways to attack blockchain and applications. We propose a DDoS attack model and establish two indicators to measure the impact of DDoS attacks on the performance of blockchain networks. Utilizing Hyperledger Fabric to construct the experimental environment, 6 experiments with different number of attacking peer nodes were designed to simulate DDoS attack events. Another experiment simulated the whole process of DDoS attack from beginning to end. Experimental result shows that blockchain network is indeed vulnerable to the potential risk of DDoS attack. The internal peer nodes of blockchain have their probability of becoming the DDoS attacker. Even a small number of attackers (ratio below 33% or 51%) could attack blockchain. The main destruction of DDoS attack is delaying the service time of transaction, reducing the service throughput as well as performance.

Keywords Blockchain Network security Attack Consensus Denied of service Peer node

0 引 言

DDoS 通常是指分布在网络不同位置的多个攻击者同时向一个或多个目标发起攻击,使其丧失正常的服务能力,甚至导致服务瘫痪。DDoS 表现形式有流量耗尽攻击和资源耗尽攻击[1],前者通过泛洪手段消耗攻击目标的带宽资源,例如 UDP 和 ICMP 泛洪攻击[2],后者消耗攻击目标的计算资源,例如 TCP SYN 攻击[2-3]。DDoS 不仅攻击中心服务器,还对分布式计算与资源网络构成安全威胁,例如云计算[4]和物联网,滥用物联网资源,消耗物联网终端能量,导致服务中断、延时、性能下降[5]。2016 年 10 月 Dyn 攻击导致 Twitter、Amazon 等网络服务中断[6]。2018 年代码托管网站 GitHub 遭到大规模的 DDoS 网络攻击,每秒流量最高达到 1.35 TB[7]。

区块链是一种分布式数据库,大量分散的对等节点在 P2P 网络上构建一个区块链网络[8],利用冗余的账本数据库和共识算法在不可信的开放网络环境中建立信任关系,因此区块链网络也是一种分布式计算与

收稿日期:2021-05-30。广东省教育厅普通高校重点领域专项项目(2019KZDZX1045);广东省教育厅普通高校特色创新项目(2019GKTSCX029);广东科学技术职业学院校级科研项目(XJPY202104)。**刘昌平**,讲师,主研领域:区块链,信息安全。**刘海**,副教授。**李威**,副教授。

资源网络,同样面临包括 DDoS 在内的各种安全攻击。一般将区块链应用体系划分为应用层(含智能合约层)、共识层、网络层、存储层(或数据层)[9-10],并从不同层研究区块链的安全问题及其对策。日食攻击(Eclipse Attack)是区块链网络层的一种典型攻击手段[11],攻击目标是隔离受害节点使之脱离区块链网络,仅接收攻击节点的信息,当受害节点达到一定数量时即可发起包括 DDoS 在内的其他攻击。女巫攻击(Sybil Attack)[12]是另一种网络层攻击手段,攻击节点伪造多个虚假身份并进入区块链网络,攻击区块链账本数据库的冗余机制,当受控节点达到一定数量时即可发起其他攻击,例如 DDoS、"双花"攻击(Double Spending)[13]等。文献[15-16]研究发现,通过攻击 Bitcoin[14]的内存池来增加合法用户的交易成本,达到 DDoS 攻击的目的。Zheng 等[17]提出当矿池规模相对较大时可对其他矿池发起 DDoS 攻击。文献[18]中指出,区块链网络面临 DDoS 攻击,在 Bitcoin 网络中 51% 攻击也能够诱发 DDoS 攻击,当矿池拥有足够的算力时能够阻止其他矿工获得区块的记账权。还有不少研究者将区块链技术应用于 DDoS 攻击的防御,缓解 DDoS 攻击对应用系统的压力[19-20],多应用于物联网技术领域。

据上述分析,区块链网络 DDoS 攻击的来源可能是多种攻击手段,例如攻击者先采用日食攻击或女巫攻击控制一定数量的对等节点,然后通过这些受控节点在区块链网络中发起 DDoS 攻击。DDoS 攻击也可能来源于其他途径,例如对等节点本身资源受限、负载过重、离线、不诚信等,或者遭到其他恶意代码的攻击,使得自身服务能力下降。因此,区块链网络仍然存在 DDoS 攻击的潜在风险,有必要研究区块链网络 DDoS 攻击的特征、破坏性等问题,为抵御 DDoS 攻击、评估区块链网络运行状况提供依据。

为此,本文提出一种区块链网络 DDoS 攻击模型,研究对等节点可能发生的攻击行为和攻击事件,分析区块链网络 DDoS 攻击的特征,评估 DDoS 攻击对区块链网络服务可能造成的影响及程度,并为下一步研究检测、防范 DDoS 攻击的方法、路线提供必要的参考建议。

1　相关技术

1.1　区块链

普遍认可的区块链类型包括公有链、联盟链和私有链。公有链一般是指对等节点可以自由加入或退出,自由交易并参与交易共识,没有固定的身份认证机构的区块链,典型应用平台有 Bitcoin[14]、Ethereum[21]等。公有链的去中心化程度最高。

联盟链,又称行业链,通常由行业或群体发起构建并指定若干对等节点共同参与交易共识,其他对等节点存储完整的账本数据库,需要设置身份认证机构,联盟链的去中心化程度次之,典型应用平台有 Hyperledger Fabric[22]。

私有链通常为一个小团队或个人所有,采用公有链或联盟链应用平台的部分技术构建私有链应用环境,网络结构和用户相对固定,典型应用平台有 BlockBench[23]。

1.2　Hyperledger Fabric

Hyperledger Fabric[22]是一个联盟链基础软件平台,每个通道(Channel)对应一个独立的账本数据库,通道内的成员划分成若干个组织(Org),每个对等节点(Peer)可以加入到 1 个或多个通道中,每个通道有 1 个特殊的排序组织(Orderer Org),排序节点(Orderer)负责将已共识的交易(Transaction)打包成区块。Fabric 智能合约称为链码(Chain Code,CC),安装在通道及对等节点上,Peer 调用链码函数即产生待共识的交易,仅安装了相应链码的 Peer 才能参与共识该链码函数产生的交易。Fabric 的缺省共识策略是,通道中 50% 以上组织且每个组织至少 1 个 Peer 节点确认交易的有效性,因此在图 1 所示 Fabric 网络中 Org1 的 peer1、Org2 的 peer2 能够共识 1 笔交易,但 Org1 的 peer3、Org3 的 peer1 不能共识交易,原因是 Org1 的 peer3 没有安装 CC,不能参与共识。

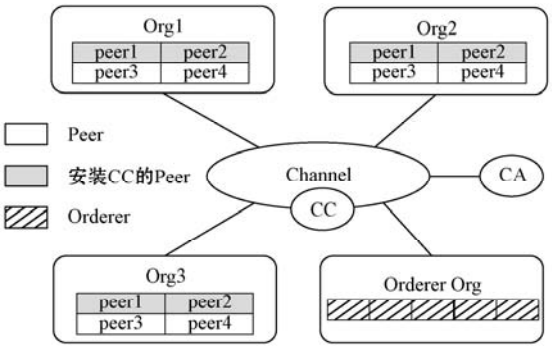

图 1　Fabric 网络

2　区块链网络 DDoS 攻击模型

2.1　基本定义

区块链网络在拓扑结构上表现为 P2P 网络,网

络中的节点通常需要提供 2 种服务:交易共识和交易查询。交易共识是指节点参与新交易的验证、对新交易达成一致与共识的服务,即交易背书服务。交易查询是指节点响应查询请求,在本地账本中查询并反馈历史交易的服务,通常用于历史交易验证与溯源。交易共识和交易查询是区块链网络 DDoS 攻击的主要对象,攻击者可以通过一种或多种攻击行为发起 DDoS 攻击。为方便阐述,本文首先建立如下定义。

定义 1 DDoS 攻击行为,区块链网络的节点在提供共识与查询服务时有意或无意地存在下述一种或多种行为。

(1) 延时响应服务。节点由于资源受限或有意拖延,交易成功但导致交易完成时间滞后,耗时增大,系统吞吐量下降。

(2) 蓄意阻止服务。节点有意破坏、阻止共识进程,例如篡改交易的内容或使用无效的数字证书等,阻止交易完成,导致交易失效。

(3) 忽略服务请示。节点有意忽略共识或查询服务请求,拒绝提供服务,导致交易失败。

(4) 离线。承担着共识与查询义务的节点脱离区块链网络,导致交易因超时而失败,服务耗时增大。

定义 2 正常节点,是指正常履行交易共识、交易查询职责并提供相应服务,不存在定义 1 所述 DDoS 攻击行为的节点。

定义 3 失信节点,是指有意或无意地发生一种或多种 DDoS 攻击行为的节点。日食攻击或女巫攻击的受控节点可能成为失信节点。

定义 4 交易无效,是指失信节点成功地执行攻击行为,交易写入区块但被标注为无效。无效的交易将同步到所有节点。

定义 5 交易失败,是指失信节点成功地执行攻击行为,交易数据没有写入区块。失败的交易不会同步到其他节点。

定义 6 区块链网络 DDoS 攻击模型,是指区块链网络中失信节点有意或无意地发生定义 1 所述攻击行为的一种或多种组合,从而导致交易时间延长、交易无效或失败、网络服务性能下降,甚至无法正常提供交易共识与查询服务。

根据定义 1 和定义 6 可知,失信节点实施的攻击行为可列为表 1 所示的 6 种攻击事件,各攻击事件之间是相互独立的事件。

表 1 攻击事件

事件	攻击行为组合	后果
1	1	交易成功但延时
2	1,2	交易无效
3	1,3	交易失败
4	2	交易无效
5	3	交易失败
6	4	交易失败

2.2 DDoS 攻击的评价

设区块链网络正常节点的数量为 m,失信节点的数量为 n,完成一次交易至少需要 k 个节点提供背书服务。设定 k 个节点中只要有 1 个节点发生了表 1 所示攻击事件 2 - 事件 6 之一,该交易无效或失败;只要攻击事件包含攻击行为 1 或 4,交易耗时增大,交易吞吐量下降。设 1 次交易的正常耗时为 t,攻击行为 1 和 4 导致的延时为 Δt,交易总数为 T。无效或失败的交易总数 T_F 如式(1)所示,服务延时总量 D 如式(2)所示。为评价 DDoS 攻击对区块链的破坏性,建立 2 个定义。

定义 7 交易失败率,是无效或失败的交易数 T_F 在交易总数 T 中的比率,用 F_T 表示。

定义 8 交易延时比,是指服务延时总量 D 与相同交易数量的正常耗时之间的比值,用 F_D 表示。

定义 6 所述的 DDoS 攻击模型对区块链网络的性能影响用式(3)所示的 F_T、F_D 来评价,其中 F_T 刻画了 DDoS 攻击对交易吞吐量造成的破坏,F_D 刻画了 DDoS 攻击对服务延时造成的影响。

$$T_F = \frac{5}{6}\left(1 - \frac{C_m^k}{C_{m+n}^k}\right)T \tag{1}$$

$$D = \frac{2}{3}\Delta t\left(1 - \frac{C_m^k}{C_{m+n}^k}\right)T - tT \tag{2}$$

$$\begin{aligned} F_T &= \frac{T_F}{T} = \frac{5}{6}\left(1 - \frac{C_m^k}{C_{m+n}^k}\right) \\ &\lim_{n\to+\infty,m\to0} F_T = \frac{5}{6} \\ F_D &= \frac{D}{tT} = \frac{2\Delta t}{3t}\left(1 - \frac{C_m^k}{C_{m+n}^k}\right) - 1 \\ &\lim_{n\to+\infty,m\to0} F_D = \frac{2\Delta t}{3t} - 1 \end{aligned} \tag{3}$$

2.3 DDoS 攻击的特征

在定义 6 所述的模型中,失信节点分布在区块链网络中,呈现分布式攻击特征,攻击的目标是区块链网络的服务性能,使之性能降低或者局部网络失去正常

服务的能力。此外,区块链网络 DDoS 攻击模型还具有下述特征。

(1) 攻击门槛低。只要接收到交易共识或查询请求,任何 1 个失信节点都可以单独地,或者与其他失信节点一起发起 DDoS 攻击。正常节点在资源耗尽或遭受恶意程序攻击时,也可能转变为失信节点。

(2) 不必形成合谋。发起 DDoS 攻击时,失信节点不必像合谋攻击那样事先达成同盟并伪造账本,彼此之间不必相互协同,甚至失信节点之间可能完全相互隔离。

(3) 破坏性相对小。少量失信节点的 DDoS 攻击行为给区块链网络造成的影响是较小的,数量庞大的失信节点可能导致区块链服务中断,但网络服务仍可恢复,不至于整个网络被劫持。

(4) 攻击者来源多样化。日食攻击[11]、女巫攻击[12]、51% 攻击[18]能够劫持正常节点成为失信节点。正常节点在资源受限、负载过重、自私不诚信或者遭受其他恶意代码攻击时也会出现部分 DDoS 攻击行为。

3　实验与对比分析

Hyperledger Fabric 的 Peer 节点安装用户链码访问区块链数据,Peer 节点都安装有系统链码 QSCC(Query System Chaincode)[22],用于查询历史区块数据,因此任何 Peer 节点都能够提供历史交易查询服务。本文以 Hyperledger Fabric 为平台搭建区块链应用环境,并实施区块链网络 DDoS 攻击。

3.1　实验环境

在 Hyperledger Fabric V2.2 上创建 1 个通道(Channel),包括 1 个排序组织和 5 个节点组织,排序组织包括 5 个 Orderer 节点,每个节点组织包括 10 个 Peer 节点。在通道内安装 1 个用户链码 CC1 并提供接口函数供 Peer 节点调用,50 个 Peer 节点安装 CC1,因此每个 Peer 节点均可提供交易共识和查询服务。通道的共识策略是 Fabric 缺省共识策略,因此对于任意交易,至少需要 3 个 Peer 节点提供共识或查询服务且这 3 个 Peer 节点来自不同的节点组织。本文实验的做法是:首先从 5 个节点组织中随机选择 3 个,然后分别从这 3 个节点组织中随机选择 1 个 Peer 节点作为服务节点。

在实现方式上,采用 Docker 容器[24]实施上述 Orderer 节点和 Peer 节点。在 Fabric 的基础上修改 Peer 源码,使之在提供服务时发起表 1 所述的攻击事件,将修改后的 Peer 封装成新的 Docker 镜像,称之为 SelfPeer。在 50 个 Peer 节点中设置不同数量的 SelfPeer 节点,即定义 3 所述的失信节点。实验的网络环境见图 2 所示。

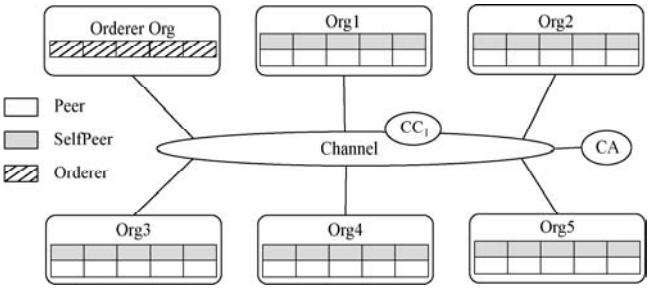

图 2　实验的网络环境

3.2　DDoS 攻击分组实验

3.2.1　实验方案

本部分实验设置 6 组实验方案,正常节点数量 m、失信节点数量 n 以及提供共识、查询服务的节点数量 k 见表 2 所示。表 2 中的“离线”表示发起攻击行为 4 的失信节点数量,“在线”表示发起攻击行为 1 – 3 的失信节点数量。在表 2 所示分组方案中“离线”与“在线”保持 1∶5的数量关系,使得表 1 所示的攻击事件以等概率发生,“占比”表示 $n/(m+n)$。方案 A 的失信节点数量 n 为 0,表示正常情况下的实验方案,与其他方案进行对比分析。

表 2　DDoS 攻击的分组实验

分组	m	n(SelfPeer)		k	占比/%
		在线	离线		
A	50	0	0	3	0
B	44	5	1	3	12
C	38	10	2	3	24
D	32	15	3	3	36
E	26	20	4	3	48
F	20	25	5	3	60

攻击行为 1 的延时设为 3 秒,对每个分组实验,同时启动 10 个线程,每个线程持续运行 10 分钟,不间断地调用 CC_1 的接口函数并产生新交易,记录每个交易的完成状态(成功、无效或失败)以及耗时,统计各状态的交易总量。

3.2.2　分组对比分析

表 2 所示 6 种分组的实验结果如表 3 所示。其中 F_T 是同一实验分组中无效/失败的交易数与交易总量之间的比值,F_D 是指按时间排列的前 3 500 次交易总量里,分组 A 耗时 278 秒作为基准,其他 5 个分组完成相同数量交易的总耗时按式(3)的计算结果,描述了

不同实验分组完成相同的交易量所需要的时间。

表 3 DDoS 攻击对性能的影响

分组	总交易量	无效/失败交易量	平均耗时/s	性能影响	
				F_T/%	F_D/%
A	7 674	207	0.54	2.7	—
B	7 659	2 331	0.71	30.4	-2.9
C	5 399	2 865	1.08	53.1	42.1
D	4 463	3 050	1.32	68.3	69.4
E	3 938	3 197	1.50	81.2	92.4
F	3 771	3 272	1.57	86.8	99.3

A 组出现了少量的无效/失败交易，原因是 CC_1 函数调用过于频繁，交易量过大造成节点负载过重，导致部分交易因超时而失败。B 组的少量节点发起延时攻击，反而缓解了 A 组的节点负载压力，表现为 F_D 指标略有改善，但是 F_T 增大。C－F 组的失信节点逐渐增多，DDoS 攻击的影响逐渐显现，F_T、F_D 明显增大，F_T 逐渐逼近式(3)F_T 的极限，F 组的 F_T 已超过式(3)的极限，其原因是压力测试造成负载过重(例如 A 组的 $F_T=2.7\%$)。按 $t=0.54$ s、$\Delta t=3$ s 计算，式(3)$F_{的}$ 极限是 270%，表 3 各分组的 F_D 逐渐逼近式(3)的 F_D 极限，交易平均耗时上升。

6 组实验完成相同交易量(前 3 500 次交易)所需耗时如图 3 所示。A 组与 B 组的耗时相差不大，C－F 组的失信节点逐渐增多，遭受延时攻击的交易数量增多，说明 DDoS 攻击对区块链服务的延时影响愈加明显，降低了区块链网络的交易吞吐量，服务性能下降。

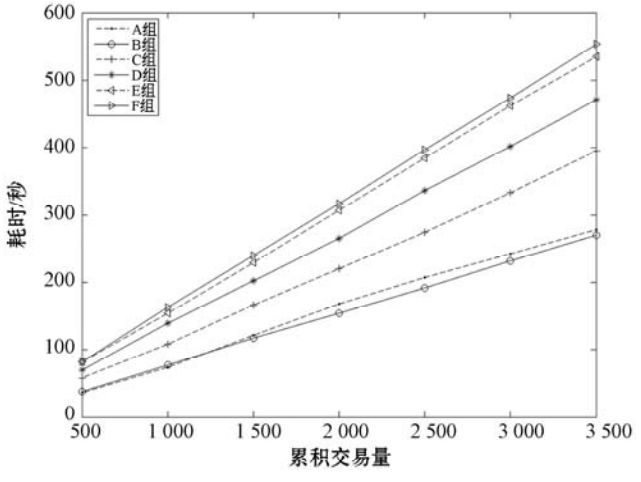

图 3 相同交易量的耗时

6 组实验的单次交易耗时分布见图 4 所示。A 组的大部分交易在 1 秒内完成；B－F 组在 1 秒内完成的交易数量逐渐减少，在 3～4 秒间完成的交易数量逐渐增多，说明 DDoS 攻击对交易的延时影响非常明显，对网络吞吐量及系统性能影响显著。

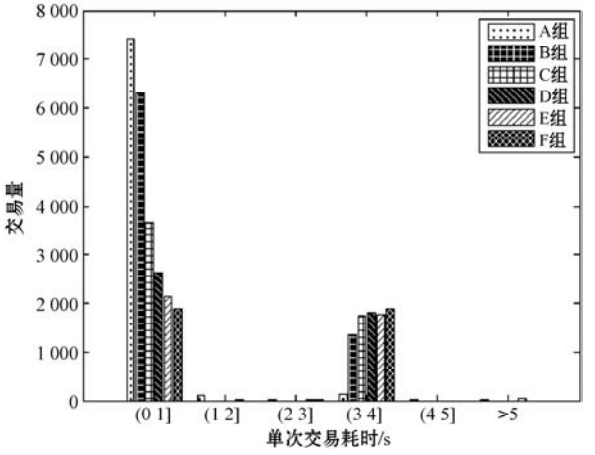

图 4 单次交易耗时分布

综合分析本部分的实验数据及结果，区块链网络存在 DDoS 攻击安全隐患，失信节点不仅能够造成区块链交易无效或失败，给交易共识造成障碍，还能够延迟交易共识的完成时间，对区块链的交易吞吐量、系统性能造成严重影响。失信节点占比较小时(B、C、D 组占比低于 PoW 共识算法的容错门限 51%[14]以及 PBFT 共识算法的容错门限 33%[25])仍能发起 DDoS 攻击且具有破坏性。

3.3 DDoS 攻击过程仿真实验

3.3.1 实验方案

本部分实验的目的是仿真区块链网络 DDoS 攻击从开始到结束的全过程，并与正常情况($n=0$，表 2 的 A 组实验)的网络性能进行对比。为此，设置 DDoS 攻击持续 10 分钟，攻击过程各时刻失信节点数量用式(4)计算，其中 $f'(x)$ 服从高斯分布 $N(5,4)$ 和均匀分布 $U[-3,3]$，$f(x)$ 约束 $f'(x)$ 使其在[0 40]上取值，表示不同时刻失信节点的累积数量，如图 5 所示。

$$f'(x)=[40\times e^{-(x-5)^2/8}]+[U[-3,3]]$$
$$f(x)=\begin{cases}f'(x) & f'(x)\geqslant 0\\ 0 & f'(x)<0\end{cases} \tag{4}$$
$$x=0,1,2,\cdots,10$$

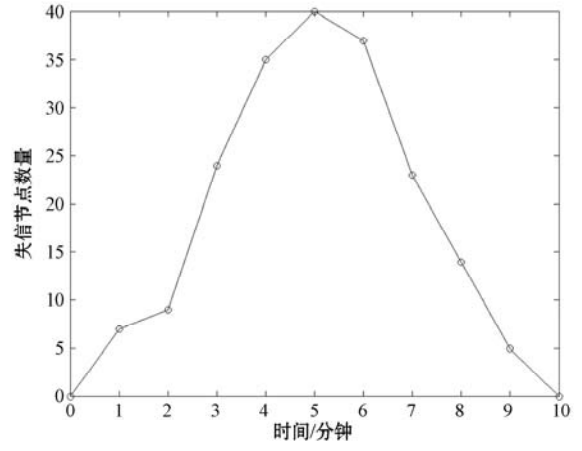

图 5 攻击过程的失信节点数量分布

实验方案是:同时启动 10 个线程不间断产生新交易并且持续 20 分钟。前若干分钟按表 2 的 A 组实验设置进行,中间按照图 5 在不同时刻设置失信节点发起 DDoS 攻击并持续 10 分钟左右,最后若干分钟再重复表 2 的 A 组实验。

3.3.2　实验数据分析

整个实验的总交易量及无效/失败交易量随时间的分布如图 6 所示。实验的前 6 分钟是表 2 的 A 组实验数据,每分钟交易量维持在 800 次左右,没有无效或失败的交易。自第 7 分钟开始到第 16 分钟是 DDoS 攻击的全过程,区块链网络的每分钟交易量显著下降,无效/失败交易量明显上升,在第 11 分钟各自达到极值,这个时刻区块链网络的失信节点数量最大,与图 5 的失信节点数量分布相吻合。自第 16 分钟到实验结束,区块链网络恢复正常,每分钟的正常交易量恢复到实验开始的状况。

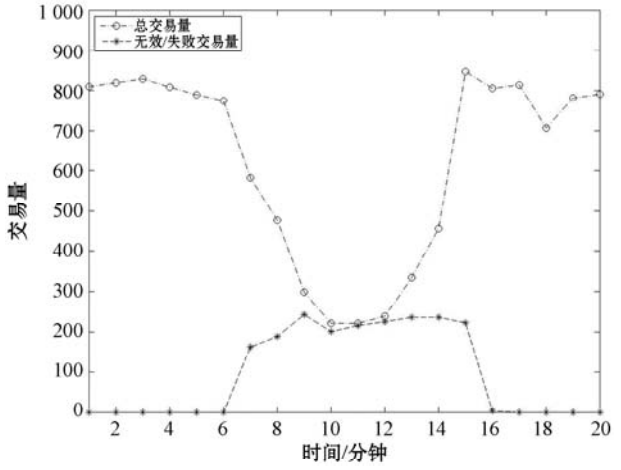

图 6　攻击过程的交易量

图 6 所示的实验结果反映出,DDoS 攻击对区块链网络的性能具有破坏性。在 DDoS 攻击开始的前 2 分钟,失信节点数量分别是 7 和 9,占比仅为 14% 和 18%,从图 6 第 7、8 分钟可以看出,此时区块链网络的性能下降非常明显。这说明,即使恶意节点数量少于 PoW 共识的容错门限 51%[14] 或者 PBFT 共识的容错门限 33%[25],仍能发起 DDoS 攻击并造成破坏。

在图 6 的第 11 分钟,失信节点占比为 80%,此时基本上已不能达成交易共识,随后失信节点数量减少,区块链网络性能恢复正常,说明遭受 DDoS 攻击的区块链网络仍可以恢复。

攻击过程中单次交易的平均耗时随时间分布如图 7 所示。自 DDoS 攻击开始(第 7 分钟),单次交易的平均耗时明显增加,第 11 分钟到达峰值,自第 16 分钟回归正常。图 7 数据表明,失信节点占比为 14% 和 18%(第 7、8 分钟)时,平均耗时明显增加,说明即使少量的恶意节点发起 DDoS 攻击,也能对交易共识所需时间造成影响。DDoS 攻击结束后,单次交易平均耗时也能恢复正常。

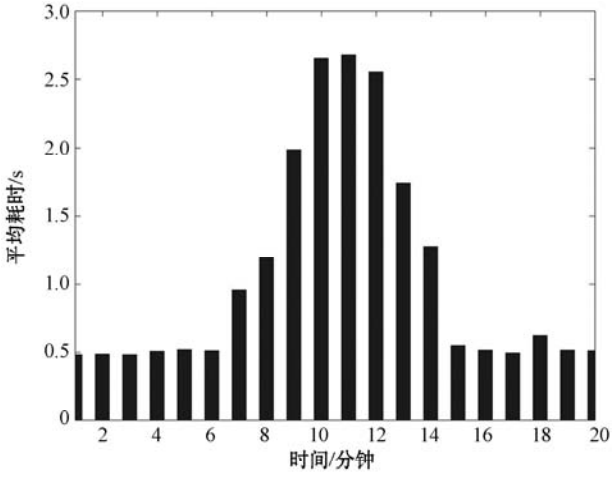

图 7　攻击过程的单次交易平均耗时

在 DDoS 攻击的全过程中,影响评价指标 F_T、F_D 如图 8 所示。从第 6 秒开始 F_T 逐渐增大,失败或无效交易量的比例越来越大。一方面,DDoS 攻击造成性能影响,另一方面,实验环境面临高强度测试压力,两方面因素叠加,致使 F_T、F_D 在第 11 分钟达到峰值,此时失信节点占比达到 80%,整个区块链网络濒临瘫痪。第 12 分钟开始区块链网络性能逐渐恢复,F_T、F_D 逐渐回归到攻击前的状态。

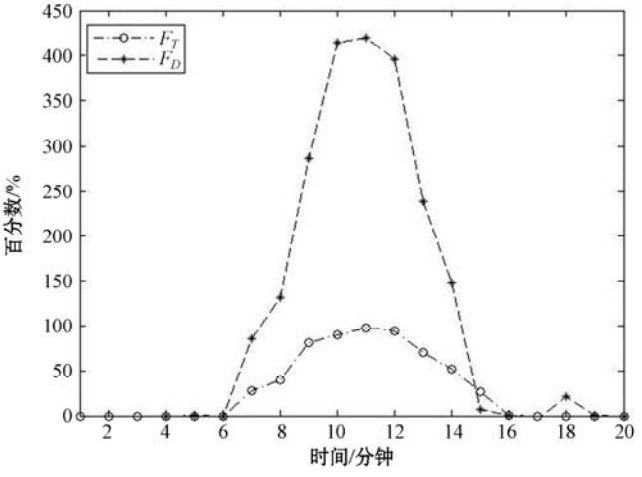

图 8　DDoS 攻击对性能的影响

3.4　实验小结

本节两部分实验数据及对比分析表明,区块链网络存在 DDoS 攻击的安全隐患,即使少量的恶意节点仍能对区块链网络性能造成破坏,攻击严重时会造成交易共识受阻,交易结束时间延长,网络服务的吞吐量下降,攻击停止后区块链网络服务能够恢复正常。3.3 节实验也表明了一种检测 DDoS 攻击区块链网络的思路,即实时监测区块链网络的运行性能,发现服务性能异常点。

日食攻击或女巫攻击控制区块链网络对等节点，利用受控节点进一步发起其他攻击行为，包括 DDoS 攻击。因此，当检测到 DDoS 攻击时，区块链网络可能还隐藏着日食攻击等其他攻击行为。本文实验为抵御其他攻击手段提供参考价值。

DDoS 攻击者的来源也可能是资源受限、负载过重或者自私、不诚实的节点，这些节点共享了区块链服务资源，但不能尽职履行职责。为维护区块链网络的公平和信任，需要检测这些失信节点。

4 结 语

本文从区块链网络安全角度出发，提出了一种 DDoS 攻击模型，在 Hyperledger Fabric 联盟链平台上仿真了 DDoS 对区块链网络的攻击。由于 DDoS 攻击区块链网络的门槛低，攻击者之间不必相互协同，又能够破坏区块链的服务性能，因此在区块链规模化应用时，还需要进一步研究 DDoS 攻击的应对之策。为防范 DDoS 攻击区块链网络，本文为后续研究工作揭示了 2 种可能的研究方向：(1) 通过防范日食攻击、女巫攻击等攻击手段，防范攻击者控制区块链网络的对等节点，是防范 DDoS 攻击的途径之一；(2) 对区块链网络的运行状况进行实时监测，发现区块链网络运行性能的异常情况，监测对等节点的网络行为，发现存在性能瓶颈的节点以及自私、不诚信的节点，并对整个区块链网络的服务性能及安全态势做出科学准确的评价。

参 考 文 献

[1] Prasad K M, Reddy A R M, Rao K V. DoS and DDoS attacks: Defense, detection and traceback mechanisms—A survey[J]. Global Journal of Computer Science and Technology: E Network, Web & Security, 2014, 14(7): 15 - 32.

[2] Mahjabin1 T, Xiao Y, Sun G, et al. A survey of distributed denial-of-service attack, prevention, and mitigation techniques[J]. International Journal of Distributed Sensor Networks, 2017, 13(12): 1 - 33.

[3] Mallikarjunan K N, Muthupriya K, Shalinie S M. A survey of distributed denial of service attack[C]//10th International Conference on Intelligent Systems and Control, 2016: 1 - 6.

[4] Somani G, Gaur M S, Sanghi D, et al. DDoS attacks in cloud computing: Issues, taxonomy, and future directions [J]. Computer Communications, 2017, 107: 30 - 48.

[5] Arış A, Oktuğ S F, Voigt T. Security of internet of things for a reliable internet of services[J]. Autonomous Control for a Reliable Internet of Services, 2018, 10768: 337 - 370.

[6] Wang C. The 2016 Dyn attack and its lessons for IoT security [EB/OL]. [2021 - 05 - 19]. https://mse238blog.stanford.edu/2018/07/clairemw/the-2016-dyn-attack-and-its-lessons-for-iot-security/.

[7] Varghese S. Github hit by biggest ever DDOS attack at 1.35 TBPS[J]. Exchange, 2018(5): 8.

[8] 于戈，聂铁铮，李晓华，等. 区块链系统中的分布式数据管理技术—挑战与展望[J]. 计算机学报，2019，42(116)：28 - 53.

[9] 江沛佩，王骞，陈艳姣，等. 区块链网络安全保障：攻击与防御[J]. 通信学报，2021，42(1)：151 - 162.

[10] Li X Q, Jiang P, Chen T, et al. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107(6): 841 - 853.

[11] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on Bitcoin's peer-to-peer network[C]//24th USENIX Security Symposium, 2015: 129 - 144.

[12] Douceur J R. The sybil attack[C]//1st International Workshop on Peer-to-Peer Systems, 2002: 251 - 260.

[13] Zhang S J, Lee J H. Double-spending with a sybil attack in the Bitcoin decentralized network[J]. IEEE Transactions on Industrial Informatics, 2019, 15(10): 5715 - 5722.

[14] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2021 - 05 - 19]. https://bitcoin.org/en/bitcoin-paper.

[15] Saad M, Njilla L, Kamhoua C, et al. Mempool optimization for defending against DDoS attacks in PoW-based blockchain systems[C]//IEEE International Conference on Blockchain and Cryptocurrency, 2019: 285 - 292.

[16] Saad M, Thai M T, Mohaisen A. POSTER: Deterring DDoS attacks on blockchain-based cryptocurrencies through mempool optimization[C]//Asia Conference on Computer and Communications Security, 2018: 809 - 811.

[17] Zheng R, Ying C, Shao J, et al. New game—Theoretic analysis of DDoS attacks against Bitcoin mining pools with defence cost[J]. Network and System Security, 2019: 567 - 580.

[18] Saad M, Spaulding J, Njilla L. Exploring the attack surface of blockchain: A systematic overview[EB]. arXiv: 1904.03487, 2019.

[19] Singh R, Tanwar S, Sharma T P. Utilization of blockchain for mitigating the distributed denial of service attacks[J]. Security and Privacy, 2020, 3(3): 1 - 13.

[20] 周启惠，邓祖强，邹萍，等. 基于区块链的防护物联网设备 DDoS 攻击方法[J]. 应用科学学报，2019，37(2)：213 - 223.

[21] Ethereum. Ethereum development document [EB/OL]. [2021 - 05 - 19]. https://ethereum.org/en/developers/docs/.

[22] Read the Docs. A blockchain platform for the enterprise [EB/OL]. [2021 - 05 - 19]. https://hyperledger-fabric.readthedocs.io/en/release-2.2/index.html.

(下转第 392 页)

图 7 – 图 10 均说明四个微博传播预测模型在用户活跃度高的时刻以及数据集数量多的时刻效果更好。与其他三个模型相比,本文模型的召回率不会随着时刻的变化出现较大波动,说明本文模型不会随着时间、微博用户活跃情况和数据集的变化而产生较大变化,模型稳定性较好,模型能够在小数量的训练集上获得较好的效果并且模型随着训练集的增大效果随之增加。

单独对指定微博话题进行微博传播预测,可以验证实验模型在指定话题中的预测准确性,衡量模型实用性如何。如图 11 所示,本文随机选定五个微博话题#春晚#、#生日快乐#、#立冬#、#医保新政策#、#期末#,用四个模型对五个话题进行微博传播预测实验,比较四个模型的准确率。

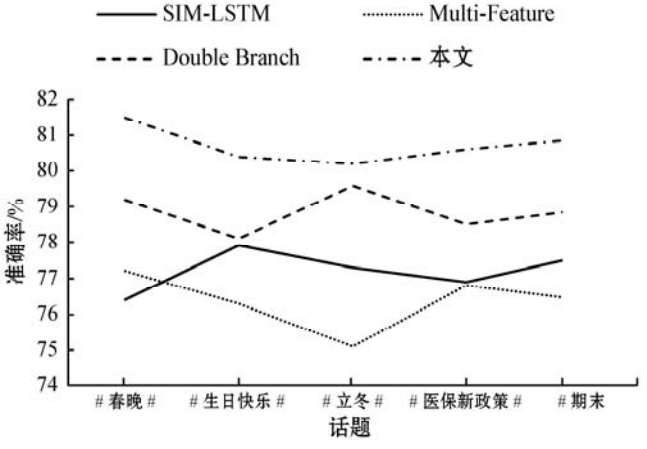

图 11 指定话题模型准确率对比

可以看出,不同模型在不同微博话题中的预测准确率有所差异,但本文所用的基于三分支神经网络的多特征微博传播预测模型在五个不同话题中的预测准确率均高于其他三个模型,说明本文所用模型在单个话题中的预测效果依旧良好,模型稳定且效率高。

通过对整体数据集进行实验,对不同时刻、不同话题的部分数据集进行实验,发现本文模型在准确率、召回率和 F1 值上均高于其他三个模型,模型的稳定性高,性能良好。

3 结 语

本文提出的基于三分支神经网络的多特征微博传播预测模型经过实验验证,其准确率、召回率、F1 值均高于其他模型,该模型具有较高稳定性,在微博传播预测准确度上有了显著提高。但本文在研究过程中没有充分考虑“微博粉丝控评”即某些名人或者微博用户的忠实粉丝会对这些名人和微博用户进行大量重复的转发、评论,从而对微博转发预测的真实效果产生一定影响。今后的研究工作会围绕上述问题展开。

参 考 文 献

[1] 刘超,姚耿,杨宏雨. 基于微博关注网络的转发预测算法研究[J]. 数字技术与应用,2020,38(7):121 – 124.
[2] 陈振春,刘学军,李斌. 基于内容和信任度的舆情扩散研究[J]. 计算机应用与软件,2017,34(10):59 – 65.
[3] 曾辉,淦修修,彭俊,等. 基于双分支结构的融合多特征微博传播行为预测算法[J]. 科学技术与工程,2020,20(26):10822 – 10828.
[4] 孙红,左腾. 基于 PageRank 的微博用户影响力算法研究[J]. 计算机应用研究,2018,35(4):1028 – 1032.
[5] 毛国君,谢松燕,胡殿军. PageRank 模型的改进及微博用户影响力挖掘算法[J]. 计算机应用与软件,2017,34(5):28 – 32,37.
[6] 李勇. 一种改进的微博用户影响力分析算法[J]. 计算机技术与发展,2020,30(8):27 – 33.
[7] 刘玮,贺敏,王丽宏,等. 基于用户行为特征的微博转发预测研究[J]. 计算机学报,2016,39(10):1992 – 2006.
[8] Deng X, Wu W, Wang F. Deep metric learning for text data based on triplet network[J]. IOP Conference Series: Materials Science and Engineering,2020,806:218927660.
[9] He G, Li F, Wang Q, et al. A hierarchical sampling based triplet network for fine-grained image classification[J]. Pattern Recognition,2021,115:107889.
[10] Hoffer E, Ailon N. Deep metric learning using triplet network[C]//International Workshop on Similarity-based Pattern Recognition,2015.
[11] Bhople A R, Prakash S. Learning similarity and dissimilarity in 3D faces with triplet network[J]. Multimedia Tools and Applications,2021,80:35973 – 35991.
[12] Li Y, Chen Y, Wang N, et al. Scale-aware trident networks for object detection[C]//2019 IEEE/CVF International Conference on Computer Vision (ICCV),2019.
[13] 穆圣坤,张路桥,滕彩峰. 基于循环神经网络的微博转发行为预测[J]. 计算机系统应用,2019,28(8):155 – 161.
[14] 王志峰,冯锡炜,贾强,等. 多特征神经网络微博转发预测[J]. 辽宁石油化工大学学报,2017,37(6):47 – 50.
[15] 王绍卿,李翠平,王征,等. 基于多重信任关系的微博转发行为预测[J]. 清华大学学报(自然科学版),2019,59(4):270 – 275.

(上接第 372 页)

[23] GitHub. BlockBench[EB/OL]. [2021 – 05 – 19]. https://github.com/ooibc88/blockbench.
[24] GitHub. Docker-library[EB/OL]. [2021 – 04 – 27]. https://github.com/docker-library.
[25] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transaction on Computer Systems,2002,20(4):398 – 461.