基于隐马尔科夫随机场-置信能量场模型的信任邻域网络体系结构

陈子涵[1),2),3),4)] 程 光[1),2),3),4)] 唐舒烨[1),2)] 蒋山青[1),2),3)]
周余阳[1),2),3),4)] 赵玉宇[1),2),3),4)]

[1)](东南大学网络空间安全学院 南京 211189)
[2)](教育部计算机网络和信息集成重点实验室(东南大学) 南京 211189)
[3)](网络空间国际治理研究基地(东南大学) 南京 211189)
[4)](紫金山实验室 南京 211111)

摘 要 万物互联已成为未来网络发展的必然趋势,维护网络的整体性安全与鲁棒性在万物互联环境下相较于维护单一节点的安全更加重要与可行,而信任体系结构则是网络整体性安全的基础.信任链是一种链式拓扑的信任体系结构空间模型,通过定性化主动验证来构建网络内的持续信任关系,但链式拓扑的缺陷与定量信任度量的缺失使之无法适应万物互联网络环境.本文提出以信任分形网络拓扑和信任邻域扩散传递模型为基础的信任邻域网络体系结构,设计了隐马尔科夫随机场模型与置信能量场模型,结合门限控制模型,实现信任的定量度量与管理.数学分析与仿真实验表明,本文提出的体系结构能够定量度量与管理信任空间关系,打破攻击者无限攻击限期的100%整体网络攻击成功率,在10至1000个节点的14种不同节点规模下将整体网络攻击成功率最低降至39%;增加其平均理论攻击成本至2倍以上,保障网络系统的鲁棒性与整体安全性.

关键词 万物互联;整体性安全;信任体系结构;信任邻域网络;隐马尔科夫随机场;置信能量场
中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2021.02447

Trust Neighborhood Network Architecture Based on Hidden Markov Random Field Model-Confidence Energy Field Model

CHEN Zi-Han[1),2),3),4)] CHENG Guang[1),2),3),4)] TANG Shu-Ye[1),2)] JIANG Shan-Qing[1),2),3)]
ZHOU Yu-Yang[1),2),3),4)] ZHAO Yu-Yu[1),2),3),4)]

[1)](*School of Cyber Science and Engineering, Southeast University, Nanjing* 211189)
[2)](*Key Laboratory of Computer Network and Information Integration of Ministry of Education (Southeast University), Nanjing* 211189)
[3)](*International Governance Research Base of Cyberspace (Southeast University), Nanjing* 211189)
[4)](*Purple Mountain Laboratories, Nanjing* 211111)

Abstract Whether it is the traditional Internet or the emerging Internet of things, security has always been the top priority in the network environment. With the upgrading of communication technology and the development of the Internet and the Internet of Things (IoT), the Internet and the IoT will be integrated into the Internet of Everything (IoE). With the expanding scale of network, the security problem will be more serious in the IoE environment. Hence, maintaining the overall security and robustness of the network is more important than maintaining the security

收稿日期:2019-11-18;在线发布日期:2020-05-28.本课题得到国家重点研发计划项目课题(2018YFB1800602,2020YFB1804604)资助.
陈子涵,博士研究生,主要研究方向为网络空间安全、加密流量分类与识别、信任体系架构、复合深度学习、网络空间治理.E-mail:zhchen@njnet.edu.cn.**程 光**(通信作者),博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为网络安全、网络测量、加密流量识别、流量行为分析、主动防御.E-mail:gcheng@njnet.edu.cn.**唐舒烨**,硕士研究生,主要研究方向为网络空间安全、VPN网络流量分析.**蒋山青**,博士研究生,主要研究方向为网络弹性、SDN架构、区块链应用.**周余阳**,博士研究生,主要研究方向为网络空间安全、移动目标防御、入侵检测.**赵玉宇**,博士研究生,主要研究方向为网络测量与行为学、下一代网络处理器.

of a single node in the IoE environment, and trust architecture is the foundation of the overall security of the network. The current mainstream trust architecture is a trust chain model and it is a space model of trust architecture with chain topology as the transmission relation topology, which is widely applied in the Internet identity security authentication system, such as the PKI-CA system. It constructs the continuous trust relationship within the network through qualitative active verification. However, a large number of studies have shown that the defects of chain topology and the lack of quantitative trust measurement make it unable to adapt to the Internet of everything environment. In this paper, we propose a new generation trust architecture: trust neighborhood network, which is based on Hidden Markov Random Field Model-Confidence Energy Field (HMRFM-CEF) model. First of all, we innovatively introduce fractal network into the trust architecture, which is a special mesh topological structure which can guarantee the spatial robustness of overall network. Then, a trust neighborhood diffusion transfer concept in which trust nodes only have interaction with others in their own neighborhood is proposed. The concept can describe the transitive relation of trust in the fractal network spatial structure and construct it into trust neighborhood network. As a supplement of current trust architecture, a quantitative trust management model which contains credibility and trust layers are proposed. They are used to describe the trust transfer and management of the new generation of trust architecture. Afterwards, by integrating Markov random field model and hidden Markov model, we propose the mathematical modeling of trust neighborhood network with Hidden Markov Random Field Model (HMRFM), so as to realize the quantification of trust relationship and description of trust state from the mathematical perspective. Moreover, a Confidence Energy Field model based on HMRFM is proposed based on the properties of potential energy model and trust characteristics of Markov random field model. HMRFM-CEF solves the problem that the trust of the architecture requires to be initialized if the trust is needed to be calculated. Finally, we put forward the Trust Threshold Control model (TTC). By combining HMRFM-CEF with TTC, the architecture realize the calculation of trust under the dynamic change of trust relationship. Mathematical analysis and simulation experiments show that compared with trust chain architecture, the architecture proposed in this paper can quantitatively measure and manage the spatial relationship of trust, break the 100% overall network attack success rate in the case of unlimited attack duration, and reduce minimally to 39% respectively at the scale from 10 to 1000 nodes. It guaranteed that the average theoretical attack cost is increased to more than 2 times to ensure the robustness and overall security of the network system.

Keywords Internet of everything; integral security; trust architecture; trust neighborhood network; hidden Markov random field; confidence energy field

1 引 言

随着通信技术的更新换代以及移动互联网、物联网技术的发展,互联网与物联网将融为一体,“万物互联”将成为网络发展的必然趋势,连接对象将从人、家庭、企业扩展到万物,连接规模将成倍增长.在万物互联环境下,安全仍是网络环境的重中之重.但在海量节点规模下,想要保证每个节点的自身安全是相对困难的,而在大部分情况下只需要保证网络的整体安全性,这便是信任体系结构的意义所在.以 Mirai 为首的物联网病毒与以 WannaCry、GlobeImpost 为首的勒索病毒等,对现今网络环境构成了重大威胁,体现出以信任链为首的传统信任体系结构在现今网络环境下已经落后且有漏洞.

信任链是一种特殊的以链条为信任传递关系拓扑的模型,通过定性化主动验证来构建网络内的持续信任关系.信任链广泛地用于可信计算技术和互联网

身份安全认证体系中，其中最典型的就是 PKI-CA 体系.但是大量研究表明，信任链 PKI-CA 体系存在大量安全漏洞[1-6].

互联网安全隐患主要来源于匿名上网(传统 IP 协议名址不分)，万物互联将使这个问题更加突出.作为在现有互联网中占主流的链式信任模型，信任链的链式结构信任关系中任何一个节点的被攻击劫持都会造成整条信任链的崩溃.以信任链模型最常见的 PKI-CA 体系为例，不法分子只需要成功入侵一个 CA，就可以颁发假凭证，破坏整条信任链，造成该系统下信任关系的全面崩溃，整个系统都会受到安全威胁；且通信一方只能通过证书获取到对方通信者的个人信息，并没有办法确认使用该物与自己通信的是否真正的是那个“人”.再者，信任链 PKI-CA 体系只进行了定性的信任管理模式，并未实现定量化的信任管理，导致行为与信任之间的失衡.系统地说，信任链体系结构缺乏拓扑鲁棒性，且是一种定性化主动认证体系结构，不包含被动认证的方法，也无法进行信任的量化度量与差异性定量管理.主动认证虽然可以迅速、高效地构建信任体系，但它无法应对劫持和欺骗，且无法获取节点信任关系在空间维度上的动态变化.

万物互联作为现有各类网络的集大成者，具有节点众多、用户众多、自治域众多、网络复杂、整体鲁棒性需求高、权限多样且复杂等特征.信任链 PKI-CA 体系通过证书构建信任链，在节点、用户数量较多的情况下，需要颁发大量的证书，构建较长的链式结构，链式拓扑的缺陷导致其中某一环节的崩溃都将使整条信任链不安全；众多的自治域导致信任链模型必须要建立大量的 CA 进行控制，这增加了大量的网络运行成本和不安全性；复杂网络中为保证整体鲁棒性，则需要建立大量的信任链，各个信任链之间还有交叉与重复，这与最优化网络管理和信任链本身追求的降低成本的初衷背道而驰；且信任链定量信任度量的缺失(通过证书来二元化确定是否具有某项权限)与万物互联网络中多样化复杂权限管理的需求不相匹配.因此信任链模型已经无法适应万物互联网络环境.

那么如何在万物互联的环境下，提出一套新的信任体系结构，突破传统信任链体系结构的束缚，保障网络整体性安全与鲁棒性，则是亟待研究的问题.

针对现有传统信任体系存在的问题，本文提出新一代信任体系架构——信任邻域网络.我们首先将分形网络拓扑结构定为新一代信任体系结构的空间拓扑，分形网络拓扑结构相较于信任链的链式拓扑结构而言具有路径鲁棒性特征与节点鲁棒性特征，可以从根本上提高信任体系架构的鲁棒性.接着，我们提出了信任邻域扩散的概念，描述信任在空间架构中的传递关系，信任节点只与自己相邻的其他信任节点产生信任交互关系，整体网络信任以当前节点为中心向外扩散.然后我们对信任度进行了量化定义，提出隐马尔科夫随机场模型对整个信任邻域网络进行数学建模，从数学的角度进行信任传递关系的刻画.最后我们提出基于隐马尔科夫随机场模型的置信能量场模型，实现定量信任管理体系的初始化；结合信任门限控制模型，描述信任在空间维度上的定量信任管理动力学机理，实现整个信任邻域网络的构建与管理.

与现有的信任体系对比，本文所提出体系结构的贡献如下：(1)引入分形网络构建分形网络空间拓扑结构，突破信任链链式拓扑的局限，为网络整体鲁棒性奠定基础；(2)提出信任邻域扩散的概念与隐马尔科夫随机场模型，将信任体系结构建模为信任邻域网络模型，实现信任关系的动态传递；(3)在隐马尔科夫随机场模型的基础之上，结合信任的定量度量，提出基于隐马尔科夫随机场模型的置信能量场模型，实现信任的量化管理；(4)在置信能量场的基础上，结合信任门限控制模型，构建完整的信任邻域网络体系结构，打破攻击者无限攻击限期的 100%整体网络攻击成功率，增加其平均理论攻击成本，最终实现网络整体安全性的提高.

本文第 1 节介绍万物互联网络环境特点、传统信任体系结构的背景知识与新一代信任体系结构的研究意义；第 2 节介绍信任管理模型的研究现状，并阐述信任传递体系、分形网络和现有信任体系结构的研究进展；第 3 节提出信任分形网络拓扑、信任邻域扩散传递关系与基于信任度的定量信任管理模型，描述新一代信任邻域网络体系结构；第 4 节在第 3 节的基础之上，提出隐马尔科夫随机场模型对信任邻域扩散传递关系进行数学建模；提出基于隐马尔科夫随机场的置信能量场模型建模信任的定量度量与管理，最终提出门限控制模型作为信任邻域网络信任动力学机理的完善；第 5 节通过案例定性分析、数学定量分析与仿真实验对比分析的方式，论证该体系结构的有效性；最后一节总结全文工作，并展望未来的研究.

2 相关工作

2.1 信任管理模型研究进展

在庞大的网络中,节点之间的有效信任管理是现代网络中的基本要求,现有的信任模型构建主要基于传统信任链模式,包括基于私密未知密码(SUC)的不可克隆单元构建通信安全信任链[7]、基于双向传递模型的嵌入式系统可信链[8]和 TCSE 信任链模型[9].但是传统信任链体系结构仍然存在如下的问题:(1)信任链的信任只能逐层传递,不能跨层传递和动态交互,体系结构存在安全缺陷;(2)由于缺少可信度量数学模型和信任链组合安全模型,信任链的规范性与安全性尚未得到充分验证.

针对信任链存在的安全问题,现有研究提出了采用信任域和信任网络[1]以构建信任管理模型;在物联网环境下,利用物联网自身的域特性,提出网关信任体系结构构建信任域[2];且通过自认证 ID 技术(SCID)构建物联网可信网络系统[3],实现物联网智能服务信任域.

学术界认为信任网络模型具有以下优点:(1)更为直观,能够通过有向加权图的形式清晰地表现出主体间信任传递关系的走向;(2)模型抽象过程信息损失较少,同时能够比较真实地反映现实网络在结构上的特点;(3)能够应用于宏观网络层面信任传递问题的研究,可以体现网络结构对主体的影响,反映多主体之间复杂的交互行为.

不过现有的信任网络模型主要拘泥于对信任链的扩展,通过信任网络自身的网络结构鲁棒性来构建信任域,且主要在物联网领域固定而简单的节点群中构建,具有一定的适用局限性.

本文在现有信任网络模型的基础上,引入分形网络,进一步提高整体模型的鲁棒性,并使其可以适用于互联网和万物互联的网络环境中,解决了现有信任管理模型适用范围窄、具有拓扑局限性的问题.

2.2 信任传递体系的研究进展

信任传递体系是对不同情境下主体间信任传递过程的抽象,通过提取特定情境中主体间的信任传递机制来构建信任度计算方法,计算经过信任传递后各主体的信任度.对信任传递体系的研究,主要集中于信任度的计算与信任传递领域.

在信任计算方面,利用证据空间与观念空间概念模型[10]和直觉模糊集描述与量化信任[11]等通过数学模型直接对信任关系直接建模计算的方式可以较好地描述实体间信任,但是仅局限于逻辑计算与或简单信任合成;也有利用社交网络社会关系对网络信任的建模方式[12],其主要思路是将网络信任定义为社会行为在网络空间中的映射,而网络信任度则被定义为网络信任的量化值,与信任属性直接相关,是描述网络节点行为间交互程度的定量表示.

信任传递在网络安全系统中发挥着巨大的影响效应,许多研究是建立在对网络的拓扑结构、用户间的信任关系以及项目在社会网络中的流行度分析的基础上.信任传递关系中,二元模式信任关系[13]可以迅速地描述信任传递,但是在实际情况中,各个节点之间的信任是有差异性的,表现为权限的不同,而非"信与不信"的二元关系.在此基础之上,产生了利用社会网络自身信任特性,以无监督学习方式[14]构建定量信任强度的信任传递关系的方法;同时针对信任信息不加区分的问题,产生结合用户自身评分信息与社会信任关系两项要素,以构建信任关系传递的方法[15],不过该方法现用于社会网络的推荐.

综上可知,尽管国内外学者对信任传递体系问题进行了大量的研究,但应用信任传递体系解决实际问题仍存在许多局限性:(1)由于信任具有天生的不确定性和不可控性,现有信任计算模型过于简单,且不能有效地描述和度量实体信任的不确定性;(2)现有信任传递模型对信任的刻画相对简单,且多基于机器学习方法对社会网络或社交网络的信任进行逆向工程建模,与网络安全的实体信任差距较大.

本文对现有信任传递体系进行了扩展,提出信任邻域扩散传递体系与定量化信任度量与管理模式,并提出三种数学模型对网络实体间的信任进行刻画与建模,打破现有方法描述性差、适用性窄的局限.

2.3 分形网络的研究进展

Mandelbrot[16]给分形的定义为:在所有的尺度上都具有自相似的图案的数学集合或者自然形状,即图案的一部分放大之后,与整体具有相似性.现有研究表明,从网络演化的角度出发,网络的演化规则在整个演化过程中是不变的,且不变性与网络的节点数无关,预示着复杂网络中应该存在分形结构,且复杂网络的整体鲁棒性来自自身的分形结构[17].尤其体现为分形网络在对度数较大的节点进行选择性攻击下,具有比非分形网络更好的抗攻击性.这种现象解释了为什么现实中的许多生物网络都要演化为分形网络结构.更有研究表明网络的分形结构对于疾病的传播(类比于网络攻击的扩散)具有一定的抑

制作用[18]. 虽然分形网络的规律、特性及算法等还有待研究者进一步发掘，但在构建新的信任体系结构中，引入分形网络特性，可以从理论上增加该信任体系结构的整体鲁棒性.

2.4　现有信任体系结构的研究进展

现有信任体系的研究多关注于对传统 PKI 架构的扩展，随着区块链技术的发展，部分研究利用区块链去中心化管理机制的特性，使用区块链网络代替单独的 CA 存储，提出应用在物联网领域的基于区块链技术的去中心化 PKI 解决方案[4]、应用于泛在物联网的去中心化 PKI 方案 IoT-PKI[5] 和用于实现信任动态化自动认证的 PKI 区块链智能合约 Smart Contract-assisted PKI (SCP)[6]，完善单点 PKI 信任失衡的缺陷.

区块链作为当前十分热门的去中心化信任管理模型，虽然能够解决信任凭证的安全存储与认证问题，但是其仅能保证当前构建的信任体系的信任关系存储安全，并不能保证后续加入的节点的可信，也不能进行信任关系的管理. 系统地说，区块链技术的应用增强了现有体系的信任存储鲁棒性，但该类方法无法从根本上解决信任链 PKI-CA 的不安全性、人-物脱耦问题且难以支持大规模信任结构.

另一方面，传统信任链 PKI 体系模型在物联网、云环境等特殊网络环境下效果不佳，因此部分研究利用现有技术和方法探索了物联网环境下的新信任体系结构的建设. 移动物联网具有低功耗有损网络(RPL)特征，轻量级安全架构[19] 和边缘计算技术[20] 一定程度上解决了功耗与安全的平衡问题，但无法广泛解决各类异构网络信任问题，缺乏普适性；而云服务环境中，研究集中于利用云标准数据隐私模型与动态信任更新机制来实现信任评估[21]，缺乏完整体系结构；在信任变化上，基于时间衰减因子的动态信任关系模型[22] 探索了信任随时间逐渐淡化的过程，但模型相对简单且缺乏对用户之间信任空间流动关系的描述与建模.

本文提出了可同时适用于中心化存储或去中心化存储的新一代信任邻域网络体系结构，突破了传统信任链 PKI 体系的局限，从根本上创新性地改进了现有的信任体系结构，理论上保证了万物互联网络环境的整体鲁棒性与安全性.

3　信任邻域网络体系结构

在万物互联环境下，具有大量的、种类繁多的节点，每个节点与其他节点之间具有物理连接，构成了实际的网络拓扑. 而信任网络则是以物理上的网络拓扑为基础，经过一定的定义与重构，以信任行为为交互元素的逻辑网络. 因而，在考虑信任网络的描述时(而非实际建模与应用)，可以将不同的节点抽象为性质相同而参数不同的信任实体，体现为信任网络中的点.

现有的信任体系结构以信任链为主，其仅着眼于少量信任节点之间的链式关联，而实际上的信任空间关系是复杂的网状结构. 因此需要一个以网状拓扑为基础的万物互联信任网络空间架构来描述万物互联环境下的信任空间关联关系.

3.1　信任分形网络拓扑结构

从图论的角度说，在节点数相同的情况下，网状结构拓扑中边的数量一定会大于链式结构拓扑中边的数量(网状结构拓扑中边数 E 一定会大于等于节点数 V，而链式结构拓扑中边数 E 一定会等于 $V-1$). 因此，将拓扑模型应用于实际网络中时，在节点数量相同的情况下，网状拓扑相较于链式拓扑具有更多的节点与节点间的连接(不考虑两个节点间出现超过一条边的情况)，在出现部分连接失效的情况下，可以维持网络整体的连通性.

信任网络作为实际网络的重定义与重构，那么在信任网络中，网状拓扑则代表更多的节点间的信任直接交互连接. 更多的信任直接交互连接的选择，将在某些信任交互连接失效情况下，继续维持部分节点连接于当前信任网络中，以保证信任网络的整体鲁棒性. 简而言之，网状拓扑结构相较于链式拓扑结构具有路径上的鲁棒性特征.

不过，网状拓扑是一种复杂的、具有多种分布特性的拓扑模型，一般的网状拓扑并未遵循特定的节点-路径统计分布规律，统一称作随机网状拓扑. 不同的节点-边连接统计分布情况将导致整个网络在节点上的鲁棒性差异.

分形网络拓扑结构是一种特殊的网状拓扑结构，其拓扑的一部分与整体拓扑具有相似性特征，因而分形网络更倾向于在两个直接相邻节点间只有一条路径的情况下，形成节点间具有多条可达路径的拓扑结构，在部分节点失效的情况下，不会影响整体网络的路径可达性. 从而分形网络拓扑相较于普通的随机网状拓扑而言，具有节点上的鲁棒性特征.

如图 1 所示，直观地说，在节点数相同时，分形网络拓扑相较于网状拓扑与链式拓扑而言，数学期望上具有更少的脆弱节点. 其中，脆弱节点指的是失

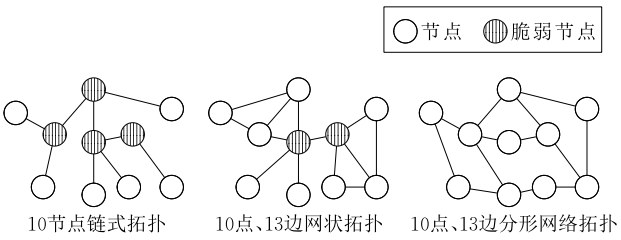


图 1 链式拓扑、网络拓扑与分形网络拓扑模型示意图

效后将导致整个网络不能够完全连通(即任意两节点间可达)的节点.

以 10 个节点为例,随机生成链式拓扑;并以 10 个节点 13 条边为例随机生成网状拓扑和分形网络拓扑.分形网络由于部分与整体的自相似性,保证了更多环路的出现,使拓扑中出现脆弱节点的概率大幅度下降.

因此,分形网络拓扑相较于链式拓扑具有节点与路径的整体鲁棒性特征,可以从根本上提高空间架构的鲁棒性.本文提出的信任体系结构将以分形网络拓扑为基础,构建空间架构,并在此空间架构上实现信任传递关系与信任管理模型.

3.2 信任邻域扩散传递体系

信任传递体系是从宏观角度对信任实体间信任描述与刻画的动力学体系,是信任交互的基础.

在信任分形网络空间架构中,信任并非一成不变,而是随着每个信任实体的行为而变化.在信任分形网络内,信任实体与其相关的其他信任实体发生交互,从而产生行为,进一步导致信任关系的变化.以网络设备为例,当前设备只能和与之物理相连的设备发生直接交互,而如果需要和其他设备发生交互,则需要通过路由、交换等手段借助与之物理相连的设备发生间接交互.因此,本文从拓扑学引入邻域的概念,利用邻域来刻画与某一信任实体直接相连的同类信任实体所构成的集合.

定义 1. 信任邻域(Trust Neighborhood).给定一个信任实体 x,称离散集合 $U(x)$ 为 x 的信任邻域,当且仅当 $U(x)$ 满足:(1)对于任意信任实体 $y\in U(x)-\{x\}$,$Connect(x,y)=1$,其中 $Connect(x,y)=\begin{cases}1, & x\text{ 与 }y\text{ 直接相连}\\0, & x\text{ 与 }y\text{ 非直接相连}\end{cases}$;(2)$x\in U(x)$;(3)$U(x)-\{x\}\neq\phi$.同时定义邻域集合 $TN(x)$ 为所有符合信任邻域定义的离散集合 $U(x)$ 的集合.

在实际网络环境中对一个实体 x 计算其信任邻域时,只需要对其相连可达的 1 跳实体进行统计即可,该类实体中的若干个实体与被统计的实体本身则构成一个邻域 $U(x)$.在信任邻域定义的基础之上,信任的动力学直接作用域则是邻域集合 $TN(x)$ 中的 x 的最大邻域 $U_{max}(x)$,也就是实际网络中当前实体 x 的所有 1 跳相连可达节点及其自身所构成的集合.在信任邻域的基础之上,本文提出信任邻域扩散的概念,描述复杂信任网络中的信任空间动力学传播方式.

定义 2. 信任邻域扩散(Trust Neighborhood Spread).信任在信任分形网络中的空间动力学传播方式.一个信任实体产生信任行为后,信任的变化仅在当前信任实体的最大邻域集合 $U_{max}(x)$ 内直接产生传播,后续的信任空间动力学传播则与当前行为非直接相关.信任沿着当前信任实体与后续邻域内信任实体方向进行扩散.

那么信任邻域网络(Trust Neighborhood Network)则是由信任实体节点组成的,符合信任邻域扩散性质的网络.

定义 3. 信任交互行为(Trust Interactive Behavior).由信任实体与其信任邻域内其他实体交互产生的,具有一定目的性的行为,具有指向性行为与非指向性行为两种.指向性行为指的是具有明确目标的信任行为;非指向性行为则是由信任实体自发产生,没有明确目标但是会对部分或所有直接相连信任实体产生影响的行为.

如图 2 所示,当前节点向自己邻域中的一个或若干个不包含自身的节点发起信任行为,这种行为只与发起节点自身和行为目标节点(或节点集)相关,与其他节点不直接相关,那么这种行为称作指向性信任交互行为.现有互联网中的直接访问、登录、指令下达、P2P 文件传输以及组播等都属于指向性信任交互行为.而与此相对的是,以自身邻域中所有节点为目标的信任行为则是非指向性信任交互行为,最典型的就是网络传输中的广播.

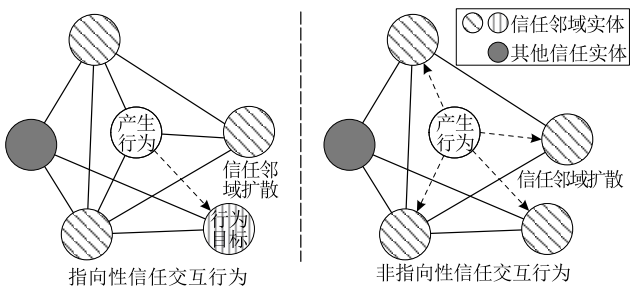


图 2 信任邻域网络中信任邻域扩散动力学模式示意图

对信任交互行为的定义完善了信任行为与信任邻域扩散之间的关系,为定量化信任度量打下基础.

信任邻域扩散传递动力学模式结合分形网络拓扑模型，形成了信任邻域网络空间架构，实现了宏观上的信任关系及信任关系变化的描述.

3.3　定量化信任度量与管理模式

信任管理模型实现的是对信任体系结构中信任实体与信任关系的微观度量与管理. 在信任邻域网络空间架构的基础之上，如果需要对信任传递关系进行管理，即在微观层面上对每个信任实体与其他信任实体间的信任关系进行度量与管理，则需要对信任实体与信任关系本身进行描述. 而定量的信任管理模型才能实现信任实体与信任关系管理的计算. 因此，本研究对信任管理中涉及到的参数进行了如下的形式化定义.

定义 4.　信任度(Credibility). 指一个信任实体在信任邻域网络中的潜在定量信任程度描述，用符号 Cfd 表示，用数值表示信任度. 以取值范围为 0～100 为例，如果信任度取值为 0，表示完全不被整个网络信任，如果取值为 100，表示完全被整个网络信任，信任度的值越大，则量化可信任的程度越高. 值得注意的是，信任度值的范围和表现形式(整数、小数或离散值区间)与实际应用场景相关，各个门限值的取值也需要通过历史数据进行标定或在模型应用过程中逐步优化，并不存在统一的计算方式(视实际应用场景而定).

但信任度并不决定其他信任实体对当前信任实体的权限，仅仅表明该信任实体在当前信任邻域网络中的被信任的程度，在信任度的基础之上，还需要结合信任评估与信任门限阈值才能形成信任实体之间的信任级别(Trust Level). 信任级别是一个实体可观察到的另一个信任实体对自身的信任反馈情况，一般为离散定性元素，与信任度和信任级别的阈值直接相关.

如图 3 所示，在一个两两节点相互连接的三节点实例网络(忽略连接网络的交换设备)中，节点 A 为文件存储服务器、节点 B 为普通服务器、节点 C 为监控服务器，每个服务器可提供给其他服务器的行为如图中矩形梯所示. 该网络中每个节点具有各自的信任度值，且每个行为执行所需要的信任度门限值也已经确定. 那么，在该网络中，各节点之间都可以进行相互访问，但节点 B 则无法向节点 C 下达指令、节点 C 也无法修改节点 A 上的文件等.

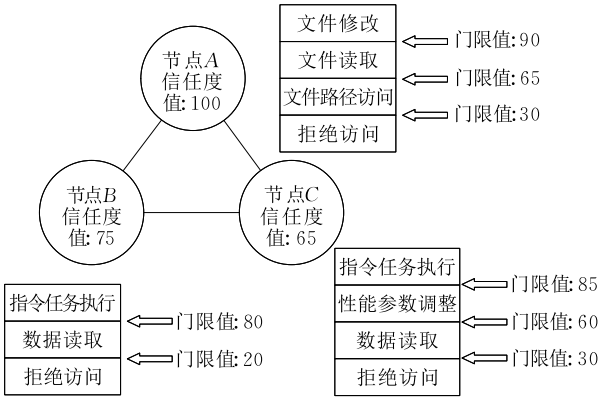


图 3　信任度与信任级别关系示意图

因此，定量的信任度结合以信任度值为区间划分的信任级别，可以实现多级信任管理，突破二元化信任管理的局限，表现为实际网络环境中的权限控制. 当一个信任实体需要某种服务时，能够提供此种服务的实体可能有多个，在信任度与信任级别的支撑下，就可以对主观的信任关系进行量化评估，从而选择一个合适的服务提供者；反之，当一个信任实体需要向其他实体提供服务时，则可以根据信任度与信任级别选择可提供的服务. 最终实现定量化的信任度量与管理，整体构成信任邻域网络体系结构.

4　基于隐马尔科夫随机场-置信能量场的信任体系结构建模

第 3 节中完成了对信任邻域网络体系结构的定义与描述，但是如果一个信任网络体系结构想要在实际中能够应用，并且证明其相较于传统信任体系结构的优越性，必须通过数学模型对其建模.

4.1　隐马尔科夫随机场

在信任邻域网络体系结构中，首先需要对信任邻域扩散传递关系进行建模.

信任作为一种可传递因子，其本身随着时间的推进与行为的产生而进行流动. 对于每一个信任实体而言，其自身的信任状态则会随着时间的推进而产生变化，且后续的信任状态与当前的信任状态有关. 因此，信任邻域网络中的信任状态关系本身具有马尔科夫性.

与此同时，根据第 3 节中信任邻域网络的描述，信任邻域网络中信任实体的信任状态仅与其邻域实体相关，因而信任邻域网络自身具有马尔科夫随机场特征. 信任状态自身虽然具有马尔科夫性，但是对于观测者而言无法直接获取当前信任节点在当前信任邻域网络中的信任状态，只能观测到当前信任状态所体现出的信任行为证据，也就是说信任邻域网络中的信任状态具有隐马尔科夫性质.

因此，本文结合马尔科夫随机场模型与隐马

尔科夫模型，提出隐马尔科夫随机场模型（Hidden Markov Random Field Model，HMRFM），从数学角度对信任传递关系进行建模.

在 HMRFM 模型中，每一个信任实体与邻域信任实体之间的信任变化相关关系通过势函数

$$X(a,b)=f(Para_{Beh},Para_{Env},X_a,X_b,Type_a,Type_b) \tag{1}$$

来表示，其中 $Para_{Beh}$ 为行为参量组，不同的信任实体行为会产生不同的行为参数，导致不同的势能变化结果，而其中行为参量组由信任实体自身性质和当前信任需求所决定；$Para_{Env}$ 为环境参量组，同样的信任实体与同样的行为在不同的环境下也会产生不同的势能变化结果，环境参量组为一系列可以描述当前物理网络环境与网络空间状态的参量；X_a 为节点 a 的信任自参量，是与节点 a 自身信任相关的参量，如信任度、其他信任影响等；X_b 为节点 b 的信任自参量；$Type_a$ 为节点 a 的类型；$Type_b$ 为节点 b 的类型.

而 HMRFM 中信任节点的自身状态的隐马尔科夫性质 $HMM(a)$ 则可以用五个元素来描述，即

$$HMM(a)=(S,O,\boldsymbol{\pi},\boldsymbol{PM}_S,\boldsymbol{PM}_O) \tag{2}$$

其中，S 为隐含状态，是满足马尔科夫性质的、模型中实际所隐含、无法通过直接观测而得到的状态，在本模型中指的是实际的信任度；O 为可观测状态，是与隐含状态 S 所关联的、可以直接观测得到的状态，在本模型中指的是信任级别；$\boldsymbol{\pi}$ 为初始状态概率矩阵，表示 S 在初始时刻 $t=1$ 的概率分布矩阵，在本模型中指的是信任度初始化的概率分布；$\boldsymbol{PM}_S$ 为 S 的转移概率矩阵，在本模型中是由环境与行为所制约的、相对稳定的转移概率稀疏矩阵，在特定情况下可由另一信任度转化函数集进行拟合；$\boldsymbol{PM}_O$ 为观测状态转移概率矩阵，在本模型中是由环境、行为、当前信任度、信任级别阈值所制约的、相对稳定的转移概率稀疏矩阵.

4.2 置信能量场

HMRFM 模型为复杂信任分形网络空间架构的信任关系转化与信任邻域扩散动力学提供了数学模型的支撑，但是并未实际解决信任网络中信任度的实际计算与信任关系转化的问题.

在对定量信任管理进行建模的时候，首先需要考虑到信任度的建模与信任度流动的建模. HMRFM 模型建模了信任流动，但无法进行信任度流动的定量计算，因此需要一个数学模型对信任度及其流动进行建模.

信任度并非无限的，信任度应该在信任实体间产生信任交互行为时有所消耗，而在一个完整的、闭环的信任体系内部，在信任体系初始化之后，信任度不会凭空产生、也不会凭空消失，因此，整个信任体系的信任度总量应该守恒，即信任度满足“信任守恒”.

HMRFM 模型中存在势能的概念，势函数产生的信任变化则是信任度的变化. 因此，基于 HMRFM 模型的势能模型性质与信任度特性，本文提出基于隐马尔科夫随机场模型的置信能量场（Confidence Energy Field based on HMRFM，HMRFM-CEF）.

HMRFM-CEF 可以用于初始化和计算信任分形网络空间架构中信任度在空间维度上的变化关系. 首先信任邻域网络中的每一个信任实体都具有自己的信任度值 Cfd，整个网络中所有信任实体在信任邻域网络构建时都具有自己的初始信任度值，整体以向量 $\boldsymbol{Vec}_{Cfd}$ 表示. 在初始信任度值向量 $\boldsymbol{Vec}_{Cfd}$、信任实体之间的网络拓扑 $\boldsymbol{Conn}_M$ 和各个信任实体自身信息 $\boldsymbol{Node}$ 的基础之上，HMRFM-CEF 通过判断各个信任实体可提供/需求服务的差异和两个物理上直接相连的信任实体的初始信任度值，判断两个物理相连的节点是否需要构建信任交互，从而初始化信任邻域网络.

如图 4 所示，在一个具有 11 个节点的网络中，节点之间的物理拓扑关系如左半图，且每个节点具有初始信任度值. 在进行初始化的过程中并没有固定的方法，图中初始化遵循的是信任度值梯度相邻则连接和物理近邻则连接的规则，保证初始化后的信任邻域网络具有分形特性即可.

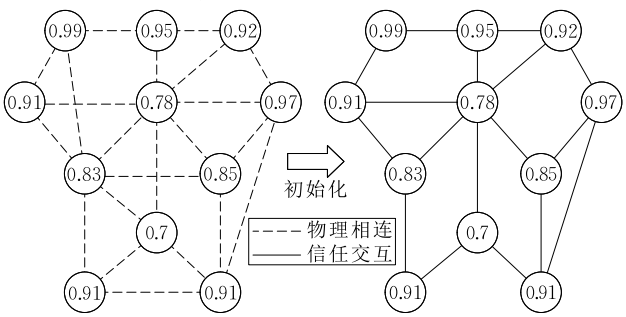


图 4 HMRFM-CEF 初始化信任邻域网络示意图

在完成信任邻域网络的初始化之后，该信任体系就可以开始运转，进行后续的定量信任管理.

4.3 信任门限控制模型

HMRFM-CEF 解决了信任邻域网络体系结构的信任度与信任关系的初始化问题，但是如果想要实现在信任体系全生命周期内的信任管理，需要实现信任度动态变化情况下的信任度与信任关系计

算. 3.3 节描述了信任度和信任级别之间的关系，信任度值结合信任级别可以实现多级信任管理. 因此，基于 HFRFM-CEF 模型，我们提出信任门限控制模型(Trust Threshold Control，TTC)，通过为各个信任实体设置多个级别的不同的阈值作为信任级别的门限进行多级信任管理，并且设置全局认证阈值 $Thres_T$.

在置信能量场中，每个节点的信任度均表现为门限控制下的可变势能；信任度值低于 $Thres_T$ 将唤醒交叉认证请求，该请求将导致信任势能在请求节点和关联节点之间的流动(在双向完成认证之前，信任度将暂存于被交互节点，但不能为被交互节点所用). 节点的势能变化将在交叉认证环节导致相关开放关联节点的置信势能以相同的趋势变化. 势能的流动趋势是整体趋于平稳，但门限的控制对势能的变化起阻挡作用. 当势能过低导致节点不可信，门限控制将彻底阻断节点能量场的交互.

图 5 中的信任邻域网络拓扑是图 4 中初始化之后的网络拓扑，假设信任度为[0,1]的取值范围的小数. 为更加清晰的显示信任度，将图中每个节点的信任度值形象化为每个节点容器中信任的颜色灰度(越浅信任度越高，越深信任度越低). 假设当前图中中部下方的节点被攻击者控制，其信任度已经降为了 0.3，继续执行信任行为则需要向周围节点发起提权认证；同时中部上方信任度为 0.78 的节点向图中其左侧和上方的节点发起了提权认证. 可以看到，在下一个时间点，0.3 信任度的节点由于无法通过其他三个节点对其的交叉认证而被阻断(移出当前网络)；0.79 信任度的节点则通过交叉认证获取了三个节点给予其的信任度值. 而且由于 0.3 信任度节点被阻断造成信任邻域网络的分形性受到影响，则自动在图 4 所示的物理拓扑中重新选择一条备选信任交互路径.

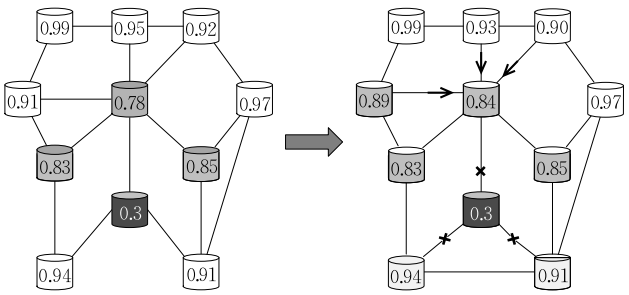


图 5　基于门限控制模型的置信能量场门限控制阻断示意图

TTC 模型保证了节点在做出一定数量的信任行为之后，逐渐丧失部分行为的权限，需要通过提权认证重新获取相应权限；在持续做出信任行为的情况下，会导致当前节点的信任度值低于 $Thres_T$，在节点遭受攻击的情况下，由于攻击者难以通过后续的交叉认证，将导致该节点被阻断而脱离当前信任网络，即该节点被逻辑隔离出当前实际网络中，保障了网络的整体安全性.

5　实验与分析

5.1　数学定量分析

假设在同样的节点自身环境与网络环境下，分别应用信任链体系结构与信任邻域网络体系结构，构建网络内节点的信任关系，并通过数学模型进行定量分析.

在进行模型的定量分析对比之前，需要对当前网络环境进行建模. 假设一共有 V 个节点，这些节点构成连接数为 E 的拓扑结构，该拓扑结构中包含且仅包含一个连通分量，每个节点具有同等的被成功攻击的概率 $P(Atk)$，每个被攻击的节点在同一个时间步内具有向任意直接相连的未被攻击节点进行成功攻击转移的概率 $P(Trans)$. 假设一个时间步内，攻击者仅攻击一个未被攻击的节点或对已经被攻击节点直接相连的未被攻击节点进行攻击转移，两个事件相互独立，如果同时发生则选择更加符合实际攻击链模式的攻击转移；且攻击链仅考虑最简单的二状态马尔科夫链 AMC(未被攻击的初始状态与已被攻击的最终状态).

以上假设构成网络环境与网络攻击模型

$$NEAM=\{V,E,\boldsymbol{Node},\boldsymbol{Conn}_M,P(Atk),P(Trans),AMC\} \tag{3}$$

其中 $\boldsymbol{Node}$ 表示节点向量、$\boldsymbol{Conn}_M$ 表示节点连接关系的矩阵，以下定量分析均遵循该模型.

从攻击者角度出发，不考虑网络中节点自身交互行为的情况下，分别计算成功攻击该网络中所有节点所需要消耗的时间步的数学期望. 信任链被完全攻击的时间步数学期望

$$E(Timestep_{TC})=\frac{1}{P(Atk)}+\left(\alpha*\frac{1}{P(Trans)}+(1-\alpha)*\frac{1}{P(Atk)}\right)*(V-1) \tag{4}$$

其中 α 是攻击转移行为选择参数，代表攻击者从攻击转移和直接攻击新节点这两种行为中选择攻击转移的可能性.

而信任邻域网络架构的拓扑模型是网络，因此需要保证信任邻域网络中边的数量大于等于 V，小

于等于实际网络拓扑的连接数 E. 不妨假设信任邻域网络模型实例中的边数量为 K，拓扑使用稀疏矩阵 ***SMNN*** 表示. 信任邻域网络中信任节点之间的信任关系根据 HMRFM-CEF 模型表示，节点交互行为的势函数 $X(A,B)$ 产生节点信任度的改变，所有节点具有其初始信任度值向量 $\boldsymbol{Vec}_{Cfd}$，信任度门限阈值为 $Thres_T$. Q 为当前已经被攻击的节点的集合，$I(Q)$ 表示在 Q 情况下根据 HMRFM 门限控制计算得到的攻击成功系数，信任邻域网络体系结构被完全攻击的时间步数学期望

$$
\begin{aligned}
E(Timestep_{TNN}) &= \frac{1}{P(Atk)} + \sum_{i=0}^{V-1}\left[E(I(Q_i)) * \alpha * \frac{1}{P(Trans)} + (1-\alpha) * \frac{1}{P(Atk)}\right] \\
&= \frac{1}{P(Atk)} + \sum_{i=0}^{V-1}\left[\frac{E(X(Q_i, \arg b(SMNN(a,b)=1)))}{E(\boldsymbol{Vec}_{Cfd}(Q_i) - Thres_T) * P(Trans)} * \right. \\
&\quad \left. \alpha * \frac{1}{P(Trans)} + (1-\alpha) * \frac{1}{P(Atk)}\right],\ a \in Q_i \\
&= \frac{1}{P(Atk)} + \sum_{i=0}^{V-1}\left[\frac{\sum_q \sum_b X(q, argb(SMNN(q,b)=1))}{Num(Q_i) * Num(B) * \sum(\boldsymbol{Vec}_{Cfd}(q) - Thres_T) * P(Trans)} * \right. \\
&\quad \left. \alpha * \frac{1}{P(Trans)} + (1-\alpha) * \frac{1}{P(Atk)}\right],\ q \in Q_i \\
&= \frac{1}{P(Atk)} + (1-\alpha) * \frac{1}{P(Atk)} * (V-1) + \alpha * \frac{1}{P(Trans)} * \\
&\quad \sum_{i=0}^{V-1}\left[\frac{\sum_q \sum_b X(q, argb(SMNN(q,b)=1))}{(i+1) * Num(B) * \sum(\boldsymbol{Vec}_{Cfd}(q) - Thres_T) * P(Trans)}\right],\ q \in Q_i
\end{aligned} \tag{5}
$$

其中，B 为 $argb(SMNN(x,b)=1)$，指的是 ***SMNN*** 中与节点 x 相连的未被攻击的节点 b 的集合.

对两种信任体系结构的被完全攻击时间步数学期望进行差运算可以发现，在信任邻域网络体系结构中，由于 HMRFM-CEF 门限控制的存在，只需要通过合理的参数设置，即保证

$$
\sum_{i=0}^{V-1}\left[\frac{\sum_q \sum_b X(q, argb(SMNN(q,b)=1))}{(i+1) * Num(B) * \sum(\boldsymbol{Vec}_{Cfd}(q) - Thres_T) * P(Trans)}\right] > V-1 \tag{6}
$$

就可以保证系统在一定时间内理论上被攻击的可能性降低，从而确保系统的安全.

5.2 仿真实验对比分析

在数学定量分析的基础之上，为了验证信任邻域网络在实际网络模型下相较于信任链的优势，本文通过 Matlab 仿真实验对两种模型进行了对比分析.

万物互联是传统互联网、云计算网络、移动互联网、物联网等网络形式的有机融合，因此万物互联网络中并没有固定的网络拓扑模型，其总体结构类似于无标度网络特征. 如果考虑一个实际的万物互联网络中的拓扑模型，则需要同时考虑到现有常用的各类网络拓扑模型. 现今常用网络拓扑模型大多具有以下常见三类环境特征：骨干网三层类树状拓扑（传统互联网）、数据中心 Fat-tree 拓扑（云计算网络）、Ad-hoc 自组织星型层级拓扑（移动互联网与物联网），因此，仿真实验中的节点数量和连接数量需要均衡三类拓扑以符合实际节点与连接分布情况. 根据 ChinaNet 骨干网 2019 年初和 CERNET 教育网 2019 年上半年的公开报告可以发现，大规模骨干网拓扑中连接数 E 约为节点数 V 的 1.3～1.7 倍；根据各大厂数据中心产品设计报告可以发现，Fat-tree 拓扑中连接数 E 为节点数 V 的 1.5～3 倍；而根据各移动网络运营商 2018 至 2019 年度报告及智能物联网厂商报告，节点数众多的 Ad-hoc 网络中，连接数 E 一般为节点数 V 的 1.1～1.5 倍. 因此，为了同时满足三类网络拓扑的节点数与连接数关系，在仿真环境中连接数 E 应选取为节点数 V 的 1.5 倍.

在 5.2 节数学定量分析中网络环境与网络攻击模型 $NEAM$ 的基础上，由于 $NEAM=\{V,E,\boldsymbol{Node},\boldsymbol{Conn}_M,P(Atk),P(Trans),AMC\}$，因此仿真实验中还需要确认节点数量 V、节点拓扑关系 $\boldsymbol{Conn}_M$、节点自身信息 ***Node***、被成功攻击的概率 $P(Atk)$ 与成功攻击转移的概率 $P(Trans)$.

为了简化仿真实验，不考虑各个节点之间的差异性，因此，***Node*** 中每个节点的信息是相同的，即将每个节点视为除命名外其他属性均相同的节点；基

于已经确定的节点数 V 和连接数 E 通过随机算法构建具有包含且仅包含一个连通分量的图拓扑结构 T，$\boldsymbol{Conn}_M$保存 T 的拓扑信息，因为每个节点属性都是相同的，所以不考虑节点之间连接的权重差距，所有节点间仅考虑是否相连. 根据实验室前期研究结果，设有不同防御手段的设备被成功攻击的概率具有较大差异，而由于设备之间的信任关系与配置的相似性，进行攻击转移的概率将达到直接攻击成功概率的 3 倍以上.

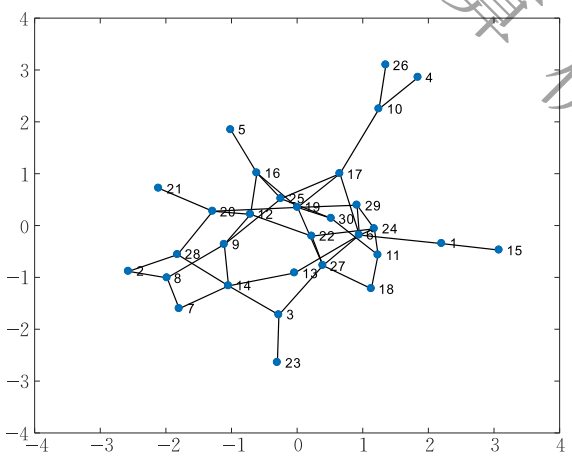
因此，仿真实验将分别设置一下三类不同防御级别设备的 $P(Atk)$和 $P(Trans)$进行对照实验，攻击概率参数配置情况如表 1 所示.

表 1　三类不同防御级别设备的攻击概率参数表

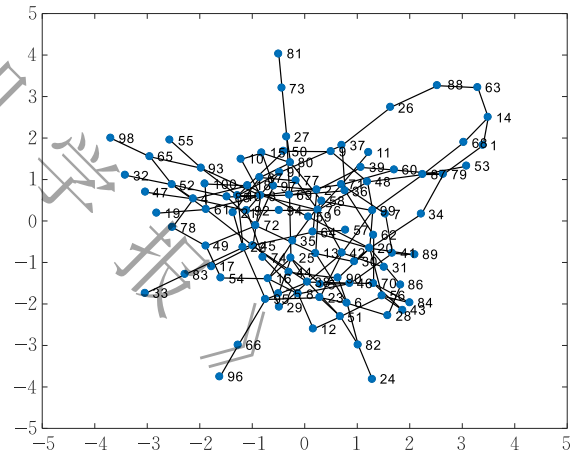
防御级别	$P(Atk)$	$P(Trans)$
无防御设备	0.20	0.50
低防御强度	0.10	0.30
高防御强度	0.02	0.07

节点数量 V 将直接影响网络的规模：前文已经提到，万物互联网络是由各类网络形态有机组合而成的. 互联网是具有分形特征的无标度网络，物联网则是由大量的、节点数量与地理范围有限的节点簇组成的网络. 因此，万物互联网络仍具有分形性特征. 且由于网络自治域的存在，对万物互联网络中信任邻域网络体系结构与信任链体系结构的对比仿真实验无需考虑互联网整体节点规模数量巨大的问题，只需要考虑某一个具有自我管理能力的节点集群，这也是符合目前互联网管理模式的.

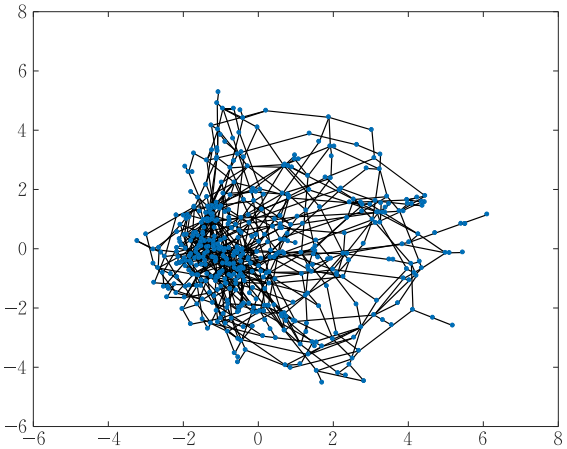
与日常网络行为与管理最直接相关的三种网络节点规模分别是：小型办公场所、服务器集群或网络机房、区域性网络交换集群. 以高校为蓝本，统计各实验室和办公室得出平均联网设备规模为 30；对与网络研究相关的实验机房进行统计得出一个实验机房的设备总体规模为 100 左右；而校园网骨干网络节点的数量约为 500. 为增加实验节点规模的适用性，本文选择 10、20、30、50、100、200、300、400、500、600、700、800、900、1000 十四种不同的节点规模进行仿真，其中 30、100 与 500 节点规模的拓扑如图 6 所示.



(a) 节点数为30



(b) 节点数为100



(c) 节点数为500

图 6　仿真网络环境部分拓扑图

攻击转移行为选择参数 α 代表攻击者攻击喜好，并不影响两种信任体系结构对比仿真实验的结果，不妨令 $\alpha=0.9$.

对于信任邻域网路体系结构而言，还需要确定初始信任度值向量 $\boldsymbol{Vec}_{Cfd}$、势函数 $X(A,B)$ 和信任度门限阈值 $Thres_T$. 为了简化仿真实验计算，首先将信任度计算限制为正整数运算，且为每个信任节点设置相同的初始信任度值，初始值为 9，不同的信任度初始值只决定当前节点的初始可信任程度. 在一个信任邻域网络第一次构建的时候，需要根据节点自身的特性去初始化，但仿真实验中所有节点视为同类型节点，因此设置相同初始信任度值是可行的. 然后，势函数 $X(A,B)$ 中不考虑各种信任行为的差异性，因为对不同类型信任行为进行差异性信任度消耗建模需要其他模型的支持，该内容并不在本文的研究范围之内，故将每次行为消耗的信任度值设为 1. 最后，由于未考虑节点差异性与不同类型信任行为之间的差异性信任度消耗，因此信任度门限阈值的数量(权限级别的层数)并不会对实验结果产生影响，因此不考虑多信任度门限阈值的层级化信任行为管理(即 HMRFM 中可观测状态 O 仅包括可访问与拒绝访问两个状态)，也不考虑信任度门限阈值随网络环境的变化，将 $Thres_T$ 设为 3. 所有实验场景的设置参数如表 2 所示.

表 2 实验场景各项参数表

参数项	初始值
$\boldsymbol{Vec}_{Cfd}$	9
$X(A,B)$	1
$Thres_T$	3
α	0.9

根据以上参数设计的模拟攻击算法(具体攻击算法内容请参阅附录)，我们分别进行了 42 类(14 种不同节点规模与 3 种不同的防御级别设备的组合)仿真实验，每类随机 5 个拓扑，每个拓扑进行 500 次仿真实验，共计 105 000 次. 统计应用两种不同信任体系结构的相同网络被完全攻击所需要的次数及攻击成功率，以校园教育网的三种子网规模(30、100、500)和超大规模子网(1000)为例，结果如表 3～表 6 所示.

表 3～表 6 为相同节点规模下仿真攻击实验整体网络攻击成功率与成功攻击时的平均攻击次数的对比，而在不同节点规模下的整体网络攻击成功率如图 7、图 8、图 9 所示.

表 3 30 个节点两种体系结构的仿真攻击实验对比结果表

攻击结果		信任体系结构			
		信任链		信任邻域网络	
		成功攻击平均攻击次数	成功率/%	成功攻击平均攻击次数	成功率/%
节点类型	无防御设备	81.676	100	145.837	99.4
	低防御强度	143.216	100	293.574	93.0
	高防御强度	630.558	100	1466.186	45.2

表 4 100 个节点两种体系结构的仿真攻击实验对比结果表

攻击结果		信任体系结构			
		信任链		信任邻域网络	
		成功攻击平均攻击次数	成功率/%	成功攻击平均攻击次数	成功率/%
节点类型	无防御设备	266.720	100	496.167	99.4
	低防御强度	457.962	100	993.000	92.4
	高防御强度	2031.520	100	4993.620	41.0

表 5 500 个节点两种体系结构的仿真攻击实验对比结果表

攻击结果		信任体系结构			
		信任链		信任邻域网络	
		成功攻击平均攻击次数	成功率/%	成功攻击平均攻击次数	成功率/%
节点类型	无防御设备	1319.724	100	2499.111	99.0
	低防御强度	2281.152	100	4971.347	91.0
	高防御强度	10044.064	100	24985.792	41.4

表 6 1000 个节点两种体系结构的仿真攻击实验对比结果表

攻击结果		信任体系结构			
		信任链		信任邻域网络	
		成功攻击平均攻击次数	成功率/%	成功攻击平均攻击次数	成功率/%
节点类型	无防御设备	2632.456	100	4992.940	99.2
	低防御强度	4554.232	100	9978.989	91.4
	高防御强度	20026.594	100	50224.419	40.6

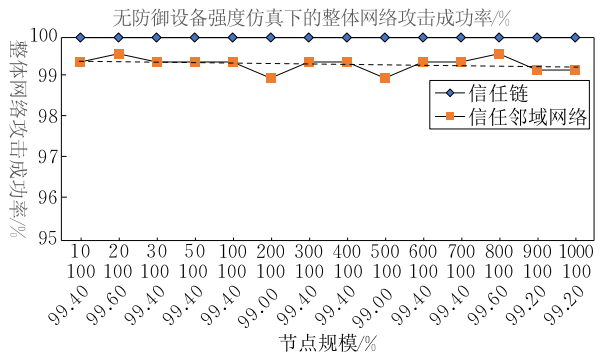


图 7 无防御设备强度攻击仿真成功率趋势折线图

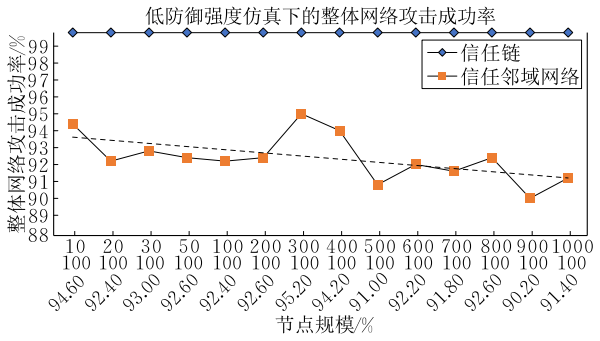


图 8　低防御强度攻击仿真成功率趋势折线图

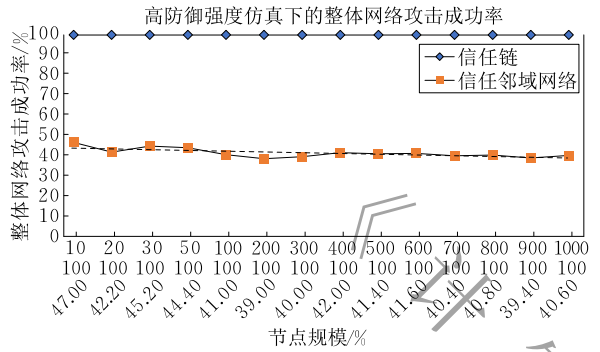


图 9　高防御强度攻击仿真成功率趋势折线图

从以上实验结果中可以发现，无论信任链的规模多大，无论何种防御强度，只要没有其他的交叉验证存在，攻击沿着信任链进行蔓延直至将整个网络攻陷，只是一个时间问题. 而在信任邻域网络中，不同规模的节点数量下，信任邻域网络的整体防御效能在相同类型防御强度下的表现结果相近，且随着节点规模的增大，整体防御效果也逐渐提高，主要原因在于 HMRFM-CEF 对信任度进行了计算从而在信任度较低时产生交叉认证，如果某一被攻击节点无法通过交叉认证，那么该节点将会被阻断从而隔离，更大的节点规模由于网络拓扑矩阵的秩更高，在被完全攻击之前的阻断可能性也更大；纵向对比可以发现，在节点数相同时，更好的防御强度将带来更好的整体安全性，因为更好的防御强度将使攻击者的单次攻击更加困难，使攻击者在攻破下一节点之前有更大的概率触发交叉认证，从而被阻断；最后，仿真结果表明，即便是在没有防御设备的情况下，信任邻域网络体系结构仍然有较小的概率可以使整个网络系统不被完全攻破，且攻击者成功攻击所消耗的成本倍于相同防御强度下的信任链体系结构，这是因为即使没有防御设备，攻击者在尝试中仍然有可能触发交叉认证被阻断.

信任体系结构最终将应用于实际网络环境中，因此本文在整体网络安全性攻击仿真实验的基础之上，对两种信任体系结构在实际网络环境中的系统资源开销、网络性能开销和存储开销进行了分析与对比.

对于系统资源开销，本文在同一台设备下分别进行了 2 kb 文件的 1024 位密钥（现有证书密钥长度）、1536 位密钥（未来可能的密钥长度）RSA 直接解密（代表信任链中证书的解密过程）和五元二阶拟合运算（五个元分别代表势函数 $X(A,B)$ 中除 $Type_A$ 自身节点类型外的其他参量）、四阶张量查询（四个维度分别代表势函数 $X(A,B)$ 中除 $Type_A$、$Type_B$ 外的其他参量，代表信任邻域体系结构计算中最消耗资源的势函数结果的运算）各一千次，运算消耗时间如表 7 所示.

表 7　性能实验对比结果表

仿真类型	时间/s
RSA 1024	338.9
RSA 1536	867.4
拟合运算	989.4
张量查询	351.3

系统资源开销仿真结果表明，信任邻域体系结构单节点计算所消耗的系统资源虽然比解密证书要多一些，但是在可接受的范围以内，如果使用高阶张量对势函数结果进行预存储，则可以大幅度降低系统计算资源.

对于网络性能开销，考虑相邻两个节点进行信任交互行为，在传统信任链 PKI-CA 体系结构中，只有在证书生命周期结束之后才需要重新传输证书进行验证，而信任邻域网络中每个节点的信任度值在更新以后（每次信任交互行为产生之后）需要向其他节点更新该值. 如果在实际网络环境应用中，采用中心化信任度值的分发与更新，则不会对节点自身网络性能造成影响；如果使用去中心化的区块链进行信任度值的存储与更新，则仅会对网络性能造成少量的影响（更新只在交互双方的邻域内传播）.

对于存储开销，由于在实际网络环境中，随着节点类型的改变、相邻节点数量的变化（拓扑的改变）和认证数据的变化，都会导致存储开销的变化. 但是，从算法存储复杂度理论上分析，假设总结点数相同为 N_{node}，信任链体系结构的每一个节点的存储开销主要在于信任证书的缓存，那么 $S(n)_{SingleNode}=N_{node}*O(L_{Cert})=O(n)$；整个信任链的存储开销在于公钥基础设施 PKI 的存储，那么 $S(n)_{Entire}=N_{node}*O(L_{PubKey})=O(n)$. 对于信任邻域网络而言，由于每个节点需要存储邻域节点的信任度值、势函数、门限

阈值,因此

$$S(n)_{SingleNode}=\frac{\sum_{i}^{N_{node}}(N_{nbh}^{i}*O(L_{VecCfd}))}{N_{node}}+S(L_X)+O(L_{ThresT})=S(L_X)+O(n) \tag{7}$$

其中如果势函数采用拟合函数可以视为 $S(L_X)=O(n)$,如果势函数采用高阶张量进行离散存储则 $S(L_X)=O(n^4)$,但是受限于实际网络中的行为种类数量且被存储单元为势函数运算值,实际存储消耗在可接受范围内;而整个信任邻域网络则不存在整体性存储开销.

因此,总体而言,信任邻域网络体系结构虽然从整体系统、网络性能与存储开销上高于信任链体系结构,但是处于可接受范围内.

以上两个仿真结果表明,虽然信任邻域网络的成本开销更高,但相较于传统信任链体系结构,信任邻域网络体系结构在不同规模节点数量、不同节点类型的情况下,均可以成倍提高攻击者的攻击成本,打破攻击者无限攻击期限的 100%整体网络攻击成功率并在特定情况下降低其至一个较低的成功率(尤其是在节点规模庞大并且整体网络系统具有高防御强度设备的情况下),有效提高了整体网络系统的防护能力,提高网络整体安全性.

6 总结与展望

本文在传统信任链体系结构的方案上进行了突破,提出了新一代信任邻域网络体系结构.我们首先为新一代信任体系结构引入分形网络空间拓扑模型,保障其空间架构上的鲁棒性;接着提出信任邻域扩散传递关系模式构建信任邻域网络,并提出 HMRFM 模型对信任邻域网络进行数学建模;然后提出基于 HMRFM-CEF 的信任定量管理模式与初始化方法,实现信任的量化管理;最后提出 TTC 模型,实现信任关系动态变化情况下的信任度与信任关系计算,构建完整的信任邻域网络体系结构.数学分析与仿真实验表明,相比于信任链体系结构,信任邻域网络体系结构能够在不同节点规模、节点类型等异构网络环境下,有效地提高攻击者的攻击成本至 2 倍以上,降低攻击者在无限攻击限期情况下的攻击成功率,实现整体网络防护能力的根本性提高.解决了传统信任体系结构管理模型鲁棒性不足、传递体系简单且适用性差、体系结构本身未考虑整体鲁棒性与安全性而无法应用于万物互联网络环境的问题.

信任邻域网络是一个效果优秀的理论模型,但是在实际网络环境中,由于节点信任度和行为势函数的存在,信任邻域网络的信任管理需要进行更多的计算,相较于传统信任链体系结构的证书验证需要消耗更多的系统资源,因而在资源有限的情况下如何对信任管理进行合理的资源编排、如何存储与实时更新每一个节点的信任度并保证其安全准确是需要研究的问题.且万物互联信任体系不仅仅包含信任空间体系结构,还需要考虑信任在时间维度上的变化问题,后续研究点除了继续研究万物互联信任体系在空间上的信任关系外,还需要研究信任度与信任关系随时间的动力学演化问题.

致 谢 在此诚挚的感谢中国工程院院士、东南大学网络空间安全学院名誉院长于全院士在研究选题和思路上给予的指导!

参 考 文 献

[1] Kwak B O, Chung T S. Trust domain based trustworthy networking//Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC). Jeju Island, Korea, 2017: 1247-1259

[2] Kim E, Keum C. Trustworthy gateway system providing IoT trust domain of smart home//Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN). Milan, Italy, 2017: 551-553

[3] Kim E, Chung K, Jeong T. Self-certifying ID based trustworthy networking system for IoT smart service domain//Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC). Jeju Island, Korea, 2017: 1299-1301

[4] Singla A, Bertino E. Blockchain-based PKI solutions for IoT//Proceedings of the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC). PA, USA, 2018

[5] Won J, Singla A, Bertino E, et al. Decentralized public key infrastructure for Internet-of-Things//Proceedings of the 2018 IEEE Military Communications Conference (MILCOM). CA, USA, 2018: 907-913

[6] Ahmed A S, Aura T. Turning trust around: Smart contract-assisted public key infrastructure//Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). New York, USA, 2018: 104-111

[7] Mulhem S, Adi W, Mars A, et al. Chaining trusted links by deploying secured physical identities//Proceedings of the

2017 Seventh International Conference on Emerging Security Technologies(EST). Canterbury, UK, 2017: 215-220

[8] Li Ya-Hui, Zhang Ya-Di, Li Peng, et al. An efficient trusted chain model for real-time embedded systems//Proceedings of the 2015 11th International Conference on Computational Intelligence and Security (CIS). Shenzhen, China, 2015: 428-432

[9] Hu W, Ji D, Wang T, et al. A new trust chain security evaluation model and tool//Proceedings of the International Conference on Security and Privacy in Communication Systems. Beijing, China, 2014: 382-391

[10] Jøsang A, Marsh S, Pope S. Exploring different types of trust propagation//Proceedings of the International Conference on Trust Management. Pisa, Italy, 2006: 179-192

[11] Liao Jun, Zhang Hong, Jiang Li-Ming, et al. Subjective trust model based on intuitionistic fuzzy set theory for MANET. Journal of Nanjing University of Aeronautics & Astronautics, 2011, (4): 19

[12] Li Qiao, He Hui, Fang Bin-Xing, et al. Awareness of the network group anomalous behaviors based on network trust. Chinese Journal of Computers, 2014, 37(1): 1-14(in Chinese)
(李乔, 何慧, 方滨兴等. 基于信任的网络群体异常行为发现. 计算机学报, 2014, 37(1): 1-14)

[13] Gilbert E, Karahalios K. Predicting tie strength with social media//Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Texas, USA, 2009: 211-220

[14] Xiang R, Neville J, Rogati M. Modeling relationship strength in online social networks//Proceedings of the 19th International Conference on World Wide Web. North Carolina, USA, 2010: 981-990

[15] Li Hui, Ma Xiao-Ping, Shi Jun, et al. A recommendation model by means of trust transition in complex network environment. Acta Automatica Sinica, 2018, 44(2): 363-376(in Chinese)
(李慧, 马小平, 施珺等. 复杂网络环境下基于信任传递的推荐模型研究. 自动化学报, 2018, 44(2): 363-376)

[16] Mandelbrot B B. The Fractal Geometry of Nature. New York, USA: WH Freeman, 1982

[17] Song C, Havlin S, Makse H A. Self-similarity of complex networks. Nature, 2005, 433(7024): 392

[18] Zhang Zhong-Zhi, Zhou Shui-Geng, Tao Zou, et al. Fractal scale-free networks resistant to disease spread. Journal of Statistical Mechanics: Theory and Experiment, 2008, 2008(9): P09008

[19] Thulasiraman P, Wang Y. A lightweight trust-based security architecture for RPL in mobile IoT networks//Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference(CCNC). NV, USA, 2019: 1-6

[20] Wang Yu-Biao, Wen Jun-Hao, Zhou Wei, et al. A novel dynamic cloud service trust evaluation model in cloud computing//Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering. New York, USA, 2018: 10-15

[21] Sadique K M, Rahmani R, Johannesson P. Trust in Internet of Things: An architecture for the future IoT network//Proceedings of the 2018 International Conference on Innovation in Engineering and Technology(ICIET). Stuttgart, Germany, 2018: 1-5

[22] Wang Han-Xu, Jiang Jiu-Lei, Li Wei-Min. A dynamic trust model based on time decay factor//Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation. Guangzhou, China, 2018: 2048-2051

附录 1.　信任链体系结构模拟攻击算法.

输入：直接攻击成功概率 $PAtk$，攻击转移成功概率 $PTrans$，节点集合 ***Nodes***，攻击方式选择参数 $alpha$

输出：攻击成功的次数 $atkSuccCount$

步骤：

```
1. INIT 已被成功攻击节点集合 Q 为空，尚未被成功攻击的节点集合 U=Nodes
2. WHILE 集合 Q 为空 DO
3.    a=RandomPick(U)
4.    success=Judge(PAtk)
5.    IF success==1 THEN
6.       Q+={a}, U=U-{a}
7.    END IF
8.    atkSuccCount+=1
9. END WHILE
10. WHILE 集合 U 不为空 DO
11.    pattern=Choose(Atk,Trans,alpha)
12.    a=RandomPick(U)
13.    IF pattern==Trans THEN
14.       success=Judge(PTrans)
15.       IF success==1 THEN
16.          Q+={a}, U=U-{a}
17.       END
18.    ELSE THEN //pattern==Atk
19.       success=Judge(PAtk)
20.       IF success==1 THEN
21.          Q+={a}, U=U-{a}
22.       END
23.    END IF
24.    atkSuccCount+=1
25. END WHILE
26. RETURN atkSuccCount
```

附录 2. 信任邻域网络模拟攻击算法.

输入：拓扑全矩阵 ***FullT***，势能矩阵 ***XMatrix***，初始信任度向量 ***VecCfd***，门限阈值 *ThresT*，直接攻击成功概率 *PAtk*，攻击转移成功概率 *PTrans*，节点向量 ***Nodes***，攻击方式选择参数 *alpha*

输出：攻击次数 *atkSuccCount*，是否攻击成功 *isSucc*

步骤：

1. INIT 已被成功攻击节点集合 *Q* 为空，具有相连未被攻击节点的已被成功攻击节点集合 *QwithC* 为空，被门限控制阻断的节点集合 *OfflineNodes* 为空，尚未被成功攻击的节点集合 *U*=***Nodes***
2. WHILE 集合 *Q* 为空 DO
3. *a*=*RandomPick*(*U*)
4. *success*=*Judge*(*PAtk*)
5. IF *success*==1 THEN
6. *Q*+={*a*}, *QwithC*+={*a*}
7. *U*=*U*−{*a*}
8. END IF
9. *atkSuccCount*+=1
10. END WHILE
11. WHILE 集合 *U* 不为空 THEN
12. *pattern*=*Choose*(*Atk*,*Trans*,*alpha*)
13. IF *pattern*==*Trans* THEN
14. *success*=*Judge*(*Trans*)
15. IF *QwithC* 为空 THEN
16. CONTINUE
17. END IF
18. *cTransSource*=*RandomPick*(*QwithC*)
19. 在 ***FullT*** 中查询 *cTransSource* 相连未被成功攻击、未被阻断的节点集合 *ConnNodes*
20. IF *ConnNodes* 为空 THEN
21. CONTINUE
22. END IF
23. *cAtkTarget*=*RandomPick*(*ConnNodes*)
24. *cfd*=***VecCfd***[*cTransSource*]
25. *p*=***XMatrix***[*cTransSource*][*cAtkTarget*]
26. ***VecCfd***[*cTransSource*]=*cfd*−*x*
27. IF *success*==1 THEN
28. 从 ***FullT*** 中计算 *cTransSource* 相连节点数量 *conCount*
29. IF *conCount*=1 THEN
30. *QwithC*=*QwithC*−{*cTransSource*}
31. END IF
32. *Q*+={*cAtkTarget*}
33. *U*=*U*−{*cAtkTarget*}
34. 在 ***FullT*** 中查询 *cAtkTarget* 相连未被成功攻击、未被阻断的节点集合 *ConnNodes*
35. IF *ConnNodes* 不为空 THEN
36. *QwithC*+={*cAtkTarget*}
37. END IF
38. IF ***VecCfd***[*cTransSource*]<*ThresT* THEN
39. *OfflineNodes*+={*cTransSource*}
END IF
40. END IF
41. ELSE THEN //*pattern*==*Atk*
42. *success*=*Judge*(*PAtk*)
43. IF *success*==1 THEN
44. *cAtkTarget*=*RandomPick*(*U*)
45. *Q*+={*cAtkTarget*}
46. *U*=*U*−{*cAtkTarget*}
47. IF *cAtkTarget* 有相连未被攻击且未被阻断的节点 THEN
48. *QwithC*+={*cAtkTarget*}
49. END IF
50. END IF
51. *atkSuccCount*+=1
52. IF *Q*==*OfflineNodes* THEN
53. *isSucc*=0
54. BREAK
55. END IF
56. END WHILE
57. RETURN *atkSuccCount*, *isSucc*

CHEN Zi-Han, Ph. D. candidate. His research interests include cyber security, encrypted traffic classification and identification, trust architecture, composite deep learning and cyberspace governance.

CHENG Guang, Ph. D., professor, Ph. D. supervisor. His research interests include network security, network measurement, encrypted traffic identification, traffic behavior analysis and proactive defense.

TANG Shu-Ye, M. S. candidate. His research interests include cyber security and VPN network traffic analysis.

JIANG Shan-Qing, Ph. D. candidate. His research interests include network resilience, SDN architecture, and application of blockchain.

ZHOU Yu-Yang, Ph. D. candidate. His research interests include cyber security, moving target defense and intrusion detection.

ZHAO Yu-Yu, Ph. D. candidate. His research interests include network measurement and behavior, next generation network processor.

Background

With the upgrading of communication technology and the development of the Internet and the Internet of Things (IoT), the Internet and the IoT will be integrated into the Internet of Everything (IoE). IoE will become the inevitable trend of the development of the network. Compared with the Internet and the IoT, IoE pays more attention to maintaining the overall security and robustness of the network rather than maintaining the security of a single node in the IoE environment. As a basic model and criterion of trust interaction among nodes in network, trust architecture is indispensable in network node behavior interaction and is the foundation of the overall security of the network. The current mainstream trust architecture is a trust chain model with chain or tree as the trust transmission relation topology, which is widely applied in the Internet identity security authentication system. However, a large number of studies have shown that the defects of chain topology and the lack of quantitative trust measurement make it unable to adapt to the IoE environment.

In this paper, we propose a new generation trust architecture: trust neighborhood network, which is based on Hidden Markov Random Field Model-Confidence Energy Field (HMRFM-CEF) model. First, we innovatively introduce fractal network into the trust architecture. Then, a trust neighborhood diffusion transfer concept in which trust nodes only interact with others in their own neighborhood is proposed. As a supplement of current trust architecture, a quantitative trust management model which contains credibility and trust layers are proposed.

Afterwards, by integrating Markov random field model and hidden Markov model, we propose the mathematical modeling of trust neighborhood network with Hidden Markov Random Field Model (HMRFM). Moreover, a Confidence Energy Field model based on HMRFM (HMRFM-CEF) is proposed based on the properties of potential energy model and trust characteristics of Markov random field model.

Finally, we put forward the Trust Threshold Control model (TTC). By combining HMRFM-CEF with TTC, the architecture realizes the calculation of trust under the dynamic change of trust relationship. Mathematical analysis and simulation results show that compared with trust chain architecture, trust neighborhood network architecture can raise the cost of the attack effectively, reduce the attack success rate in the case of infinite attack period in heterogeneous network environment. It realized the fundamental improvement of the overall network protection ability.

But in actual network environment, trust management of trust neighborhood network requires more calculation and needs to consume more system resources. So, in the case of limited resources, how to schedule the trust management resource reasonably, store and update every node's trust safely and timely are need to research. Moreover, the trust system of the IoE not only includes the trust space architecture, but also needs to consider the change of trust in the time dimension. In addition to continuing to study the trust relationship of the trust system of the IoE in the space, the subsequent research points also include the dynamic evolution of trust relationship over time.

This paper is supported by the National Key R&D Program of China under Grant No. 2018YFB1800602 and No. 2020YFB1804604. This paper is part of the topic for the new generation trust architecture for IoE.

The research team has focused on IoE research for years, and some papers in this field have published in highly-ranked journals.