

基于区块链的 ARP 欺骗攻击防御方法

刘凡鸣^{1,2}, 石伟^{1,2}

(1. 河北大学网络空间安全与计算机学院, 河北 保定 071002;

2. 河北省高可信信息系统重点实验室, 河北 保定 071002)

摘要: 为了改善静态绑定方法在抵御 ARP 攻击时存在的不易维护的问题, 利用区块链技术思想, 设计了一种防御成本低、后期易维护的 ARP 欺骗攻击防御方法。改进了区块链结构, 设计了交易索引表结构, 通过对比发现攻击并及时更新数据, 防止后续攻击。正常改动 IP 后更新交易索引表中内容, 保证查询正确性。分析及实验表明, 基于区块链的防御方法具有较高安全性, 能够保证数据不被篡改, 维护成本低, 能有效防御 ARP 欺骗攻击。

关键词: 区块链; ARP 攻击; 动态更新; 加密传输

中图分类号: TP309.5

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018071

Blockchain-based ARP defense scheme

LIU Fanming^{1,2}, SHI Wei^{1,2}

1. School of Cyber Security and Computer, Hebei university, Baoding 071002, China

2. Hebei Key Laboratory of High Confidence Information Systems, Baoding 071002, China

Abstract: In order to improve the difficulty of maintaining the static binding method when defending against ARP attacks, a defense method was designed with the features of low cost of defense and easy maintenance by using the idea of a blockchain technology. The blockchain structure had been improved, and the transaction index table structure had been designed to identify attacks and update data in a timely manner to prevent subsequent attacks. The content of the transaction index table was updated after the IP address was changed normally to ensure the correctness of the query. Analysis and experiments show that the blockchain-based defense method has the following merits: high security, guaranteeing the data is not tampered with, low cost of maintenance, and effective prevention against ARP spoofing attacks.

Key words: blockchain, ARP attack, dynamic update, encrypted transmission

1 引言

在以太网中, 数据传输是依据 MAC 地址完成的。ARP 是一种根据 IP 地址获取主机 MAC 地址的 TCP/IP 协议。协议的设计基于对网络各节点的信任, 源主机在接收到目的主机的回应包时不会对目的主机的身份进行验证。针对该设计缺陷发起

的 ARP 欺骗是一种常见网络攻击方式, 攻击者冒充目的主机向源主机发送大量伪造应答报文, 导致目的主机发送的报文无法被源主机接收, 源主机接收攻击者发送的伪造数据分组, 最终将攻击者的 MAC 地址当作目的主机 MAC 地址保存到 ARP 缓存表, 影响正常通信。

现有的 ARP 攻击方法大致会对用户主机产

收稿日期: 2018-06-02; 修回日期: 2018-06-27

通信作者: 刘凡鸣, lfmhbu@126.com

生3种影响。当攻击者向主机发送大量伪造ARP包时,主机正常更新及读取ARP缓存表效率受到影响,从而影响网络速度,严重情况下还会导致网络瘫痪。若攻击者在正常通信主机间发起攻击,则可以监听通信双方数据,窃取用户敏感信息,造成信息泄露等严重问题。如果针对网关节点发起伪造攻击,则会影响局域网内节点正常上网功能,给用户使用带来极大不便。

现有防御方案大多采用静态绑定IP-MAC地址方式或ARP数据分组信息校验方式控制ARP攻击。

静态绑定方法是目前较常用的方法^[1-4]。通过将各个通信终端IP和MAC地址进行双向绑定,避免ARP缓存表的动态更新,攻击者无法再通过发送ARP响应包更新主机缓存表,实现了ARP攻击的防御目的。但是此种方法的缺陷在于需要为局域网内的每个节点分配固定IP,若节点不常使用会造成IP资源的浪费,同时若后期需要变动IP地址时,维护成本较高。

对于ARP攻击,目前还没有较完善、高效的防御方法有效应对ARP攻击,现有防范策略都在一定程度上具有局限性。基于区块链技术,本文提出一种ARP攻击防御方案,该方案具有维护及部署低成本,IP地址可动态更新的优势,与端口隔离策略不同,本方案不会对网络的其他功能产生影响,并可有效保证已存储MAC地址的安全性。本文的主要贡献如下。

1) 提出了一种ARP攻击防御方案,该方案融合了区块链技术优势,通过签名验证机制,保证数据的安全性,避免MAC值被篡改。

2) 改进了区块链结构,实现了IP地址的有效更改。

3) 引用基于散列验证的加密机制保证数据传输的完整性,保证主机接收到的MAC地址与存储在区块链的值保持一致。

2 预备知识

2008年,中本聪首次在其论文中提出了比特币的概念,阐述了点对点电子现金系统的处理流程^[5]。区块链技术作为比特币系统中的核心技术,受到广泛关注。2015年区块链技术迅

速兴起,首先在金融领域掀起浪潮,后续逐步应用到大数据、人工智能、物联网等领域迸发出新的火花。

区块链是有多个节点构成的去中心化的分布式记账系统。将某一时间内的数据存储在区块内,区块间通过链表连接,利用非对称密钥、散列算法等密码学方法处理存储数据,保证了数据可溯源、不易篡改、公开透明的特性^[6-8]。

1) 区块链结构

区块链由若干个区块通过链式结构组合而成。每个区块内包含区块头和区块体2部分,如图1所示。区块头中包含上一个区块的散列值、时间戳、设定的验证条件以及找到的满足该验证要求的随机数nonce。区块体中则包含该区块内存储的交易序列^[9-10]。

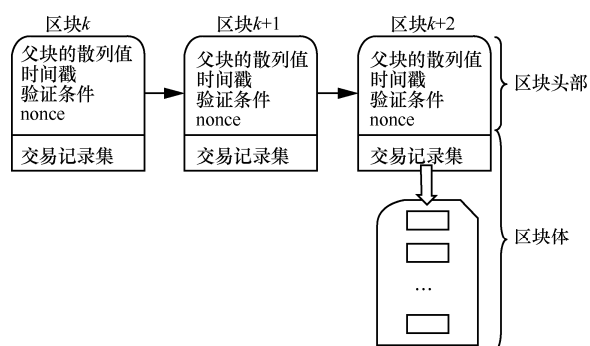


图1 区块链结构

2) 区块链身份验证

区块链中采用非对称密钥加密机制验证交易发起方身份。密钥成对出现,包含一个私钥和一个公钥。私钥用于加密交易信息形成签名。公钥通过节点私钥生成,对网络中其他节点公开,用于验证签名核实身份。区块链系统中,节点发起交易时,首先用自己的私钥对交易处理,得到数字签名^[11]。然后将交易记录连同签名一起发送到网络。网络中节点接收到交易后,会利用交易发起方公钥对其身份进行验证,通过公钥签名验证结果判断该交易是否由私钥持有人发出。只有通过验证后才会把交易放入具体区块内,然后通知矿工节点开始挖矿操作。挖矿的过程就是根据提前设定好的工作难度,寻找满足该条件的一个随机数,然后将找到的随机数填入区块nonce字段。

3) 区块链不可篡改特性

在区块链中, 会对每一个区块的区块头做 SHA256 加密运算, 得到一个散列值。而每个区块的区块头中都包含其父区块的散列值, 所以当区块链中父区块的内容发生改变后, 该区块的散列值会发生改变, 导致其子区块的散列值也发生改变, 子区块散列变化又会导致子孙区块的散列值变化, 依次类推。这样的设计机制保证了数据的可靠性与一致性^[12-13], 数据一旦存入就很难被篡改。

4) 区块链应用

区块链技术不仅可以在金融领域发挥作用, 在非金融领域也能起到很好的效果。人工智能、大数据等新兴领域在信息安全角度对去中心化、分布式、可溯源追踪、高效率等方面要求较高, 区块链具备的去中心化、防篡改、可溯源追踪等特性与新兴产业在安全领域的发展需要较匹配, 因此可以将区块链技术应用于上述领域实际问题。

在信息安全领域, 目前区块链技术主要用于数据防护、访问控制、授权、身份认证等方向^[14]。区块链的去中心化结构可以保证已存储信息不被篡改, 隐私保护领域结合, 如基于区块链的隐私保护^[15]、基于区块链共识机制实现节点位置验证^[16]、基于区块链实现可信定位系统^[17]等。

3 基于区块链的 ARP 攻击防御方案

3.1 方案总体描述

在 ARP 执行过程中, 目标主机在接收到 ARP 广播包后会填写其 IP 和 MAC 地址, 并以单播方式向源主机发送响应包。由于协议缺少对 ARP 响应包发出主机的身份认证机制, 若攻击主机伪装成目的主机也向源主机发送 ARP 响应包, 则源主机可能会接收攻击主机发来的 ARP 响应分组, 并更新源主机上的 ARP 缓存表, 产生 ARP 攻击, 影响通信安全。

本文提出一种基于区块链技术的 ARP 攻击防御方法, 方案如图 2 所示。在局域网络基础上, 构建了一条区块链, 实现了网络内主机对区块链的查询和存储操作。通过更改区块链结构实现了 IP 地址有效修改机制, 方便主机节点快速查找 MAC 地址信息, 引用基于散列验证的加密机制保

证数据传输的完整性, 保证主机接收到的 MAC 地址与存储在区块链的值保持一致。在存储过程中, 利用信用评价机制确定交易处理顺序, 通过数字签名机制验证交易发起方身份, 保证交易的正确性, 实现了 ARP 攻击的防御。

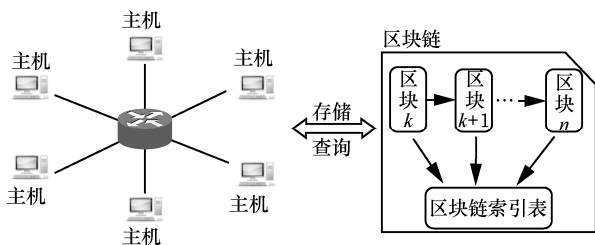


图2 方案模型

本方法主要利用区块链的不可篡改特性和交易验证机制保证数据存储的有效性, 防止数据被攻击者篡改。交易认证机制利用非对称密钥加密方法, 通过私钥对交易内容加密, 生成数字签名, 区块链中节点通过公钥对交易进行验证, 保证区块链中存储的数据是正常交易方发送的数据。由于区块链的链式设计, 后一个区块头中总是存储其父区块的散列值, 当父区块中的交易内容发生变化时, 父区块的散列值会发生相应变化, 从而与其关联的子区块头中存储的父区块散列值也会发生相应改变。而子区块的散列值变化后又会导致子孙区块的块头值发生变化, 从而导致连锁反应。当 ARP 攻击者试图改变某一区块中的交易内容时, 会导致该区块后的所有子孙区块的散列值发生改变, 每个子孙区块头部存储的父区块散列值也需要做相应修改, 并且每个保存有完整区块链结构的节点均需要完成上述操作, 篡改代价较大, 故可保证数据的安全性。

3.2 改进的区块链结构

在 ARP 通信过程中记录源主机 IP、MAC 地址以及目的主机 IP、MAC 地址。现有方案常采用 IP-MAC 静态绑定的方式来防御 ARP 攻击。但在局域网环境中, 无法保证 IP 地址一直不发生改变, 若发生改变, 则需要逐个更改局域网内设备先前绑定的 IP-MAC 值, 当局域网内设备数量较大时工作量也会随之增加。MAC 地址一般由设备网卡控制, 一般不会发生改变。

通过上述分析, 结合区块链的防篡改特性,

运用区块链思想,设计了适用于本问题的区块链结构,如图3所示。区块链环境由2部分构成,基于区块链思想设计的区块链以及在其基础上建立的区块链索引表。

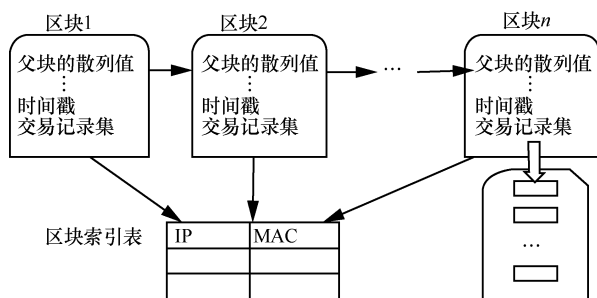


图3 改进的区块链结构

区块结构中包含父块的散列值、时间戳、交易记录集等信息。交易记录集包含某一区块内的所有交易信息,用键值对形式存储每条交易信息的具体数据。每条交易用于表示 ARP 响应包中返回的核心信息,包含被请求主机的 IP、MAC 地址、交易的发起时间等。交易号用于唯一标识一个交易,由交易中的 MAC 地址与时间戳做散列运算得到。将主机 IP 与 MAC 地址绑定到交易中,保证存储数据的一致及安全性。

为提高查询效率,在区块链基础上形成的索引表,当网络中主机信息发生变动时同步更新区块链索引表中存储的值。区块链索引表包含 IP 和 MAC 地址 2 部分。IP 代表设备的 IP 地址,MAC 地址表示设备的 MAC 地址。当局域网内某节点 IP 信息发生变化时,向系统发起新交易,通过验证后将交易加入区块内,挖矿后网络内其他节点

同步区块信息,更新区块链索引表中数据,保证表内存储的一直是网络内主机 IP 的最新值。

3.3 防御过程描述

1) MAC 地址查询过程

当局域网内某个节点想要通过 ARP 查询某一主机 MAC 地址时,首先查询区块链索引表,通过 IP 地址查询该主机的 MAC 地址,将查询到的结果加密传送给请求主机。主机将接收到的 MAC 地址与 ARP 表中查询出的 MAC 地址做对比,当两者一致时表示未遭受攻击,不一致时表示遭受攻击,以区块链中的查询结果为准进行更正。查询过程如图4所示,IP 为 10.0.0.5 的源主机想要查询 IP 为 10.0.0.6 的目的主机 MAC 地址。在区块链索引表中进行查找 IP 为 10.0.0.6 的表项,将该条表项内的 MAC 地址加密传送给源主机。

为了保证查询到的 MAC 地址能够完整、正确地传输到请求发送方,采用基于散列验证的分组加密方法保证传输过程^[18-20]。如式(1)所示,dMAC 表示通过区块链系统查询到的目的主机 MAC 地址,利用分组加密算法对 dMAC 值加密,将加密后的 dMAC 值发给源主机。接着对 dMAC 值做散列运算,并对运算后的结果进行分组加密,将加密后结果发给源主机。源主机接收到 2 次数据后,首先根据密钥 K 解密得到 dMAC,进行散列运算得到 $H(\text{MAC})_2$ 。然后同样通过 $D(E(H(\text{dMAC}), K), K)$ 得到 $H(\text{dMAC})$,比较 $H(\text{MAC})$ 和 $H(\text{MAC})_2$ 值。若一致表示传输数据完整、未被篡改,将 dMAC 值写入源主机的缓存表中。

$$\langle E(\text{dMAC} \| H(\text{dMAC}), K) \rangle \quad (1)$$

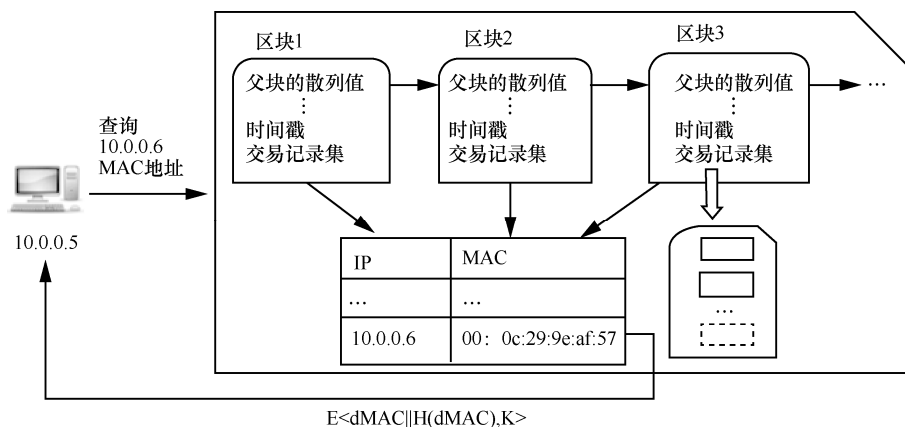


图4 查询过程

2) MAC 地址存储过程

当查询区块链索引表没有找到被请求 IP 时, 由被请求方发起一条新交易, 交易中包含其 IP 与 MAC 地址以及时间戳等信息。网络中节点会对交易发起方身份进行验证, 将交易加入区块内, 矿工节点根据设定进行挖矿操作, 直到有节点最先找到一个随机数, 能满足提前设定好的工作难度。其余节点在验证完该随机数的正确性之后将该条记录加入区块中。这里假设局域网内的所有节点均为矿工节点, 并且每个节点上保存有完整的区块链信息。

在 ARP 的处理过程中, 可能会遭受 ARP 攻击, 如图 5 所示。当主机 A 请求主机 B 的 MAC 地址时, 主机 E 作为攻击者也会发起应答。此时让 2 个应答者分别发起新交易, B 的交易包含 B 的 IP 和 MAC 地址、时间戳等, E 作为攻击中间人, 在交易中发送其 MAC 地址。主机 B 在发起交易时利用自己的私钥对交易内容进行签名, 将签名和交易发送到网络。主机 E 也会利用其私钥生成签名或伪造数字签名, 同样将签名和交易发送到网络。通过非对称密码验证思想, 网络中的节点根据提前存储的主机 B 的公钥验证 2 个交易, B 发起的交易通过验证, 而 E 发起的交易则验证失败。这样就阻止了主机 E 发起的 ARP 攻击, 避免存储错误的主机 B 的 MAC 地址。

为了保证正常节点与攻击节点同时发起交易时, 正常节点有较高处理级别, 在验证过程中引

用信用评价机制。信用等级从 1 开始, 每次成功通过验证, 该节点的信用等级会增加 1。当下次再出现正常节点与攻击节点同时发起交易时, 系统先根据信用级别确定交易发送队列, 级别值越大的优先级越高, 这样保证了正确交易信息可以被更快速地处理, 节省时间开销。同时也要考虑正常节点的操作频率问题, 如正常节点在某个时间段内频繁对节点 IP 信息进行修改, 笔者认为这种操作会导致网络资源浪费, 需要降低该正常节点已有的信用值。

3.4 安全性分析

针对 ARP 缺陷, 设计了基于区块链防篡改特性的攻击防御方法, 将主机 IP 与 MAC 地址作为交易内容存储到区块内。为了方便查询与对比, 在区块链基础上, 生成了交易索引表。定时将交易索引表中数据与主机 ARP 缓存表中内容做对比, 若两者不一致, 则表示检测到攻击, 系统及时将交易索引表中的查询结果替换到 ARP 缓存表的相应位置, 保证缓存表正确性, 有效防御后续攻击。

定理 1 交易数据具有不可伪造性。

证明 区块链的数字签名机制保证了攻击者无法伪造正常主机发送交易数据。交易发起方通过其自有的私钥对交易内容进行加密处理, 形成数字签名。网络内超过一半主机通过发送方公钥完成身份验证后才将交易加入具体区块中。除非攻击者已窃取到交易发起方的全部私钥信息, 否则无法伪造

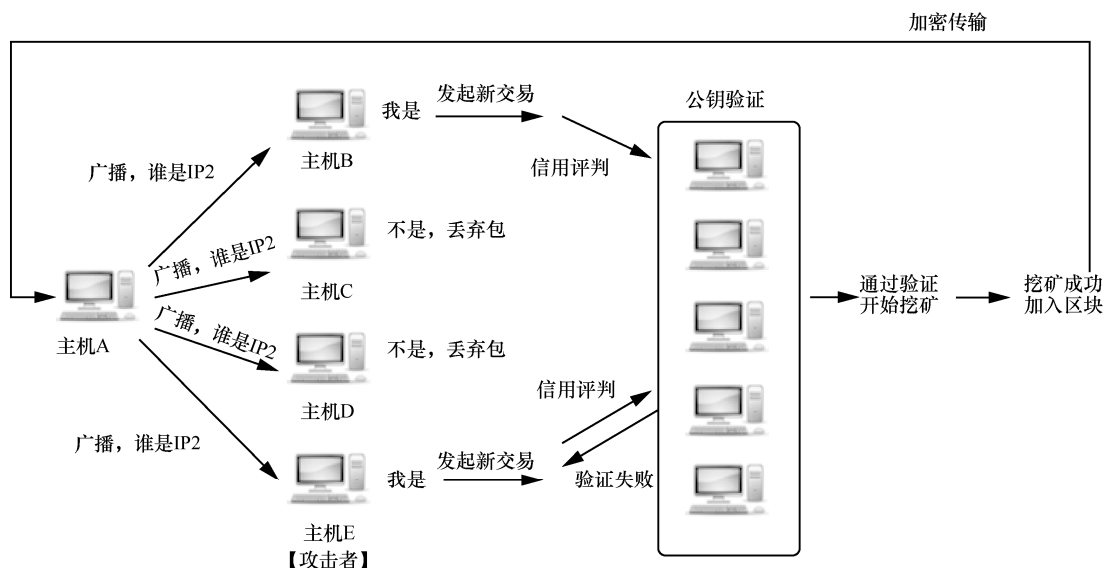


图5 新建交易

发起方发送包含错误数据的交易信息。

定理 2 攻击者对区块链中交易数据的篡改操作不会生效。

证明 假设攻击者试图修改区块链中某一区块中存储的交易数据。由于区块链的链式结构设计，相邻区块间具有很强的关联性，父区块的散列值变化后，子区块的散列值也会发生改变，子区块散列值变化后，子孙区块的散列值也会随之发生改变。因此若想修改某一区块内的交易数据时，必须修改其后所有子孙区块的散列值。同时，攻击者需要篡改所有存储完整区块链的节点，在节点上完成上述关联改动操作，攻击代价较大，故攻击主机对数据实施篡改的目的难以实现。

4 实验分析

本文搭建了由3个虚拟机构成的小型局域网环境，每个局域网节点安装Kali操作系统。局域网3节点的IP及MAC地址对应关系如表1所示。

表 1 局域网环境		
节点名称	IP 地址	MAC 地址
节点 A	10.0.0.5	00:0c:29:78:84:e5
节点 B	10.0.0.6	00:0c:29:9e:af:57
节点 C	10.0.0.7	00:0c:29:3f:d5:26

1) 正确性验证

假设节点 A 请求节点 B 的 MAC 地址，通过区块链索引表没有查询到节点 B 的 IP 信息，那么主机 B 会发起交易，将其 IP、MAC 地址、时间戳信息存入交易，用私钥 K 对交易签名后将交易放入具体区块中。同时攻击节点 C 也发起交易，伪装成节点 B，将错误的 MAC 地址放入交易，用伪造的私钥 K' 对交易签名，企图将错误信息存入区块链。两类交易信息对比情况如表 2 所示。通过身份验证机制的评判，节点 B 发起的交易验证成果，顺利存入区块。节点 C 发送的交易验证失败，交易未存入区块。主机 B 发送的交易顺利

存入区块，界面如图 6 所示。

页面日志			
序号	交易ID	发送方	MAC地址
1	0000000000000000000000000000000000000000000000000000000000000000	10.0.0.6	00:0c:29:9e:af:57

图 6 交易界面截图

2) 查询效率分析

通过区块链索引表和区块链结构设计，可以使节点方便快捷地查询出区块链中存储的被请求节点的 MAC 地址。对区块链中不同位置的区块交易记录做查询，统计查询性能。

这里对区块链中不同位置的 500 条交易记录做 MAC 地址查询，随机分 10 组，每组统计 50 条查询时间的平均值。如图 7 所示，index 代表通过区块链索引表查询 MAC 地址花费的时间，block 代表从区块链中直接查询 MAC 地址花费的时间，可以看出，本文改进的区块链结构具有较好的查询性能。

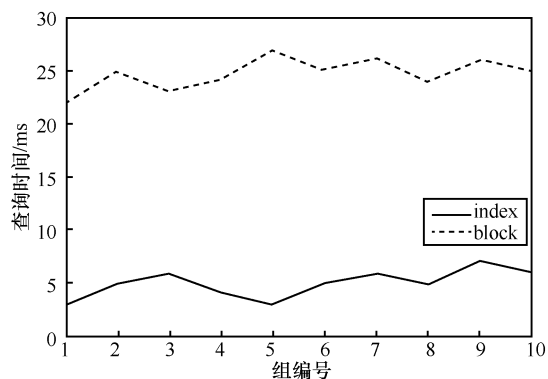


图 7 查询时间

3) 更新效率分析

当需要更新局域网内节点 IP 时，只需要进行 2 个操作过程。首先由 IP 更新节点重新发送一条新交易，将修改后的 IP 存入交易内，验证成功后交易就会加入区块中，等待节点挖矿。当某节点挖到区块后，其他节点进行同步更新，保证所有节点存储最长的区块链，同时更新区块链索引表。

假定每个区块包含 50 个交易，任选一个节点

表 2 两类交易对比						
交易类型	交易号	IP 地址	MAC 地址	时间戳	签名	验证结果
正常发送的交易	HASH (MAC+时间戳)	10.0.0.6	00:0c:29:9e:af:57	1528092267.83	私钥 K 对交易签名	正确
攻击者发起的交易	HASH (MAC+时间戳)	10.0.0.6	00:0c:29:3f:d5:26	1528092740.55	私钥 K' 对交易签名	错误

测试同步区块链所需的时间。如图8所示,横轴代表该节点与最长区块链长度的差值,纵轴代表同步所需的时间。从图中可以看出,随着区块链长度差距的增大,同步所需时间也随之增加,但当差距超过3个块时,时间增长率变缓,同步更新时间小于8 s。

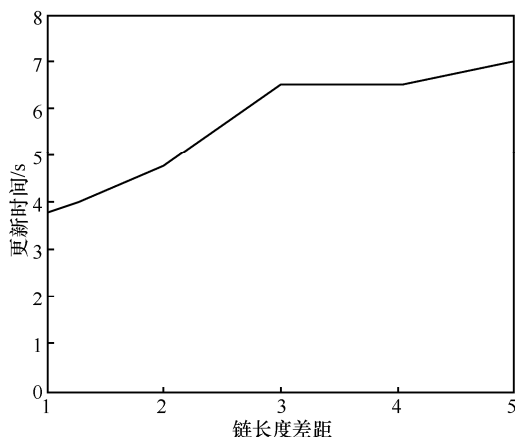


图8 更新时间

4) 处理时间对比

静态绑定方法的思路是固化 ARP 缓存表,防止攻击者修改表项内容。但在局域网环境中,当某主机发生更改主机 IP 的情况时,需要由管理者手动逐一修改网络内主机中包含该修改主机 IP-MAC 映射关系的静态缓存表项;当网络为新增主机分配 IP 时,同样需要管理者手动逐一增加网络内所有主机的静态缓存表项。当网络内主机数量较少时,该方法还比较适用,当主机数量较多时,该方法会产生巨大工作量,可用性较差。

本文方法基于绑定思想,在区块链结构上进行了改进,增加了区块链索引表结构。当局域网内有正常修改主机 IP 的操作时,该主机会主动发送包含修改后 IP 和 MAC 地址的交易,待该交易通过验证加入具体区块,挖矿后将交易索引表中的主机 IP 修改为最新值。该过程由区块链系统一次性自动完成,维护成本低。

用上述 2 种方法修改局域网内主机 IP,对比时间花费。实验从局域网内需要修改的主机数量出发,分别统计修改数量为 1、2、3 台的时间花费,取 10 次操作所需时间的平均值。如图 9 所示,横轴代表网络内需要修改的主机数量,纵轴代表修改操作花费的时间。可以看出,

随着修改主机数量的增加,本文提出的方法具有较好的时间优势。

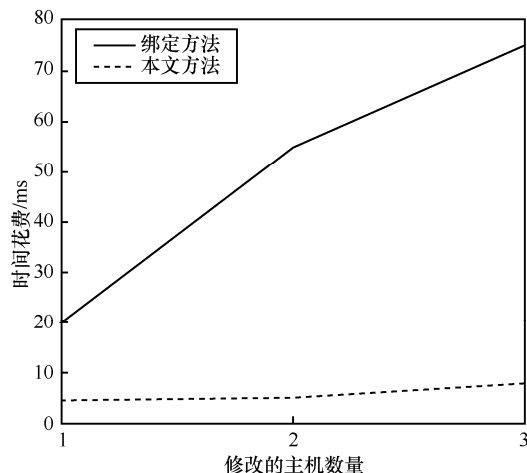


图9 2种方法耗时对比

5 结束语

本文基于区块链技术思想设计了一种 ARP 攻击防御方案。通过构建区块链环境,实现了网络内主机对区块链的查询和存储操作,保证了数据的安全性。通过更改区块链结构实现了 IP 地址有效修改机制,方便主机节点快速查找 MAC 地址信息,引用基于散列验证的加密机制保证数据传输的完整性,保证主机接收到的 MAC 地址与存储在区块链的值保持一致。在存储过程中,利用信用评价机制确定交易处理顺序,通过数字签名机制验证交易发起方身份,保证交易的正确性,实现了对 ARP 攻击的防御。

后续将进一步考虑提升该方案的安全性能,加入对时间指标的衡量,建立完善的信用评价体系,优先处理正确、信用值高的交易,减少等待时间,提升处理效率。

参考文献:

- [1] HONG S, OH M, LEE S. Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA[J]. Mathematical & Computer Modelling, 2013, 58(1-2): 254-260.
- [2] 徐书欣, 赵景. ARP 欺骗攻击与防御策略探究[J]. 现代电子技术, 2018, 41(8): 78-82.
XU S X, ZHAO J. Investigation of ARP spoofing attack and defense strategies[J]. Modern Electronics Technique, 2018, 41(8): 78-82.
- [3] 林宏刚, 陈麟, 王标, 等. 一种主动检测和防范 ARP 攻击的算法

- 研究[J]. 四川大学学报(工程科学版), 2008, 40(3):143-149.
- LIN H G, CHEN L, WANG B, et al. Research on an algorithm of active detecting and resisting ARP attack[J]. Journal of Sichuan University(Engineering Science Edition), 2008, 40(3):143-149.
- [4] 秦丰林, 段海新, 郭汝廷. ARP 欺骗的监测与防范技术综述[J]. 计算机应用研究, 2009, 26(1):30-33.
- QIN F L, DUAN H X, GUO R Y. Overview of ARP spoofing detection and prevention techniques[J]. Application Research of Computers, 2009, 26(1):30-33.
- [5] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2008.
- [6] 刘江, 霍如, 李诚成, 等. 基于命名数据网络的区块链信息传输机制[J]. 通信学报, 2018(1):24-33.
- LIU J, HUO R, LI C C, et al. Information transmission mechanism of Blockchain technology based on named-data networking[J]. Journal on Communications, 2018(1):24-33.
- [7] SWAN M. Blockchain thinking : the brain as a decentralized autonomous corporation [commentary][J]. IEEE Technology & Society Magazine, 2015, 34(4):41-52.
- [8] 张宁, 王毅, 康重庆, 等. 能源互联网中的区块链技术:研究框架与典型应用初探[J]. 中国电机工程学报, 2016, 36(15): 4011-4022.
- ZHANG N, WANG Y, KANG C Q, et al. Blockchain technique in the energy Internet: preliminary research framework and typical applications[J]. Proceedings of the CSEE, 2016, 36(15):4011-4022.
- [9] 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理:问题与方法[J]. 软件学报, 2018(1):150-159.
- QIAN W N, SHAO Q F, ZHU Y C, et al. Research problems and methods in Blockchain and trusted data management[J]. Journal of Software, 2018(1):150-159.
- [10] 朱建明, 付永贵. 基于区块链的供应链动态多中心协同认证模型[J]. 网络与信息安全学报, 2016, 2(1):27-33.
- ZHU J M, FU Y G. Supply chain dynamic multi-center coordination authentication model based on block chain[J]. Chinese Journal of Network and Information Security, 2016, 2(1):27-33.
- [11] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
- YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
- [12] 闵新平, 李庆忠, 孔兰菊, 等. 许可链多中心动态共识机制[J]. 计算机学报, 2018, 41(5): 1005-1020.
- MIN X P, LI Q Z, KONG L J, et al. Permissioned Blockchain dynamic consensus mechanism based multi-centers[J]. Chinese Journal of Computers, 2018, 41(5):1005-1020.
- [13] 刘明达, 拾以娟. 基于区块链的远程证明模型[J]. 计算机科学, 2018, 45(2).
- LIU M D, SHI Y J. Remote attestation model based on Blockchain[J]. Computer Science, 2018, 45(2):48-52.
- [14] 刘敖迪, 杜学绘, 王娜, 等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018.
- LIU A D, DU X H, WANG N, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7):2092-2115.
- [15] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: using blockchain to protect personal data[C]//2015 IEEE Symposium on Security and Privacy Workshops (SPW 2015). 2015: 180-184.
- [16] BRAMBILLA G, AMORETTI M, ZANICHELLI F. Using block chain for peer-to-peer proof-of-location[J]. arXiv:1607.00174, 2016.
- [17] 李大伟, 刘建伟, 关振宇, 等. 基于区块链的密钥更新和可信定位系统[J]. 密码学报, 2018(1).
- LI D W, LIU J W, GUANG Z Y, et al. Key update and trusted positioning system based on blockchain[J]. Journal of Cryptologic Research, 2018, 5(1): 35-42.
- [18] 于佳, 程相国, 李发根, 等. 标准模型下可证明安全的入侵容忍公钥加密方案[J]. 软件学报, 2013(2):266-278.
- YU J, CHEN X G, LI F G, et al. Provably secure intrusion-resilient public-key encryption scheme in the standard model[J]. Journal of Software, 2013(2):266-278.
- [19] 陈泯融, 张席, 何凯, 等. 改进的选择密文安全公钥加密方案[J]. 计算机学报, 2013, 36(6):1149-1154.
- CHEN M R, ZHANG X, HE K, et al. Improved public key encryption scheme secure against adaptive chosen-ciphertext attacks[J]. Chinese Journal of Computers, 2013, 36(6):1149-1154.
- [20] 李经纬, 贾春福, 刘哲理, 等. 可搜索加密技术研究综述[J]. 软件学报, 2015, 26(1): 109-128.
- LI J W, JIA C F, LIU Z L, et al. Survey on the searchable encryption[J]. Journal of Software, 2015, 26(1):109-128

[作者简介]



刘凡鸣(1990-), 女, 河北保定人, 河北大学实验师, 主要研究方向为区块链技术、云计算安全。



石伟(1992-), 男, 河北衡水人, 河北大学硕士生, 主要研究方向为信息安全、区块链技术、深度学习。