面向智能终端的快捷支付“双花攻击”检测模型

邓红莉，杨韬
（西华师范大学教育信息技术中心，四川南充 637002）

摘 要：双花攻击是基于去中心化结构的数字加密货币交易过程中存在的重要安全问题。主流的数字加密货币通过牺牲交易时间，等待全体节点验证的交易确认块数量达到预设值来对抗双花攻击。在手机、平板电脑等智能终端上由于硬件资源的限制以及对快捷支付的需求，以交易时间为代价的对抗方式显然无法满足应用场景的需求。对此，文章将人工免疫理论应用到数字加密货币的快捷支付中，提出一种面向智能终端的快捷支付“双花攻击”检测模型。该模型结合人工免疫理论，利用异常交易数据在每个交易节点训练免疫检测器，通过免疫进化与免疫应答机制对双花攻击进行快速检测并全网通报。实验结果证明，该模型能够有效预防数字加密货币快捷支付中的双花攻击。

关键词：数字加密货币；安全交易；双花攻击；人工免疫；异常检测
中图分类号： TP309.2 **文献标识码：** A

Fast payment "double spend attack" detection model for intelligent terminal

Deng Hongli, Yang Tao
(*China West Normal University Education and information technology center, SichuanNanchong 637002*)

Abstract: Double payment (double-spend attack) is an important security issue in the process of digital cryptocurrency trading based on decentralized structure. The current digital cryptocurrency counters the double-spend attack by sacrificing transaction time and waiting for the number of transaction confirmation blocks verified by all nodes to reach a preset value. Due to the limitation of hardware resources and the demand for fast payment on smart terminals such as mobile phones and Pads, the way of confrontation at the cost of transaction time obviously cannot meet the needs of application scenarios. In this regard, this paper applies the artificial immune theory to the fast payment of digital cryptocurrency, and proposes an immune-based "double flower attack" detection model. The model uses the abnormal transaction data to train the immune detector at each trading node, and the double-spend attack is quickly detected and broadcasted throughout the network through the immune evolution and immune response mechanism. The experimental results show that the model can effectively prevent double-flower attacks in fast payment of digital cryptocurrency.

Key words: digital encrypted currency;secure transaction; double-spendattack; artificial immunity; anomaly detection

1 引言

自从中本聪于2009年提出并实现比特币后，数字加密货币由于其去中心化、分布式、安全可靠以及匿名性等特性，成为一种广泛流通的虚拟货币。以比特币为例，其2017年单个比特币的价值最高约10万元，涨幅接近13倍[1]，2019年3月的市场价值约10000亿元。随着数字加密货币的发展，众多专家与学者开始关注其交易安全，而双花（Double Spending）攻击则是基于去中心化架构的数字加密货币交易过程中面临的最为重要的安全问题[2~4]。双花攻击又称“51%攻击”，是指攻击者利用算力优势（大于50%）强行修改合法的交易记录，实现一笔虚拟货币两次消费。以比特币为代表的主流数字加密货币，通过工作量证明的机制和一个记录所有确认交易的公共链来预防双花攻击，一笔交易成功后必须等待至少6个确认块，全过程大约需要1个小时[5]。等待的确认块越多交易过程越安全，但交易消耗的时间也越长。数字加密货币专家Rosenfeld推导了双花攻击成功概率与确认块数量成反比，同时等待时间与确认块数量成指数级上升[6]。艾尔兰学者Sompolinsky在爱尔兰国家科学基金支持下，研究了交易吞吐量与双花攻击成功率之间的关系，并计算了合法交易吞吐量的安全边界[7,8]。

目前，智能手机与平板电脑上的各类应用是数字货币交易的主要平台。一方面这类终端硬件资源有限，另一方面其所承载的金融应用通常对时效性要求较高，需要实现快捷支付。但是，传统的双花攻击防御策略只适用于交易时间达到几十分钟的慢支付场景。在快捷支付场景中，货物与货币的交易时间非常短（几秒到几十秒），如手机确认支付后立即进行货物交接或服务（如自动售货机和快餐支付）。而数字加密货币用户可能同时拥有多个匿名账户，当攻击者得到货物或服务后实施双花攻击，将难以核实攻击者真实信息。欧盟国家经济（NEC）实验室研究员Karame与Bambert分析了快捷支付中的双花攻击，并认为目前主流数字加密货币中的安全策略无法有效预防快捷支付中的双花攻击[9~11]。

为此，本文基于安全领域最新的人工免疫理论，提出了一种基于免疫的数字加密货币快捷支付“双花攻击”检测模型。在该模型框架中，数字加密货币的交易节点上会加入一个基于免疫方法的检测模块，该检测模块的主要功能是提取交易数据的抗原特征，利用提取的抗原特征生成检测器检测双花攻击，将检测到双花攻击的检测器传递给交易网络中的其他节点以及威胁监控中心，以便其他节点能快速的检测到此双花攻击。

2 双花攻击简介（以比特币为例）

比特币是目前最成功、市值最大的数字加密货币，其它主流数字加密货币都采用了与比特币类似的技术或模式，本节首先以比特币为代表介绍数字加密货币的工作原理，然后分析数字加密货币快捷支付中双花攻击实施的条件。

比特币支付无需第三方认证机构确认交易的正确性以及合法性。每个用户（比特币节点）将可参与交易的合法性验证以及确认，所有合法的交易将被记录在一个公开的账本上，每个节点都可无条件的得到该账本，账单的记录呈链表的方式，后来加入的账单都有前一个账单的地址信息，支付、收入比特币的地址、比特币的数量、支付的时间等信息。参与交易验证的节点便是矿工节点，他们利用CPU计算资源进行挖矿（利用CPU资源计算随机数），通过工作量证明（POW）机制进行账单记录权的争夺，胜利者将得到一份比特币作为奖励。当矿工争夺到账单记录权时，其将发送信息告诉其他比特币网络中的矿工。根据比特币白皮书中的说明可知[4]，比特币网络以交易时间为代价来累积确认交易区块的高度从而对抗双花攻击。如图1比特币快捷支付中双花攻击示意图所示，攻击者首先发送正常交易TRv给卖主，然后用同样的比特币发送交易TRa到一个共谋的地址，当攻击者得到货物或服务并且交易TRa在下一个区块得到确认时，双花攻击成功。

然而在比特币快捷支付领域，交易发生的时间较短，双花攻击的可能性极大的提高。快捷支付中的双花攻击如图1所示，成功实施一个双花攻击必须满足三个条件。

（1）正常的交易TRv必须先添加到卖主的比特币钱包中（第一次花费），双花交易TRa后续添加（第二次花费）。根据比特币协议，广播时后到

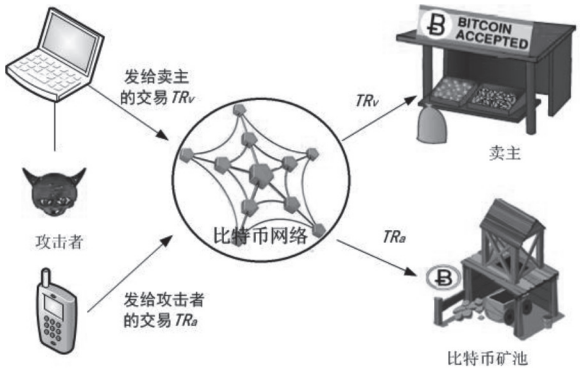

图1 比特币快捷支付中双花攻击示意图

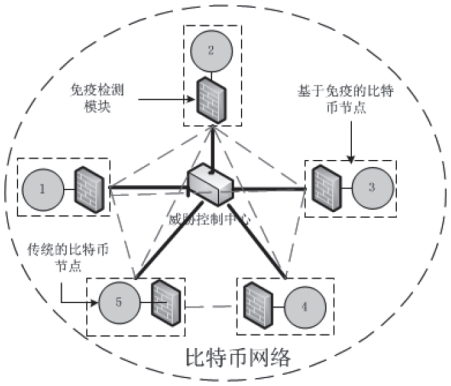

图2 基于免疫的检测模型体系架构图

达的同源交易将被丢弃，若正常交易TRv比双花交易TRa后到达卖主节点，它将被丢弃掉，卖主将要求攻击者重新支付，双花交易TRa变为正常支付，攻击失败。

（2）双花交易TRa在有效时间内被区块链多数节点确认，如果交易TRv先被区块链多数节点确认，那么交易TRa就不会被接下来的区块所接受，攻击者的双花攻击将失败。

（3）卖主的服务时间必须远小于检测到异常所需的时间。因为比特币用户是匿名的，而且一个用户可拥有多个账号，所以当服务结束了，即使卖主意识到了异常，也很难鉴别出攻击者，导致双花攻击的可能性增大。

3 基于免疫的数字加密货币快捷支付“双花攻击”检测模型

为解决快速交易中可能出现的双花攻击，本文提出一种基于免疫的数字加密货币快捷支付“双花攻击”检测模型（Immune-based Digital Cryptocurrency Fast Payment "Double Spend Attack" Detection Model, IMDM）。如图2所示（以比特币交易为例），IMDM由大量的基于免疫的数字加密货币节点以及威胁控制中心通过数字加密货币网络链接组成，其中基于免疫的数字加密货币节点包括传统的数字加密货币节点和检测模块，检测模块的功能是检测异常行为并与其他节点通过数字加密货币网络直接或间接的进行信息共享以及互动联防，而网络中的数字加密货币威胁控制中心将接受疫苗或发送疫苗到各个节点，以及接受各个节点的联动防御请求。这种疫苗发放的策略与生物免疫中的“二次应答”相似，极大地减少了成熟检测器训练周期，从而降低了对硬件资源的需求；而检测器对异常交易特征的学习能力使得成熟检测器能够快速匹配到攻击数据，从而降低了检测时间。

为描述本检测模型，本文需要定义一些基本概念。定义字符串集合$\Omega = \bigcup_{i=1}^{\infty}\{0,1\}^i$；数字加密货币网络中的交易数据包$\Upsilon \subset \Omega$，集合$\Psi = \bigcup_{i}^{n} = 1 \Psi_i, \Psi_i = \{x = \ < x_1, \cdots, x_j, \cdots, x_d > | x_j \in \Upsilon\}$，其中n是Ψ数量，d是x的维度大小。x是类似于数字加密货币网络中交易数据包的特征码。集合$\Re = \{< a, b > | a \in \Psi, b \in \Upsilon\}$，抗原集合$Ag \in \Re$，其中$\forall x \in Ag, x.b$是数字加密货币原始的交易数据包，x.a是数据包x.b的特征码，主要包括时间戳、交易哈希值、数字加密货币原地址、数字签名、数字加密货币数量等内容。抗原集合Ag包括自体集合Self和非自体集合Noself两个子集，满足条件$Self \cup Nonself = Ag, Self \cap Nonself = \emptyset$。在此检测模型中，自体集合为数字加密货币网络中的正常数据包，非自体集合为双花攻击数据包。检测器集合$Dts = \{\bigcup_{i=1}^{n} dt_i | dt_i = < a, age, count > | a \in \Psi, count \in N, \ age \in N\}$，其中n是检测器集合Dts的数量，a是检测器dt的抗原特征，age是检测器dt的年龄，count是检测器dt匹配到的非自体抗原的数量。检测器集合Dts包含三种类型的检测器：未成熟检测器I、成熟检测器T和记忆检测器M，未成熟检测器是初始生成的检测器，当其在耐受阶段没有匹配到自体抗原时将进化为成熟检测器。成熟检测器在其生命周期内匹配到足够的非自体抗原，其将进化为记忆检测器。因此，$I = \{x | x \in Dts, x.age < \lambda \wedge x.count = 0\}$，$T = \{x | x \in Dts, \ \forall y \in Self, f_{match}(x.a, y) = 0 \wedge \lambda \le x.age \le \ max\_age \wedge x.count < \ \beta\}$，

$M=\{x|x\in Dts,\quad \forall y\in Self, f_{match}(x.a,y)=0\wedge x.age\geq max\_age\wedge x.count\geq\beta\}$，其中$\lambda$是耐受周期，$\beta$是成熟检测器进化为记忆检测器的阈值，f_match是基于检测器和抗原的亲和度的匹配函数:如果亲和度大于特定的阈值就返回1，否则返回0。匹配函数可以是r位连续匹配、汉明距离、欧拉距离等[12]。

图3为检测模块的框架图，共有三个主要步

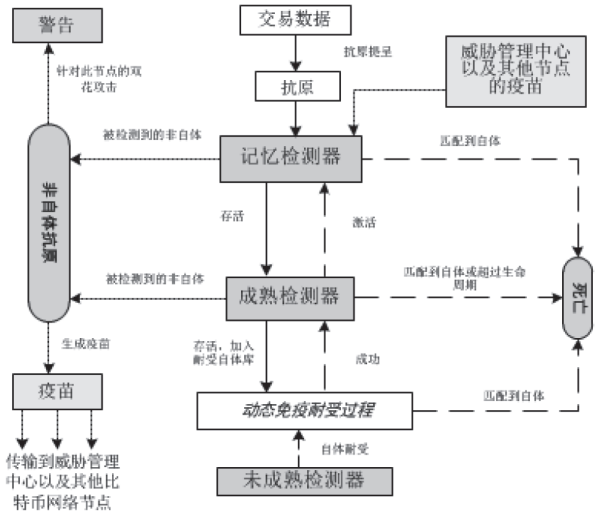

图3 检测模块的框架图SelfDetector

骤：（1）自体集Self的动态演化。提取的数字加密货币交易的抗原由记忆检测器和成熟检测器进行检测，其中在生命周期内没有被检测到的抗原将添加到自体集合中，并用于动态免疫耐受阶段；（2）检测器的动态演化。新生成的未成熟检测器需要进行自体耐受，经过自体耐受的未成熟检测器将进化为成熟检测器，而其中检测到自体的未成熟检测器将被删除(否定选择算法[12])。成熟检测器有一个生命周期，在生命周期内检测到足够的非自体抗原的成熟检测器将进化为记忆检测器，否定它将死亡(被删除)。记忆检测器检测到了自体抗原时将会被删除，否则将一直存在；（3）攻击检测和生成疫苗。从数字加密货币交易中提取抗原特征，当一个非自体抗原(双花攻击)被成熟检测器检测到时，检测模块将生成对应的疫苗并将其发送到数字加密货币网络中的其他的免疫节点，以及威胁控制中心。如果此双花攻击时针对本节点，该节点的检测模块将显示一个警告信息给该节点的拥有者。

4 模拟实验及结果分析

本小节将利用真实交易数据集对基于免疫的数字加密货币交易异常模型进行模拟实验，根据检测模型描述，抗原被定义固定长度的字符串，包括数字加密货币源地址、时间戳、交易哈希值、签名信息、数字加密货币的数量等。表1为从数字加密货币交易中提取的特征的字段结构描述以及其大小。为了测试该模型的性能，本文从数字加密货币门户网站(https://block chain.info)采取真实数据集包括2000个正常交易数据（自体）和1000个双花攻击数据（非自体）。其中一半的自体（正常交易数据）被选为训练集合，剩下的数据作为测试集合。

表1 提取的数字加密货币交易的字段

序号	字段名	大小(字节)	备注
1	hash	4	交易单的哈希值
2	timestamp	64	交易发生的时间
3	version	4	此交易版本号
4	flag	2	交易验证性标签
5	value	8	交易的数字加密货币数量
6	fees	64	交易的手续费用
7	tx_in	32	数字加密货币来源地址
8	tout	32	交易的目的地址
9	size	8	交易的长度
10	script	64	加密标记

模型参数的选取规则一般根据具体的真实网络环境来确定。由于自体self的动态定义，耐受周期的大小λ决定了成熟检测器生成的速度，而生命周期max_age决定了成熟检测器的死亡速度，其中生命周期的取值应该大于耐受周期，以保证生成足够的成熟检测器。激活阈值β决定成熟检测器转化为记忆检测器的速度，其取值越小越能快速产生记忆检测器。自体集合的大小max_s取决于计算机的处理能力，如果不影响系统的运行效率，尽可能的取一个较大的值，以保证更好的检测效果。因此，在本实验中，本文分别设置λ=2,max_age=8,max_s=500,β=3。检测率DR和误报率FAR作为本实验的两个对比评价标准，其计算方式定义为：

$$DR=\frac{TP}{TP+FN},FAR=\frac{FP}{FP+TN}$$

其中，TP、TN、FP、TN分别是正确肯定的非自体的数量、正确否定的自体数量、错误肯定的自

体数量和错误否定的非自体数量。

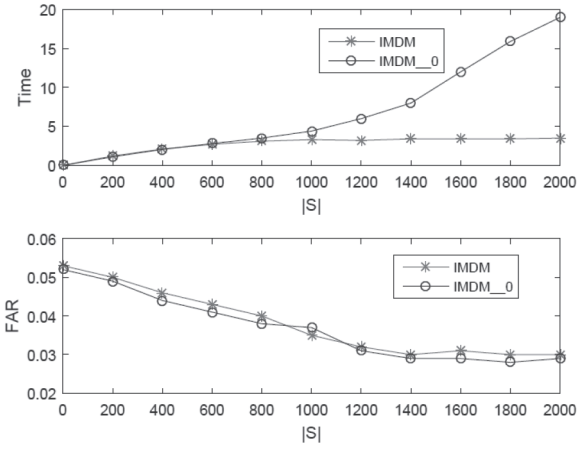

图4 自体数量对检测器训练的影响

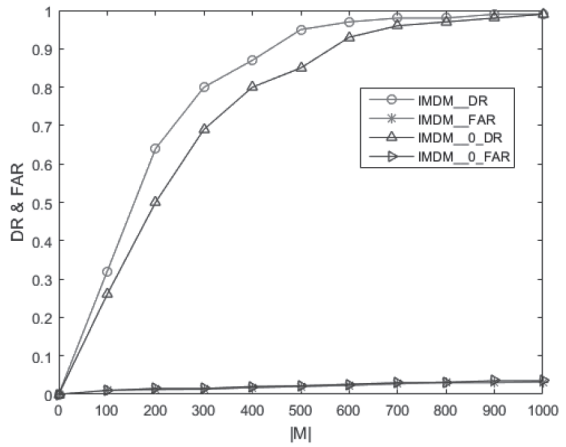

图5 IMDM在模拟环境中的检测性能

图4展示在不同自体数量下IMDM和IMDM_0模型的性能对比结果,其中MDM_0是IMDM模型未加入自体动态进化以前的模型，生成成熟检测器的数量是500个,|S|是自体集合的大小。从图4中可以看出，在自体数量小于max_s(500)以前，两个模型的成熟检测器生成的时间代价相差不大，但是超出max_s后IMDM由于采用了自体动态进化机制，参与免疫耐受的自体数量是固定的一个常数，因此生成固定数量的成熟检测器时，时间复杂度不会随自体规模的增加而剧烈增长。而图4中下图可以看出，因为动态进化规则剔除的是一些旧的、无用的自体，所以采用动态进化机制的IMDM并未增加模型的误报率FAR。

在检测器训练完毕后，本文利用Ubuntu内部测试环境对成熟检测器的性能进行进一步验证。一共初始化5个测试节点，每个测试节点随机向测试网络发送正常或双花攻击数据。为了模拟智能终端资源受限的真实场景，每个节点只运行比特币钱包程序和免疫节点管理程序（负责检测器进化、分发与匹配）。而成熟检测器被激活后会进化为记忆检测器，所以记忆检测器的数量大小|M|代表着成熟检测器和记忆检测器的检测能力。图5展示模型IMDM在不同检测器数量|M|下的检测性能，其中自体的数量为1000。从图中可以看出，两个模型的误报率FAR相差不多，几乎为0，表示模型能有效的识别自体集合。随着|M|的增加，两个模型的检测率DR随之增加，并且IMDM的检测率优于IMDM_0。当|M|大于600时，IMDM几乎能识别所有的攻击，随着记忆检测器的增加，模型的检测能力得到大幅度的上升，这表示模型具有较强的自学习能力。图6展示不同数量记忆检测器|M|的情况下，模型IMDM所消耗的时间代价。IMDM由于有检测器的动态演化，生成的检测器能更快的检测到攻击，所以其消耗的时间比IMDM_0更小，当|M|为1000时，时间代价最大，但也小于5s，这表示此模型能快速的检测出双花攻击，所以它能适用于数字加密货币快速支付的情景。

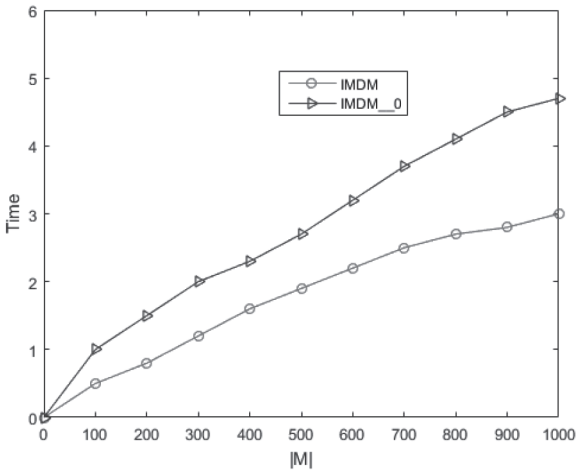

图6 IMDM模型的时间效率

5 结束语

数字加密货币在智能终端平台上的快捷支付是数字加密货币发展的一个重要领域。本文提出的基于免疫的数字加密货币双花攻击检测模型IMDM，从体系架构到自体、检测器的动态演化，以及具体的检测策略都满足了智能终端硬件资源受限，对检测时效性高的具体需求。实验结果表明IMDM能够

有效的检测出双花攻击，能够适应数字加密货币的快捷支付场景。

基金项目：

1.四川省科技厅苗子工程重点项目（项目编号：2019JDRC0084）；

2.南充市科学与技术研发项目（项目编号：17YFZJ0016）。

参考文献

[1] Coin Market Cryptocurrency market capitalization [EB/OL]. https://coinmarketcap.com/curren cies/bitcoin/historical-data/.March 15, 2018.

[2] F. Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016,(2):42－47.

[3] 张明德, 张清国, 毕马宁. 基于区块链技术的比特币安全性研究[C].全国网络安全等级保护技术大会. 2017.

[4] 赵甜,魏昂,周鸣爱. 区块链安全发展现状、问题与对策研究[J]. 网络空间安全,2019,11：21-25.

[5] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2009.

[6] Meni Rosenfeld. Analysis of hashrate-based double spending[J]. Eprint Arxiv, 2014.

[7] Yonatan Sompolinsky. Secure High-Rate Transaction Processing in Bitcoin[J]. Springer Berlin Heidelberg, 2015.

[8] Yonatan Sompolinsky Bitcoins security model revisited [EB/OL]. https://arxiv.org/abs/ 1605.09193. May, 2016.

[9] Ghassan O Karame, Elli Androulaki, and Srdjan Capkun. Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin[C]. In Conference on Computer & Communication Security, 2012.

[10] Ghassan O Karame, Elli Androulaki, Srdjan Apkun. Misbehavior in bitcoin: A study of double-spending and accountability[J]. Acm Transactions on Information & System Security, 2015,18(1):1－32.

[11] T Bamert, C Decker, L Elsen, and R Wattenhofer. Have a snack, pay with bitcoins[C]. In IEEE Thirteenth International Conference on Peer-To-Peer Computing, 2013.

[12] Stephanie Forrest, Steven A Hofmeyr, and Anil Somayaji. Computer immunology[J]. Immunolo gical Reviews, 2007,216(1):176－197.

作者简介：

邓红莉（1982-），女，汉族，四川遂宁人，四川大学，博士，西华师范大学，副教授；主要研究方向和关注领域：深度学习、自然语言处理。

杨韬（1982-），男，汉族，四川遂宁人，四川大学，博士，西华师范大学，副教授；主要研究方向和关注领域：网络空间安全、人工免疫。