(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 6 月 23 日 (23.06.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/127342 A1

(51) 国际专利分类号:
H04L 67/01 (2022.01) *G06K 9/62* (2022.01)

(21) 国际申请号: PCT/CN2021/124772

(22) 国际申请日: 2021 年 10 月 19 日 (19.10.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

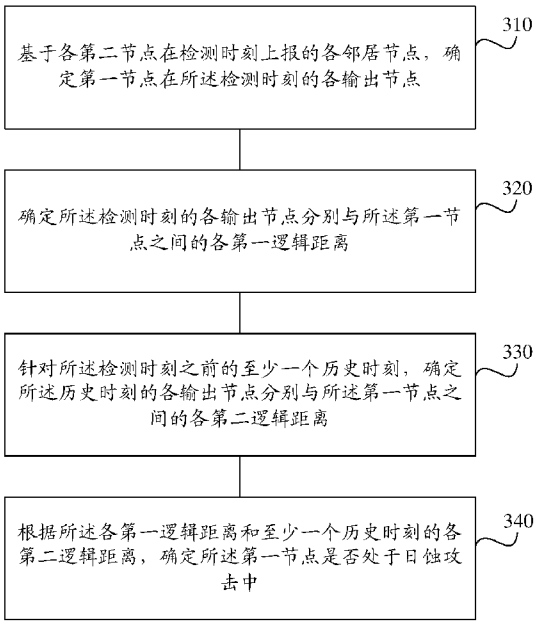
(30) 优先权:
202011486985.5 2020年12月16日 (16.12.2020) CN

(71) 申请人: 深圳前海微众银行股份有限公司 (**WEBANK CO., LTD.**) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 北京邮电大学 (**BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS**) [CN/CN]; 中国北京市海淀区西土城路10号, Beijing 100876 (CN)。

(72) 发明人: 刘杨 (**LIU, Yang**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 常庆安 (**CHANG, Qingan**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 彭木根 (**PENG, Mugen**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 关建峰 (**GUAN, Jianfeng**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 陈宇杰 (**CHEN, Yujie**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 李辉忠 (**LI, Huizhong**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 张开

(54) **Title:** METHOD AND DEVICE FOR DETECTING ECLIPSE ATTACK FOR BLOCKCHAIN

(54) 发明名称: 一种区块链日蚀攻击检测的方法及装置



310 DETERMINE EACH OUTPUT NODE OF A FIRST NODE AT THE DETECTION MOMENT ON THE BASIS OF EACH NEIGHBOR NODE REPORTED BY EACH SECOND NODE AT THE DETECTION MOMENT
320 DETERMINE EACH FIRST LOGICAL DISTANCE BETWEEN EACH OUTPUT NODE AT THE DETECTION MOMENT AND THE FIRST NODE
330 DETERMINE, FOR AT LEAST ONE HISTORICAL MOMENT EARLIER THAN THE DETECTION MOMENT, EACH SECOND LOGICAL DISTANCE BETWEEN EACH OUTPUT NODE AT THE HISTORICAL MOMENT AND THE FIRST NODE
340 DETERMINE, ACCORDING TO EACH FIRST LOGICAL DISTANCE AND EACH SECOND LOGICAL DISTANCE AT THE AT LEAST ONE HISTORICAL MOMENT, WHETHER THE FIRST NODE IS SUBJECTED TO AN ECLIPSE ATTACK

图 3

(57) **Abstract:** Disclosed are a method and device for detecting an eclipse attack for a blockchain. The method comprises: determining each output node of a first node at the detection moment on the basis of each neighbor node reported by each second node at the detection moment, each second node being a node in a distributed routing table of the first node, and each neighbor node being a node in a distributed routing table of the second node; and then determining each first logical distance between each output node at the detection moment and the first node; determining, for at least one historical moment earlier than the detection moment, each second

WO 2022/127342 A1

[见续页]

翔(ZHANG, Kaixiang)；中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 范瑞彬(FAN, Ruibin)；中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 李成博(LI, Chengbo)；中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。

(74) 代理人：北京同达信恒知识产权代理有限公司(TDIP & PARTNERS)；中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

logical distance between each output node at the historical moment and the first node; and determining, according to each first logical distance and each second logical distance at the at least one historical moment, whether the first node is subjected to an eclipse attack. In this way, the real-time performance and initiative of the non-restart type eclipse attack detection at the detection moment are improved, and the attack mode of the non-restart type eclipse attack is detected.

(57) 摘要：本发明公开了一种区块链日蚀攻击检测的方法及装置，包括：基于各第二节点在检测时刻上报的各邻居节点，确定第一节点在检测时刻的各输出节点，其中，各第二节点为第一节点的分布式路由表中的节点，各邻居节点为第二节点的分布式路由表中的节点，然后确定检测时刻的各输出节点分别与第一节点之间的各第一逻辑距离，针对检测时刻之前的至少一个历史时刻，确定历史时刻的各输出节点分别与第一节点之间的各第二逻辑距离，再根据各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定第一节点是否处于日蚀攻击中。以此增加在检测时刻对无重启式的日蚀攻击检测的实时性与主动性，且针对无重启式日蚀攻击的攻击方式进行检测。

一种区块链日蚀攻击检测的方法及装置

相关申请的交叉引用

本申请要求在2020年12月16日提交中国专利局、申请号为202011486985.5、申请名称为“一种区块链日蚀攻击检测的方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及金融科技（Fintech）领域，尤其涉及一种区块链日蚀攻击检测的方法及装置。

背景技术

随着计算机技术的发展，越来越多的技术（例如：区块链、云计算或大数据）应用在金融领域，传统金融业正在逐步向金融科技转变，大数据技术也不例外，但由于金融、支付行业的安全性、实时性要求，也对大数据技术提出的更高的要求。

日蚀攻击是针对区块链系统的一种攻击手段，攻击者通过日蚀攻击使得受害者节点进行重启，并将受害者节点中的路由表清空，然后通过控制特定节点（如恶意节点）对受害者节点进行信息的访问，以使受害者节点的路由表中存在的都是特定节点，使其只能接收攻击者的信息且将反馈信息发送至攻击者，从而使受害者节点无法查看真实的区块链系统的信息，导致受害者节点与区块链系统产生分裂，进而使攻击者可以使用少于 51% 的算力对区块链系统发起 51% 攻击，导致区块链系统存在安全隐患。

现有技术中，为了防御重启式日蚀攻击，通过随机森林算法对日蚀攻击进行检测。具体的，通过随机森林算法离线收集其他正常节点在各自路由表中确定的邻居节点构建随机决策森林，再根据随机决策森林收集受害者节点的在路由表中确定的多个邻居节点（特定节点），进而对受害者节点进行检测。

然而，日蚀攻击的方式包括多种，其中包括不需要使受害者节点重启也可以实现日蚀攻击，即无重启式日蚀攻击。具体的，通过与受害者节点保持频繁的数据通信，使特定节点逐步插入至受害者节点的输出节点列表中，以此入侵运行平稳的受害者节点，无需将受害者节点的路由表都存储特定节点，实现无重启式日蚀攻击，但随机森林算法只能针对路由表均为特定节点的受害者节点检测出日蚀攻击，因此随机森林算法无法检测出无重启式日蚀攻击，且随机森林算法需要离线进行检测，其实时性与主动性低。

因此，现需要一种日蚀攻击检测的方法，以检测无重启式日蚀攻击，增加对日蚀攻击检测的实时性与主动性。

发明内容

本发明实施例提供一种区块链日蚀攻击检测的方法及装置，用于检测无

重启式的日蚀攻击，增加对日蚀攻击检测的实时性与主动性。

第一方面，本发明实施例提供一种区块链日蚀攻击检测的方法，包括：

基于各第二节点在检测时刻上报的各邻居节点，确定第一节点在所述检测时刻的各输出节点；所述各第二节点为所述第一节点的分布式路由表中的节点；所述各邻居节点为第二节点的分布式路由表中的节点；

确定所述检测时刻的各输出节点分别与所述第一节点之间的各第一逻辑距离；

针对所述检测时刻之前的至少一个历史时刻，确定所述历史时刻的各输出节点分别与所述第一节点之间的各第二逻辑距离；

根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中。

上述技术方案中，基于各第二节点在检测时刻上报的各邻居节点与第一节点之间的逻辑距离，将预设数量的且各邻居节点与第一节点之间的逻辑距离最小的邻居节点确定为第一节点在检测时刻的各输出节点，基于此，无重启式日蚀攻击会构造出与第一节点之间的逻辑距离较小的邻居节点，因此，在确定出检测时刻的输出节点之后，确定出输出节点与第一节点之间的第一逻辑距离，再根据历史时刻的第二逻辑距离以及检测时刻的第一逻辑距离来确定在检测时刻时，第一节点是否处于日蚀攻击中，以此增加在检测时刻对无重启式的日蚀攻击检测的实时性与主动性，且针对无重启式日蚀攻击的攻击方式进行检测。

可选的，根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中，包括：

根据所述至少一个历史时刻的各第二逻辑距离，通过神经网络模型，确定所述检测时刻的预测逻辑距离；

根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述第一节点是否处于日蚀攻击中。

上述技术方案中，根据至少一个历史时刻的各第二逻辑距离，通过神经网络模型，确定检测时刻的预测逻辑距离，增加了对检测时刻的输出节点检测的实时性与主动性，以此增加了对无重启式的日蚀攻击检测的实时性与主动性。

可选的，根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述第一节点是否处于日蚀攻击中，包括：

根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述检测时刻是否为异常时刻；

若所述第一节点存在多个连续的异常时刻，则确定所述第一节点处于日蚀攻击中。

可选的，根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述检测时刻是否为异常时刻，包括：

针对任一所述第一逻辑距离，根据所述第一逻辑距离与所述检测时刻的预测逻辑距离，确定第一误差；

针对 N 个历史时刻中的任一历史时刻，基于所述历史时刻的各第二逻辑距离和所述历史时刻的预测逻辑距离，确定各第二误差；

根据所述 N 个历史时刻的各第二误差和所述第一误差，确定误差阈值；

若所述第一误差大于所述误差阈值，则确定所述检测时刻为异常时刻。

上述技术方案中，针对任一第一逻辑距离对应的输出节点进行检测，若在检测时刻，任一输出节点对应的第一误差大于误差阈值，则确定检测时刻为异常时刻，防止攻击者逐步占据第一节点的输出节点表，增加了对无重启式日蚀攻击检测的准确性。

可选的，根据所述 N 个历史时刻的各第二误差和所述第一误差，确定误差阈值，包括：

根据所述 N 个历史时刻的各第二误差和所述第一误差得到第一向量；

根据所述第一向量和指数移动加权平均算法确定第二向量；

根据所述第二向量得到所述误差阈值。

可选的，根据公式（1）得到所述误差阈值，包括：

$$\epsilon=\frac{\Delta\mu(e_s)/\mu(e_s)+\Delta\sigma(e_s)/\sigma(e_s)}{|e_a|+|E_{seq}|^2} \qquad (1);$$

其中，ϵ 为误差阈值；$\mu(e_s)$ 为所述第二向量的平均值；$\sigma(e_s)$ 为所述第二向量的标准差；$\Delta\mu(e_s)$ 为所述第二向量中异常值的平均值；$\Delta\sigma(e_s)$ 为所述第二向量中异常值的标准差；$|e_a|$为所述第二向量中异常值的集合的模；$|E_{seq}|^2$ 为所述第二向量中，连续的异常值的集合的模的平方；所述异常值是所述第二向量中历史时刻为异常时刻的值。

可选的，所述神经网络模型是根据 M 个历史时刻上报的各邻居节点与所述第一节点之间的逻辑距离进行训练得到的。

第二方面，本发明实施例提供一种区块链日蚀攻击检测的装置，包括：

计算模块，用于基于各第二节点在检测时刻上报的各邻居节点，确定第一节点在所述检测时刻的各输出节点；所述各第二节点为所述第一节点的分布式路由表中的节点；所述各邻居节点为第二节点的分布式路由表中的节点；

确定所述检测时刻的各输出节点分别与所述第一节点之间的各第一逻辑距离；

处理模块，用于针对所述检测时刻之前的至少一个历史时刻，确定所述历史时刻的各输出节点分别与所述第一节点之间的各第二逻辑距离；

根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中。

可选的，所述处理模块具体用于：

根据所述至少一个历史时刻的各第二逻辑距离，通过神经网络模型，确定所述检测时刻的预测逻辑距离；

根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述第一节点是否处于日蚀攻击中。

可选的，所述处理模块具体用于：

根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述检

测时刻是否为异常时刻；

若所述第一节点存在多个连续的异常时刻，则确定所述第一节点处于日蚀攻击中。

可选的，所述处理模块具体用于：

针对任一所述第一逻辑距离，根据所述第一逻辑距离与所述检测时刻的预测逻辑距离，确定第一误差；

针对 N 个历史时刻中的任一历史时刻，基于所述历史时刻的各第二逻辑距离和所述历史时刻的预测逻辑距离，确定各第二误差；

根据所述 N 个历史时刻的各第二误差和所述第一误差，确定误差阈值；

若所述第一误差大于所述误差阈值，则确定所述检测时刻为异常时刻。

可选的，所述处理模块具体用于：

根据所述 N 个历史时刻的各第二误差和所述第一误差得到第一向量；

根据所述第一向量和指数移动加权平均算法确定第二向量；

根据所述第二向量得到所述误差阈值。

可选的，根据公式（1）得到所述误差阈值，包括：

$$\epsilon=\frac{\Delta\mu(e_s)/\mu(e_s)+\Delta\sigma(e_s)/\sigma(e_s)}{|e_a|+|E_{seq}|^2} \quad (1);$$

其中，ϵ 为误差阈值；$\mu(e_s)$ 为所述第二向量的平均值；$\sigma(e_s)$ 为所述第二向量的标准差；$\Delta\mu(e_s)$ 为所述第二向量中异常值的平均值；$\Delta\sigma(e_s)$ 为所述第二向量中异常值的标准差；$|e_a|$ 为所述第二向量中异常值的集合的模；$|E_{seq}|^2$ 为所述第二向量中，连续的异常值的集合的模的平方；所述异常值是所述第二向量中历史时刻为异常时刻的值。

可选的，所述神经网络模型是根据 M 个历史时刻上报的各邻居节点与所述第一节点之间的逻辑距离进行训练得到的。

第三方面，本发明实施例还提供一种计算设备，包括：

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行上述区块链日蚀攻击检测的方法。

第四方面，本发明实施例还提供一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可执行指令，所述计算机可执行指令用于使计算机执行上述区块链日蚀攻击检测的方法。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例提供的一种随机森林算法的攻击检测方法的示意图；

图 2 为本发明实施例提供的一种系统架构示意图；

图 3 为本发明实施例提供的一种区块链日蚀攻击检测的方法的流程示意

图；

图 4 为本发明实施例提供的一种区块链日蚀攻击检测的装置的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

区块链系统是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，而建立的物理网络基础是点对点（*P2P*）的分布式网络。用以太坊为例，以太坊底层分布式网络，即 *P2P* 网络，使用了经典的 *Kademlia*（*Kademlia Distributed Hash Table*，分布式哈希表）网络，简称 *KAD*，是一种分布式散列表技术，以异或运算为节点之间逻辑距离的度量基础，其中，*KAD* 的路由表是通过称为 *K* 桶的数据构造而成，*K* 桶记录了节点 *ID*（*Identity document*，身份标识号），逻辑距离等信息，在不同版本的以太坊客户端中，*K* 桶的数量也不是一致的，例如，在以太坊客户端 1.8 版本中，*K* 桶的数量为 17，每个桶中存储有 16 个节点 *ID*。其中，*K* 桶中的路由表是根据节点发现机制得到的。

现有技术中存在多种攻击方式，例如女巫攻击和日蚀攻击，通过女巫攻击和日蚀攻击将正常节点隔离开区块链系统，以达到在低于 51%算力时，实现 51%攻击，例如，以太坊节点的 *TCP*（*Transmission Control Protocol*，传输控制协议）接口是在两个表中确定的，包括输出节点表和输入节点表，其中，输入节点表是根据 *K* 桶中的节点确定的，输出节点表中预设数量（如一半数量）的节点是在输入节点表中选择的，其余的节点是通过节点发现机制确定的。攻击者通过女巫攻击构建大量的恶意节点，通过控制僵尸网络不断地去连接以太坊节点，即达到刷新这两张节点表的目的，使得这两张节点表都保存恶意节点的地址，攻击者再通过 *DDoS*（*Distributed Denial of Service*，分布式拒绝服务）攻击等方法，让以太坊节点重启，以此使以太坊节点的输出节点表和输入节点表存储的均是攻击者控制的恶意节点。

现有技术中，为了检测出以太坊节点收到了日蚀攻击，给出了随机森林算法的检测方法，图 1 示例性的示出了一种随机森林算法的攻击检测方法的示意图，如图 1 所示，随机森林算法在以太坊的正常节点中收集正常数据包，作为数据包训练集，其中，正常数据包中包括多个邻居节点，数据包是根据节点发现机制得到的，例如，节点 *A* 随机生成目标节点 *B*，并计算出节点 *A* 与目标节点 *B* 之间的逻辑距离 l_{AB}，节点 *A* 在自身的 K 桶中找出节点 *C*，需要说明的是，节点 *A* 与节点 *C* 之间的逻辑距离 l_{AC} 小于逻辑距离 l_{AB}，然后节点 *A* 向节点 *C* 发送 *find-node*（查找节点）请求（查询与目标节点 *B* 之间的逻辑距离的节点的请求），其中，*find-node* 请求包括目标节点 *B* 的 *ID*，节点 *C* 根据

目标节点 *B* 的 *ID* 确定出预设数量（如 16 个）的节点 *D* 等多个节点，需要说明的是，节点 *D* 等多个节点在节点 *C* 的 *K* 桶中，与目标节点 *B* 的 *ID* 之间的逻辑距离最小。然后在正常节点的数据包的训练集中提取特征向量，然后根据包括特征向量和标签的训练集训练出随机森林模型，并在随机森林模型中加入标签。

在测试过程中，随机森林模型运行攻击脚本，通过不断向受害者节点发送 *find-node* 请求，以收集受害者节点返回的包含有恶意节点的攻击数据包，然后提取攻击数据包的特征向量，通过随机森林模型进行预测，将随机森林模型预测的结果视作检测的预测标签。

需要说明的是，随机森林算法是由大量决策树共同组成的，随机森林算法可以在较低计算资源消耗的情况下给出较为准确的探测结果。在上述测试过程中，随机森林算法实现流程为：1、采用 *Bootstrap*（前端工具包）方法随机从训练集中提取 *k* 个训练样本，从而生成 *k* 个分类树。2、从 *k* 个分类树的节点中随机选取 *S* 个变量，并选出具有代表性的变量，再由多个分类点选出分类的阈值。3、不修建分类树，令其保持无限增长，每当输入新的训练样本时，将被构建好了的决策树森林拆分，并通过分类树投票得到最终标签。

根据上面所述，基于随机森林算法的检测日蚀攻击的方法需要收集海量正常节点的数据包，需要预先构建随机决策森林，再对需要探测的数据进行标签分类，当判定存在恶意节点的攻击数据包时，则认为受害者节点遭受到了攻击。因此，基于随机森林算法的检测日蚀攻击的方法无法实时检测以太坊节点，而且，当存在一个数据包被标签为攻击数据包时，就认为发生了攻击，误报率较高。

另外，基于随机森林算法的检测日蚀攻击的方法针对的日蚀攻击类型有限，只可以重启式日蚀攻击，即检测受害者节点重启后侵占以太坊节点的 *TCP* 链接的低资源消耗的日蚀攻击模式。

但是目前，存在一种名为 *False Friend Attack* 的无重启式日蚀攻击模式，该攻击模式可以利用以太坊网络中正常节点的邻居节点会断开连接的特点，通过构造长期在线的女巫节点，在节点发现机制过程中侵占受害者节点的 *TCP* 接口中的输出节点表，无需等待以太坊节点重启，而这种无重启式日蚀攻击是基于随机森林算法的检测日蚀攻击的方法所无法检测的。

为了进一步地描述 *False Friend Attack* 的日蚀攻击模式，下面再具体实例中阐述 *False Friend Attack* 的日蚀攻击实现方式。

实例 1

在以太坊客户端 1.8 版本，受害者节点的包括 25 个 *TCP* 连接 *ID*，分为包括 8 个输出节点的输出节点表和包括 17 个输入节点的输入节点表。由于以太坊网络不对输入的节点链路施加限制，攻击者可以根据构建的多个女巫节点，并持续向受害者节点发送 *TCP* 入站连接请求，轻松地利用输入节点表主动与受害者节点建立连接，直到占领完成为止，以实现侵占输入节点表。受害者节点的输出节点表是通过两个机制选择的，第一种机制是通过 *Read Random Nodes* 函数在受害者节点的每个 K 桶中的首个节点中随机选择的，即在输入

节点表中随机选择的。另一种机制是通过节点发现机制选择的，受害者节点在通过发现机制得到邻居节点后，在邻居节点中确定出与受害者节点最近的4个节点，作为输出节点，得到输出节点表。

False Friend Attack 日蚀攻击可以入侵运行平稳的受害者节点，无需使受害者节点重新启动。在 *False Friend Attack* 攻击模型中，包括两种机制，第一种机制，只需要在受害者节点的每个 *K* 桶中的头部注入一个女巫节点即可确保以太坊节点的输出节点表完成了侵占。受害者节点选择输出节点表的节点时，一部分取决于第一种机制，如通过 *Read Random Nodes* 函数在输入节点表中随机选取4个节点作为输出节点。

针对另一种机制：攻击者需要在的受害者节点的每个 *K* 桶中至少放置一个女巫节点，以便以太坊节点向攻击者发送 *find-node* 请求，攻击者在接收到受害者节点的 *find-node* 请求后，返回预先制造的虚假的女巫节点（*neighbors* 列表），其中，*neighbors*（邻居）列表中的节点是与受害者节点距离较近的女巫节点，因此，攻击者通过伪造与受害者节点之间短距离的节点侵占受害者节点的输出节点表。

需要说明的是，节点之间的逻辑距离是根据节点的 *ID* 通过异或运算计算得到的。例如，比如节点 *ID* 为 000111 的节点与节点 *ID* 为 000110、000011 的节点之间的逻辑距离计算为：000111Å000110=000001（十进制 1）、000111Å000011=000100（十进制 4）。

因此，现需要一种日蚀攻击检测的方法，以针对无重启式日蚀攻击的攻击方式进行检测，并增加在检测时刻对无重启式的日蚀攻击检测的实时性与主动性。

图 2 示例性的示出了本发明实施例所适用的一种系统架构，该系统架构包括第一节点 210 和第二节点 220。

其中，第二节点 220 是第一节点 210 通过在自身的 *K* 桶中确定的，具体的，第一节点 210 随机生成一个目标节点，并计算出第一节点 210 与目标节点之间的逻辑距离，然后确定出第一节点 210 在自身的 *K* 桶中的第二节点 220，第一节点 210 与第二节点 220 之间的逻辑距离小于第一节点 210 与目标节点之间的逻辑距离，需要说明的是，第二节点 220 可以为多个，也可以为预设的数量，例如，确定出第一节点 210 在自身的 *K* 桶中确定出 10 个小于第一节点 210 与目标节点之间的逻辑距离的节点，随机选取 3 个作为第二节点 220。

第一节点 210 用于向第二节点 220 发送 *find-node* 请求，以使第二节点 220 查询出邻居节点，并将邻居节点反馈至第一节点 210。

第一节点 210 在得到邻居节点之后，在邻居节点中确定出输出节点，并对输出节点进行检测，进而确定出检测时刻是否为异常时刻。

需要说明的是，上述图 2 所示的结构仅是一种示例，本发明实施例对此不做限定。

基于上述描述，图 3 示例性的示出了本发明实施例提供的一种区块链日蚀攻击检测的方法的流程示意图，该流程可由区块链日蚀攻击检测的装置执行。

如图 3 所示，该流程具体包括:

步骤 310，基于各第二节点在检测时刻上报的各邻居节点，确定第一节点在所述检测时刻的各输出节点。

本发明实施例中，各第二节点为第一节点的分布式路由表中的节点，各邻居节点为第二节点的分布式路由表中的节点。

具体的，第二节点是第一节点根据目标节点在第一节点的分布式路由表中确定的，各邻居节点是第二节点根据目标节点在第二节点的分布式路由表中确定的。为了更好的描述第一节点如何确定输出节点，下面将在具体的实例中进行阐述。

实例 2

在检测时刻，第一节点 a 随机的生成目标节点 b，其中，随机的生成目标节点 b 包括目标节点 b 的节点 *ID*，并通过第一节点 a 的节点 *ID* 和目标节点 b 的节点 *ID* 计算出第一节点 a 与目标节点 b 之间的逻辑距离 l_{ab}，然后第一节点 a 在自身的分布式路由表中找出第二节点 c，其中，第一节点 a 与第二节点 c 之间的逻辑距离 l_{ac} 小于逻辑距离 l_{ab}。在确定出第二节点 c 之后，第一节点 a 向第二节点 c 发送 *find-node* 请求，其中，*find-node* 请求中包括目标节点 b 的节点 *ID*。以使第二节点 c 根据目标节点 b 的节点 *ID* 确定出 16 个的邻居节点 d，其中，邻居节点 d 是第二节点 c 的分布式路由表中，与目标节点 b 之间的逻辑距离最小的 16 个节点，然后由第二节点 c 将邻居节点 d 反馈至第一节点 a。

第一节点 a 在得到 16 个邻居节点 d 之后，计算出各邻居节点 d 与第一节点 a 之间的各逻辑距离 l_{ad}，在 16 个逻辑距离 l_{ad} 中确定 4 个最小值，则最小值对应的邻居节点 d 为第一节点在检测时刻的各输出节点。

步骤 320，确定所述检测时刻的各输出节点分别与所述第一节点之间的各第一逻辑距离。

本发明实施例中，在第一节点确定输出节点时，根据输出节点的节点 *ID* 得到输出节点与第一节点之间的第一逻辑距离。

步骤 330，针对所述检测时刻之前的至少一个历史时刻，确定所述历史时刻的各输出节点分别与所述第一节点之间的各第二逻辑距离。

本发明实施例中，在历史时刻中，第一节点根据第二节点确定出输出节点，进而确定出历史时刻的输出节点与第一节点之间的各第二逻辑距离。例如，结合实例 2，历史时刻为检测时刻的前一时刻，历史时刻的第二节点 e 与第一节点之间的为第二逻辑距离。

步骤 340，根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中。

本发明实施例中，根据历史时刻的第二逻辑距离确定出检测时刻的预测逻辑距离，进而确定第一节点是否处于日蚀攻击中。

进一步地，根据至少一个历史时刻的各第二逻辑距离，通过神经网络模型，确定检测时刻的预测逻辑距离，再根据各第一逻辑距离与检测时刻的预测逻辑距离，确定第一节点是否处于日蚀攻击中。

本发明实施例中，可以根据至少一个历史时刻的各第二逻辑距离确定检测时刻的预测逻辑距离，也可以根据至少一个历史时刻的各邻居节点与第一节点之间的逻辑距离确定检测时刻的预测逻辑距离，在此不做限定，使用第二逻辑距离可以增加确定检测时刻的预测逻辑距离的准确度。

例如，检测时刻为 t，每个检测时刻的输出节点为 4 个，将检测时刻之前的两个历史时刻（t-1 和 t-2）的输出节点作为神经网络模型的输入样本，即输入样本 X 为 $X=\{x_1^{(t-1)}, x_2^{(t-1)}, \ldots, x_4^{(t-2)}\}$，其中，样本 X 中的每个特征（如 $x_1^{(t-1)}$）包括预处理后的第二逻辑距离，预处理包括归一化处理，编码处理等。然后根据输入样本 X 得到检测时刻的预测逻辑距离 $x_*^{(t)}$。其中，检测时刻的预测逻辑距离用于确定检测时刻是否为异常时刻，根据异常时刻确定第一节点是否处于日蚀攻击中。

进一步地，根据各第一逻辑距离与检测时刻的预测逻辑距离，确定检测时刻是否为异常时刻，若第一节点存在多个连续的异常时刻，则确定第一节点处于日蚀攻击中。

具体的，针对任一第一逻辑距离，根据第一逻辑距离与检测时刻的预测逻辑距离，确定第一误差，针对 N 个历史时刻中的任一历史时刻，基于历史时刻的各第二逻辑距离和历史时刻的预测逻辑距离，确定各第二误差，根据 N 个历史时刻的各第二误差和第一误差，确定误差阈值，若第一误差大于误差阈值，则确定检测时刻为异常时刻。

本发明实施例中，在检测时刻，存在多个第一逻辑距离，针对任一第一逻辑距离进行确定，在任一第一逻辑距离对应的第一误差大于误差阈值时，确定检测时刻为异常时刻，需要说明的是，为了降低误报率，也可以在大于误差阈值的第一误差大于预设数量时，确定检测时刻为异常时刻，在此不限定具体数量确定检测时刻为异常时刻。

其中，误差阈值是将 N 个历史时刻的各第二误差和第一误差作为一个向量得到的。具体的，根据 N 个历史时刻的各第二误差和第一误差得到第一向量，再根据第一向量和指数移动加权平均算法确定第二向量，最后根据第二向量得到误差阈值。

进一步地，根据下述公式（1）得到误差阈值，包括：

$$\epsilon=\frac{\Delta\mu(e_s)/\mu(e_s)+\Delta\sigma(e_s)/\sigma(e_s)}{|e_a|+|E_{seq}|^2} \qquad (1);$$

其中，ϵ 为误差阈值；$\mu(e_s)$ 为第二向量的平均值；$\sigma(e_s)$ 为第二向量的标准差，$\Delta\mu(e_s)$ 为第二向量中异常值的平均值，$\Delta\sigma(e_s)$ 为第二向量中异常值的标准差，$|e_a|$ 为第二向量中异常值的集合的模，$|E_{seq}|^2$ 为第二向量中，连续的异常值的集合的模的平方，异常值是第二向量中历史时刻为异常时刻的值。

本发明实施例中，公式（1）是一种无监督的阈值计算方法，为了更好的解释如何确定检测时刻的误差阈值，下面将结合实例 2 在具体实例中进行阐述。

实例 3

在检测时刻，确定出输出节点 $d1$、$d2$、$d3$、$d4$，针对输出节点 $d1$ 得到输出节点 $d1$ 与第一节点之间的第一逻辑距离，根据上述得到的预测逻辑距离 $x_*^{(t)}$，得到第一误差 $e_1^{(t)}$，$e_1^{(t)}=\left|d1-x_*^{(t)}\right|$，再根据前两个（即 N 为 2）历史时刻的第二误差（如 $e^{(t-1)}$ 和 $e^{(t-2)}$）得到第一向量 $\boldsymbol{e}$，$\boldsymbol{e}=[\ e^{(t-2)},\ e^{(t-1)},\ e_1^{(t)}]$，再将第一向量 $\boldsymbol{e}$ 通过指数移动加权平均算法得到第二向量 $\boldsymbol{e}_s$，$\boldsymbol{e}_s=[e_s^{(t-2)},\ e_s^{(t-1)},\ e_{s1}^{(t)}]$，然后根据第二向量 $\boldsymbol{e}_s$ 得到异常值的集合，如 t-1 的历史时刻为异常时刻，则异常值的集合 $\boldsymbol{e}_s^*$，$\boldsymbol{e}_s^*=[e_s^{(t-1)}]$。然后根据第二向量 $\boldsymbol{e}_s$ 和异常值的集合 $\boldsymbol{e}_s^*$，通过上述公式（1）确定出检测时刻 t 的误差阈值 $s1$，最后根据第一误差 $e_1^{(t)}$ 与误差阈值 $s1$ 的大小确定检测时刻是否为异常时刻。如，第一误差 $e_1^{(t)}$ 大于误差阈值 $s1$，则检测时刻为异常时刻。

示例性的，在检测时刻的其他输出节点根据相同的方法确定第一误差 $e_n^{(t)}$ 是否大于误差阈值 sn，其中，n 为输出节点的数量。

需要说明的是，在本发明中，不局限于对输出节点的检测，也可以对第二节点反馈的各邻居节点进行检测，但会相应的增加检测过程中的计算量。

其中，指数移动加权平均算法用于对第一向量 $\boldsymbol{e}$ 分别给予不同的权数，按不同权数求得移动平均值，并以最后的移动平均值为基础，确定第二向量 $\boldsymbol{e}_s$。

本发明实施例中，神经网络模型是根据 M 个历史时刻上报的各邻居节点与第一节点之间的逻辑距离进行训练得到的，例如，将检测时刻的前一时刻至前 M 各时刻的 M 个历史时刻第一节点得到的各居节点作为训练样本，根据 M 个训练样本进行训练，得到神经网络模型。

进一步地，可以通过 *Dropout* 方法训练神经网络模型，以防止神经网络模型在训练时存在过拟合且训练时间过长的缺陷。

本发明中所提及的任一逻辑距离包括但不限于通过节点 *ID* 得到的逻辑距离通过归一化、*one-hot* 编码处理后的距离特征。

基于相同的技术构思，图 4 示例性的示出了本发明实施例提供的一种区块链日蚀攻击检测的装置的结构示意图，该装置可以执行区块链日蚀攻击检测的方法的流程。

如图 4 所示，该装置具体包括:

计算模块 410，用于基于各第二节点在检测时刻上报的各邻居节点，确定第一节点在所述检测时刻的各输出节点；所述各第二节点为所述第一节点的分布式路由表中的节点；所述各邻居节点为第二节点的分布式路由表中的节点；

确定所述检测时刻的各输出节点分别与所述第一节点之间的各第一逻辑距离；

处理模块 420，用于针对所述检测时刻之前的至少一个历史时刻，确定所述历史时刻的各输出节点分别与所述第一节点之间的各第二逻辑距离；

根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中。

可选的，所述处理模块 420 具体用于：

根据所述至少一个历史时刻的各第二逻辑距离，通过神经网络模型，确定所述检测时刻的预测逻辑距离；

根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述第一节点是否处于日蚀攻击中。

可选的，所述处理模块 420 具体用于：

根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述检测时刻是否为异常时刻；

若所述第一节点存在多个连续的异常时刻，则确定所述第一节点处于日蚀攻击中。

可选的，所述处理模块 420 具体用于：

针对任一所述第一逻辑距离，根据所述第一逻辑距离与所述检测时刻的预测逻辑距离，确定第一误差；

针对 N 个历史时刻中的任一历史时刻，基于所述历史时刻的各第二逻辑距离和所述历史时刻的预测逻辑距离，确定各第二误差；

根据所述 N 个历史时刻的各第二误差和所述第一误差，确定误差阈值；

若所述第一误差大于所述误差阈值，则确定所述检测时刻为异常时刻。

可选的，所述处理模块 420 具体用于：

根据所述 N 个历史时刻的各第二误差和所述第一误差得到第一向量；

根据所述第一向量和指数移动加权平均算法确定第二向量；

根据所述第二向量得到所述误差阈值。

可选的，根据公式（1）得到所述误差阈值，包括：

$$\epsilon=\frac{\Delta\mu(e_s)/\mu(e_s)+\Delta\sigma(e_s)/\sigma(e_s)}{|e_a|+|E_{seq}|^2} \quad (1);$$

其中，ϵ 为误差阈值；$\mu(e_s)$ 为所述第二向量的平均值；$\sigma(e_s)$ 为所述第二向量的标准差；$\Delta\mu(e_s)$ 为所述第二向量中异常值的平均值；$\Delta\sigma(e_s)$ 为所述第二向量中异常值的标准差；$|e_a|$为所述第二向量中异常值的集合的模；$|E_{seq}|^2$ 为所述第二向量中，连续的异常值的集合的模的平方；所述异常值是所述第二向量中历史时刻为异常时刻的值。

可选的，所述神经网络模型是根据 M 个历史时刻上报的各邻居节点与所述第一节点之间的逻辑距离进行训练得到的。

基于相同的技术构思，本发明实施例还提供一种计算设备，包括：

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行上述区块链日蚀攻击检测的方法。

基于相同的技术构思，本发明实施例还提供一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可执行指令，所述计算机可执行指令用于使计算机执行上述区块链日蚀攻击检测的方法。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1、一种区块链日蚀攻击检测的方法，其特征在于，包括:

基于各第二节点在检测时刻上报的各邻居节点，确定第一节点在所述检测时刻的各输出节点；所述各第二节点为所述第一节点的分布式路由表中的节点；所述各邻居节点为第二节点的分布式路由表中的节点；

确定所述检测时刻的各输出节点分别与所述第一节点之间的各第一逻辑距离；

针对所述检测时刻之前的至少一个历史时刻，确定所述历史时刻的各输出节点分别与所述第一节点之间的各第二逻辑距离；

根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中。

2、如权利要求 1 所述的方法，其特征在于，根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中，包括:

根据所述至少一个历史时刻的各第二逻辑距离，通过神经网络模型，确定所述检测时刻的预测逻辑距离；

根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述第一节点是否处于日蚀攻击中。

3、如权利要求 2 所述的方法，其特征在于，根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述第一节点是否处于日蚀攻击中，包括:

根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述检测时刻是否为异常时刻；

若所述第一节点存在多个连续的异常时刻，则确定所述第一节点处于日蚀攻击中。

4、如权利要求 3 所述的方法，其特征在于，根据所述各第一逻辑距离与所述检测时刻的预测逻辑距离，确定所述检测时刻是否为异常时刻，包括:

针对任一所述第一逻辑距离，根据所述第一逻辑距离与所述检测时刻的预测逻辑距离，确定第一误差；

针对 N 个历史时刻中的任一历史时刻，基于所述历史时刻的各第二逻辑距离和所述历史时刻的预测逻辑距离，确定各第二误差；

根据所述 N 个历史时刻的各第二误差和所述第一误差，确定误差阈值；

若所述第一误差大于所述误差阈值，则确定所述检测时刻为异常时刻。

5、如权利要求 4 所述的方法，其特征在于，根据所述 N 个历史时刻的各第二误差和所述第一误差，确定误差阈值，包括:

根据所述 N 个历史时刻的各第二误差和所述第一误差得到第一向量；

根据所述第一向量和指数移动加权平均算法确定第二向量；

根据所述第二向量得到所述误差阈值。

6、如权利要求 5 所述的方法，其特征在于，根据公式（1）得到所述误

差阈值，包括:

$$\epsilon=\frac{\Delta\mu(e_s)/\mu(e_s)+\Delta\sigma(e_s)/\sigma(e_s)}{|e_a|+|E_{seq}|^2} \quad (1);$$

其中，ϵ 为误差阈值；$\mu(e_s)$ 为所述第二向量的平均值；$\sigma(e_s)$ 为所述第二向量的标准差；$\Delta\mu(e_s)$ 为所述第二向量中异常值的平均值；$\Delta\sigma(e_s)$ 为所述第二向量中异常值的标准差；$|e_a|$为所述第二向量中异常值的集合的模；$|E_{seq}|^2$ 为所述第二向量中，连续的异常值的集合的模的平方；所述异常值是所述第二向量中历史时刻为异常时刻的值。

7、如权利要求 2 所述的方法，其特征在于，所述神经网络模型是根据 M 个历史时刻上报的各邻居节点与所述第一节点之间的逻辑距离进行训练得到的。

8、一种区块链日蚀攻击检测的装置，其特征在于，包括:

计算模块，用于基于各第二节点在检测时刻上报的各邻居节点，确定第一节点在所述检测时刻的各输出节点；所述各第二节点为所述第一节点的分布式路由表中的节点；所述各邻居节点为第二节点的分布式路由表中的节点；

确定所述检测时刻的各输出节点分别与所述第一节点之间的各第一逻辑距离；

处理模块，用于针对所述检测时刻之前的至少一个历史时刻，确定所述历史时刻的各输出节点分别与所述第一节点之间的各第二逻辑距离；

根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中。

9、一种计算设备，其特征在于，包括:

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行权利要求 1 至 7 任一项所述的方法。

10、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机可执行指令，所述计算机可执行指令用于使计算机执行权利要求 1 至 7 任一项所述的方法。

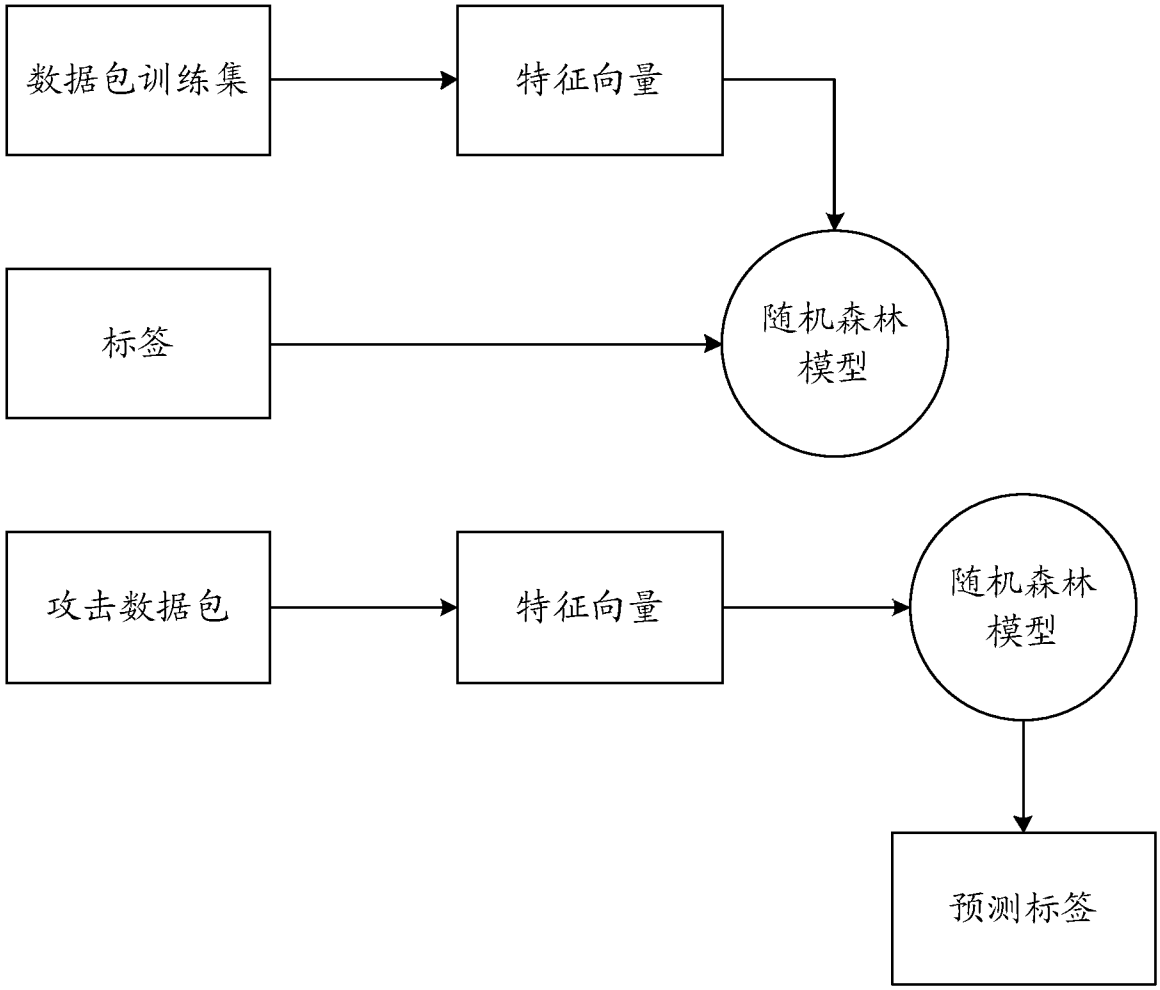

数据包训练集
特征向量
标签
随机森林模型
攻击数据包
特征向量
随机森林模型
预测标签

图 1

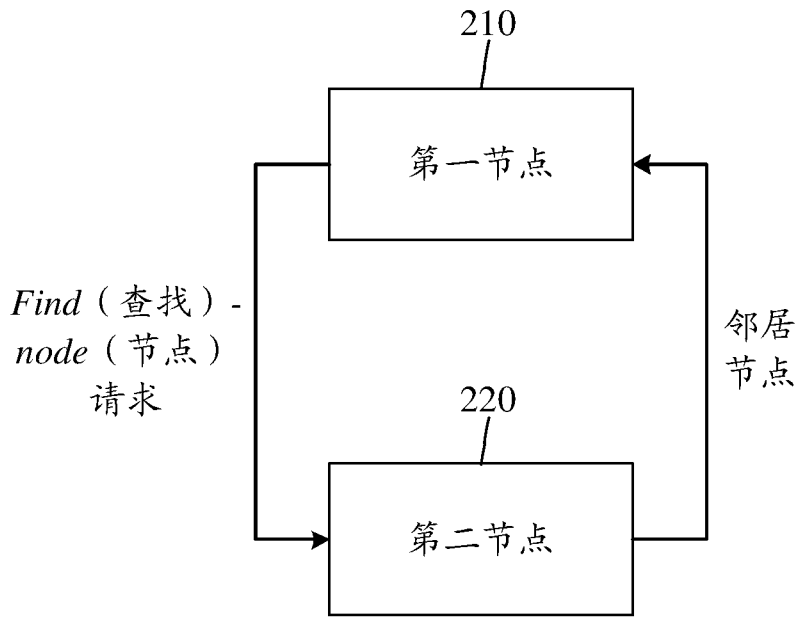

210
第一节点
Find（查找）-node（节点）请求
邻居节点
220
第二节点

图 2

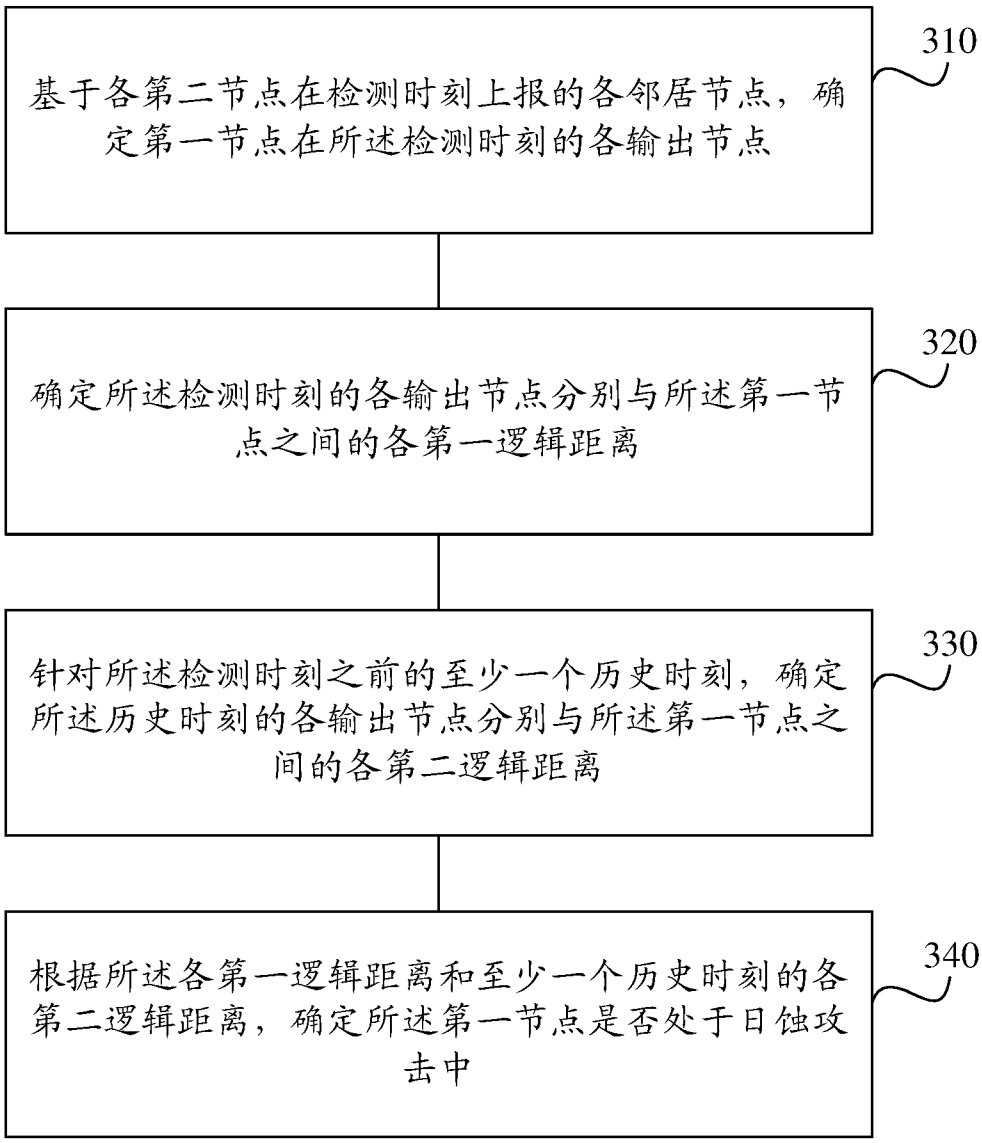

基于各第二节点在检测时刻上报的各邻居节点，确定第一节点在所述检测时刻的各输出节点
310
确定所述检测时刻的各输出节点分别与所述第一节点之间的各第一逻辑距离
320
针对所述检测时刻之前的至少一个历史时刻，确定所述历史时刻的各输出节点分别与所述第一节点之间的各第二逻辑距离
330
根据所述各第一逻辑距离和至少一个历史时刻的各第二逻辑距离，确定所述第一节点是否处于日蚀攻击中
340

图 3

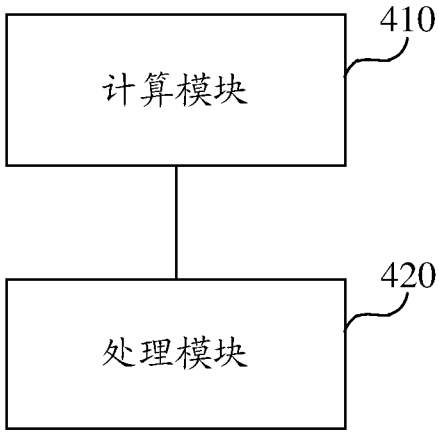

计算模块
410
处理模块
420

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/124772

A. CLASSIFICATION OF SUBJECT MATTER

H04L 67/01(2022.01)i; G06K 9/62(2022.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT; ENTXTC; CJFD; CNKI; ETSI; ENTXT; 3GPP; IETF; VEN: 区块链, 日蚀攻击, 检测, 邻近, 节点, 异常, 逻辑距离, 无重启, 连续, block chain, eclipse attack, false friend attack, detect, neighbour, neighbor, node, abnormal, logic distance, restart, continuous

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112653682 A (SHENZHEN QIANHAI WEBANK CO., LTD.; BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 13 April 2021 (2021-04-13) claims 1-10	1-10
A	CN 110191116 A (BEIJING CONFLUX TECHNOLOGY DEVELOPMENT CO., LTD.) 30 August 2019 (2019-08-30) description, paragraphs [0009] and [0010]	1-10
A	CN 110730195 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 24 January 2020 (2020-01-24) entire document	1-10
A	CN 108965259 A (FOSHAN UNIVERSITY) 07 December 2018 (2018-12-07) entire document	1-10
A	WO 2020099924 A1 (IAGON AS) 22 May 2020 (2020-05-22) entire document	1-10

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2022	**24 January 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/124772

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	崔中杰 (CUI, Zhongjie). "“针对区块链的网络攻击与防御技术综述” (non-official translation: “Overview of Cyber Attack and Defense Technologies for Blockchain”)" *《信息安全研究》 (Journal of Information Security Research),* Vol. 6, No. 11, 30 November 2020 (2020-11-30), 第3节区块链系统中网络层的攻 (non-official translation: Section 3: Cyber Attacks and Defenses in Blockchain Systems)	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/124772

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112653682	A	13 April 2021	None			
CN	110191116	A	30 August 2019	None			
CN	110730195	A	24 January 2020	None			
CN	108965259	A	07 December 2018	None			
WO	2020099924	A1	22 May 2020	AU	2019380719	A1	10 June 2021
				KR	20210096619	A	05 August 2021
				CN	112997469	A	18 June 2021
				EP	3878161	A1	15 September 2021
				CA	3118374	A1	22 May 2020
				IL	282920	D0	30 June 2021

国际检索报告

国际申请号
PCT/CN2021/124772

A. 主题的分类

H04L 67/01(2022.01)i; G06K 9/62(2022.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G06K

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNTXT;ENTXTC;CJFD;CNKI;ETSI;ENTXT;3GPP;IETF;VEN:区块链，日蚀攻击，检测，邻近，节点，异常，逻辑距离，无重启，连续，block chain, eclipse attack, false friend attack, detect, neighbour, neighbor, node, abnormal, logic distance, restart, continuous

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 112653682 A (深圳前海微众银行股份有限公司 北京邮电大学) 2021年4月13日 (2021-04-13) 权利要求1-10	1-10
A	CN 110191116 A (北京清红微谷技术开发有限责任公司) 2019年8月30日 (2019-08-30) 说明书第[0009]-[0010]段	1-10
A	CN 110730195 A (腾讯科技深圳有限公司) 2020年1月24日 (2020-01-24) 全文	1-10
A	CN 108965259 A (佛山科学技术学院) 2018年12月7日 (2018-12-07) 全文	1-10
A	WO 2020099924 A1 (IAGON AS) 2020年5月22日 (2020-05-22) 全文	1-10
A	崔中杰. ″“针对区块链的网络攻击与防御技术综述”″ 《信息安全研究》, 第6卷, 第11期, 2020年11月30日 (2020-11-30), 第3节区块链系统中网络层的攻防	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2022年1月18日	2022年1月24日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 张雪凌 电话号码 86-(010)-62411265

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/124772

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	112653682	A	2021年4月13日	无			
CN	110191116	A	2019年8月30日	无			
CN	110730195	A	2020年1月24日	无			
CN	108965259	A	2018年12月7日	无			
WO	2020099924	A1	2020年5月22日	AU	2019380719	A1	2021年6月10日
				KR	20210096619	A	2021年8月5日
				CN	112997469	A	2021年6月18日
				EP	3878161	A1	2021年9月15日
				CA	3118374	A1	2020年5月22日
				IL	282920	D0	2021年6月30日