



专题：5G 组网与 6G 展望

6G 内生安全：区块链技术

聂凯君^{1,2}, 曹宾¹, 彭木根¹

(1. 北京邮电大学网络与交换技术国家重点实验室, 北京 100876;

2. 北京邮电大学信息与通信工程学院, 北京 100876)

摘要: 随着移动通信技术逐渐朝着边缘化、分布式结构的发展, 传统外挂式边界防护的网络安全保障方法将受到越来越多的挑战, 现实中不断涌现的网络安全事故也表明, 需要从信息化系统内不断生长出自适应、自主和自成长的安全能力, 即内生安全。区块链作为一种去中心化的共享账本和数据库, 具有去中心化、几乎不可篡改、全程留痕、可以追溯、集体维护、公开透明等特点, 可以极大地满足内生安全设计需求。首先描述了内生安全的必要性和需求, 然后介绍了作为内生安全重要实现手段的区块链技术, 分析了区块链的主要研究进展和面临的困难与挑战, 提出了未来的研究方向和机遇。

关键词: 分布式; 内生安全; 区块链

中图分类号: TP393

文献标识码: A

doi:10.11959/j.issn.1000-0801.2020004

6G endogenous security: blockchain technology

NIE Kaijun^{1,2}, CAO Bin¹, PENG Mugen¹

1. State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing 100876, China

2. School of Information and Communication Engineering,
Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: With the development of mobile communication technology towards marginalization and distributed structure, the traditional network security method of external border protection will be faced with more and more challenges. The emerging network security accidents also show that it is necessary to grow self-adaptive, independent and self-growing security capabilities from the information system, that is, endogenous security. Blockchain, as a decentralized shared ledger and database, has the characteristics of decentralization, immutability, leaving traces throughout, traceability, collective maintenance, openness and transparency, etc., which can greatly meet the needs of endogenous security design. Therefore, the necessity and demand of endogenous security was described, then the blockchain technology as an important means to realize endogenous security was introduced, the main research progress, difficulties and challenges faced by blockchain were analyzed, and the future research direction and opportunities were put forward.

Key words: distributed, endogenous security, blockchain



1 引言

过去的几十年,移动通信技术的持续演进和创新,是促进我国社会经济发展的强大动力之一,并直接造就了现今移动互联网的繁荣,为支撑我国现代科技发展提供了坚实的基础。随着大数据、云计算、物联网等新兴技术的发展与应用,人、机、物互联所需的通信容量急剧增加,无线网络规模越来越大,基于集中式架构的传统无线网络体系结构所提供的平均速率、时延、连接密度等性能指标亟待突破。为了解决上述问题,主流观点认为,6G 无线网络将进一步朝着资源边缘化和网络分布式演进。与此同时,计算下沉带来的数据隐私和通信安全成为新的焦点问题,传统网络安全需要朝着内涵和自生,即“内生”方向发展。而从硬件设备支持、数据信息共识、安全态势感知、攻击防御方法等角度出发,6G 内生安全提出了 4 个方面的要求:可信增强、智能共识、智能防御和泛在协同。其中,智能共识以分布式节点的共识来排除干扰,为信息和数据提供高等级的安全。

从 1989 年的 Paxos 算法到 2013 年其改进版 Raft 算法,从 1999 年的实际拜占庭容错 (practical Byzantine fault tolerance, PBFT) 算法^[1]到 2008 年比特币中面向拜占庭容错 (Byzantine fault tolerance, BFT) 的工作量证明 (proof of work, PoW) 算法,共识机制早有研究。而作为数字货币的领头者,将共识机制融入区块链技术中,比特币证明了区块链技术为分布式环境下的应用所提供的高安全性,同时也为实现 6G 内生安全中的智能共识提供了重要的思路与方法。

传统的网络安全是一种外挂式安全,即建立一系列安全保护机制,从外部抵御不同种类的恶意攻击。而内生安全更多强调建立一套完备的信息系统安全体系,具备自我免疫、内外兼修、自我进化的特点,从网络内部增强安全防范能力,从源头上抵制攻击的产生。

现有系统缺乏安全性分析和设计,导致当前的网络安全主要面临四大难题:软/硬件设计缺陷导致的安全漏洞;开放式产业生态导致的系统后门无法彻底管控或清除;系统软/硬件代码问题难以穷尽和彻查;软硬件产品的安全性无法从源头加以控制。相比之下,内生安全在系统设计之初进行系统级的安全考量,使系统自身具备免疫能力,不仅能被动地抵御恶意攻击,还能主动地消灭各种安全风险。

因此,作为 6G 的核心关键技术之一,内生安全将与无线网络体系结构分布式和去中心化智能适配。6G 自身蕴含的边缘节点分布式和去中心化等特征,使得区块链技术能够用来提升 6G 内生安全性能。

2 区块链基本原理

2009 年,中本聪最早提出并设计了一种点对点电子现金系统——比特币^[2],由此引出了区块链的概念。区块链是一种在对等网络 (peer to peer, P2P) 中构建信任、并达成节点共识的分布式记账技术。一方面,采用共识机制来解决不可信环境下的信息一致性问题,使所有节点存有相同的交易信息。另一方面,采用数字签名、散列算法等加密技术来保障分布式网络的安全性。

2.1 区块链 6 层模型

区块链基础架构模型自下而上可以分为 6 层^[3],分别是数据层、网络层、共识层、激励层、合约层、应用层,如图 1 所示。

(1) 数据层

数据层是区块链技术的最底层结构,封装了数据区块、链式结构、非对称加密以及时间戳等技术。

(2) 网络层

网络层包括分布式对等网络 (P2P) 的组网机制、数据传播机制和数据验证机制。

(3) 共识层

共识层是区块链技术的核心,封装了网络节点的共识算法,以确保网络能够达到共识。PoW、PBFT、Raft 分别是公有链、联盟链、私有链中

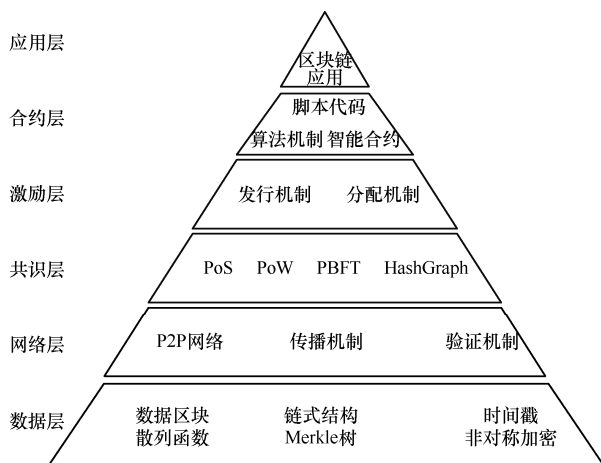


图 1 区块链 6 层模型

具有代表性的共识算法。

（4）激励层

激励层是公有链特有的结构，包括经济激励的发行机制和分配机制。例如，比特币中，激励包括两个部分，一是出块奖励，二是手续费。矿工每挖出一个区块，都会获得相应的奖励和抽取部分手续费。通过激励促使矿工争夺记账，从而达成共识。

（5）合约层

合约层封装了各类脚本语言、算法机制以及智能合约。用户可以将合约信息写入智能合约，在区块链上启动和交易，当合约事件发生时，就会触发智能合约，自动执行合约内容。

（6）应用层

应用层封装了区块链的各种应用场景，例如金融、物流、保险和物联网等。

2.2 区块链五大特征

区块链具有去中心化、信息几乎不可篡改、公开透明、集体维护、安全可信等特点。

（1）去中心化

传统网络中的交易，几乎都需要第三方机构担保。这是一种基于信用的模式，用户需要提交自己的信息给第三方机构，同时第三方机构的存在也会增加交易的成本。区块链的理念就是为了在分布式环境下建立一个去中心化网络达成共识，无须经过第三方机构确认。在区块链网络中，

不存在中心化节点，各个节点的地位平等，都能够发布交易、读取链上信息。

（2）几乎不可篡改

区块链中使用散列（Hash）算法对区块进行加密，每一个区块都存储了上一个区块的散列值，任何信息的修改，都必须改变散列值。归功于基于时间戳的链式存储结构，散列值的修改难度和代价极高，确保了信息几乎不可篡改。换句话说，在不超过区块链系统错误容忍度（一般为 33%~51%，视具体区块链技术而定）的前提下，信息一旦上链，就会被永久保存，几乎不可篡改撤销。

（3）公开透明

区块链中，矿工节点每生成一个区块，就会立刻向全网广播，实现全网数据区块的同步。所有节点都会保存最长主链的信息，新加入的节点可以向周围节点访问获取主链信息，节点可以回溯链上的所有交易信息。

（4）集体维护

区块链网络的共识是由所有节点共同决定的，区块链上的数据块由所有的节点共同维护，少数节点失效并不影响网络运作。每一个数据块需要经过所有节点的验证，得到绝大多数节点的批准才可以上链。

（5）安全可信

区块链采用散列算法、非对称加密、数字签名等密码学原理对信息进行加密，同时借助有效的共识机制来抵制恶意攻击，确保了数据的不可伪造和几乎不可篡改，具有极高的安全性。例如，基于算力机制的 PoW 共识算法，只有掌握全网 51% 的算力，才有可能做到对信息的篡改；基于投票机制的 PBFT 共识算法，只有超过 1/3 的恶意节点，才能篡改区块信息。

2.3 区块链基本流程

如图 2 所示，6G 区块链的工作流程主要分为如下步骤^[4]。

（1）所有需要内嵌安全功能的 6G 边缘节点（包



括边缘基站和边缘终端)运行在同一区块链中。

(2) 目标边缘节点生成一个交易,并将其广播至区块链中的其他边缘节点中。

(3) 其他边缘节点收到该交易后验证其是否合法。

(4) 所有处于同一区块链中的边缘节点根据共识机制选出新区块的生成者来生成并广播新区块。

(5) 所有边缘节点将新区块添加至自己的本地账本。

(6) 存至区块链账本中的交易信息触发智能合约。

(7) 边缘设备实现自适应匹配和行为决策并执行相应的任务,例如,供应链场景下的移动集装箱操作、智能能源场景下的能源供给操作等。

3 区块链关键技术

区块链关键技术包括共识机制、加密技术、数据结构以及智能合约,共同保障了区块链网络的稳定运行。

3.1 共识机制

共识机制是一套能够维护区块链系统稳定运行的方法,是区块链的最核心技术,其主要思想是在分布式环境下,使得互不相信的节点之间能够就某些信息达成一致意见。

共识机制可以分为两种类型,一类是基于证明的共识机制;另一类是基于投票的共识机制。PoW 是最具代表性的基于工作量证明的共识机制,比特币中采用的就是 PoW 算法,通过算力来保证区块链数据的安全可靠,其他主流的基于证明类的算法还有 PoS (proof of stake)、DPoS (delegated proof of stake) 等;PBFT 是具有代表性的基于投票的共识机制,数据只有被全网中大多数节点确认,才可以加入区块链,其他主流基于投票类的算法还有 Raft、Tangle、HashGraph 等。

3.2 加密技术

区块链采用的加密技术确保了链上的数据不可伪造、几乎不被篡改,保障了区块链网络数据的安全可信。区块链中主要应用的加密技术分别

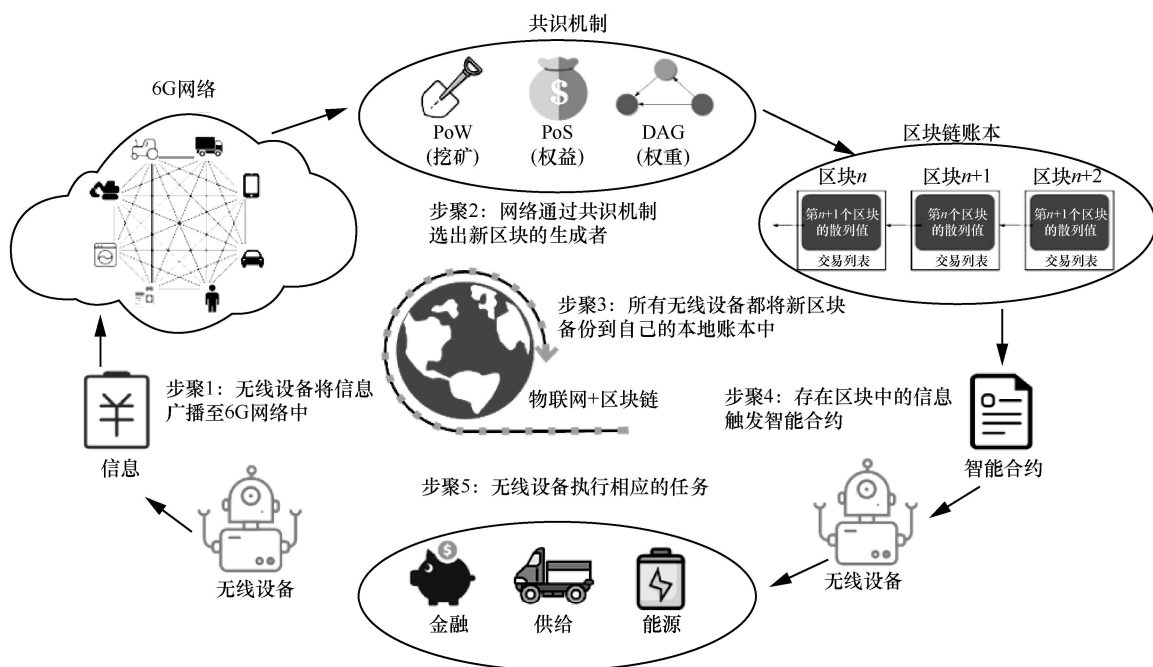


图2 6G 区块链流程

是散列算法和非对称加密。

(1) 散列算法

任意长度明文字符输入都会输出固定长度的散列值。散列算法对输入非常敏感,即使输入发生了微小改变,输出值也会发生很大的变化。散列算法具备两大特性:抗碰撞和隐秘性。抗碰撞是指无法找到两个不同的值 x 和 y ,使得 $H(x)=H(y)$,比特币中采用的 SHA256 算法,输出共有 2^{256} 种取值,理论上要输入 $2^{256}+1$ 次才能发生一次 Hash 碰撞。隐秘性是指无法通过散列值逆向推导得出原始输入数据,想要求出原始输入,只能通过穷举的方法。

(2) 非对称加密

非对称加密因其在加密和解密过程中使用不同的加密/解密密钥而得名。非对称加密使用两个非对称的密钥,分别是公开密钥和私有密钥,简称公钥和私钥。公钥和私钥是成对出现的,都可以对数据进行加密,但是必须是一个进行加密,另一个进行解密。区块链中一般采用私钥来加密,公钥来解密,公钥向全网公开,私钥则由用户自己保存。比特币中,A 向 B 支付一笔交易,A 需要使用自己的私钥对交易进行签名,全网节点使用 A 的公钥对交易进行验证。

3.3 数据结构

区块链采用链式结构来连接数据区块,保证数据区块的有效性;采用 Merkle 树来保存数据交易,保证交易不被篡改。

(1) 链式结构

区块链中,除了创世块(第一个区块)以外,当前区块都要存储前一个区块的 Hash 值,以此链接到前一区块。各个区块间依次环环相扣,形成了一条完整的链,从而记录数据区块的完整历史,同时也保证了数据区块几乎不可篡改。

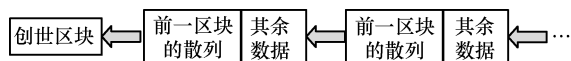


图3 区块链链式结构

(2) Merkle 树

Merkle 树实际上是一种满二叉树形式的数据结构,其最底层的每个叶节点保存的是每一笔交易的散列值,而非叶节点保存的是其两个子节点串联起来的散列值,如此递归最后只剩最顶层一个根散列值,记为 Merkle 根。Merkle 树是区块链中一种重要的数据存储结构,任何一笔交易的篡改都会引起 Merkle 根值的改变,从而保证了交易的几乎不可篡改。

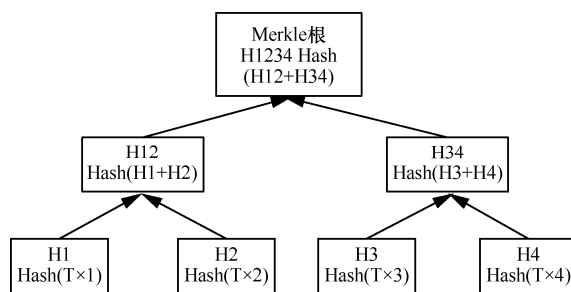


图4 Merkle 树结构

3.4 智能合约

智能合约是一段运行在区块链系统上的编程代码,通过将合约条款写入区块链系统,当特定的事件发生后,就能触发合约自动执行。

早在 1995 年智能合约的概念就被提出,然而因为技术的不成熟和兼容性,一直未能得到应用,直到区块链技术的诞生。比特币脚本是智能合约的雏形,但其系统是非图灵完备的,缺乏灵活性和可拓展性,并不能算是真正的智能合约^[5]。直到 2013 年,作为以太坊智能系统的一部分,智能合约真正从理论落地于实践,用户可以基于以太坊构建自定义的智能合约。以以太坊智能合约为例,用户在以太坊上编写智能合约主要有 3 个步骤:

(1) 用户按照商业逻辑使用 Solidity 等脚本语言编写智能合约;

(2) 以太坊虚拟机(EVM)将脚本编译成字节码;

(3) 用户将智能合约发布到区块链网络,等待被调用。

智能合约使得规则和契约可以通过代码的形



式进行传递，是区块链技术的一大创新。随着区块链技术的快速发展和智能合约的不断完善，智能合约有望达到“合约即法律”的高度。

4 国内外进展

区块链技术自面世以来，逐步发展为学术界热门研究话题之一，随后逐渐渗透到产业界的各个应用领域。

利用区块链构建 6G 分布式无线网络是一个新兴且热门的方向。有学者提出将区块链应用于智慧医疗，将病人的电子病历、基因数据等记录到区块链上，保障病人健康数据的隐私和安全。还有其他学者研究将区块链应用于物流产业，将货物的温度、湿度等信息记录到区块链上，保证货物的质量安全，并且提高物流效率。另外，利用区块链技术进行数据验证也是一个热门话题。区块链可以永久地安全保存各类许可证书、登记表等，通过访问区块链上的数据，可以快速地对数据进行公证和审计。

目前，国外有不少研究机构致力于研究适用于无线网络的区块链技术。Hedera 公司推出 Hedera Hashgraph 区块链平台，其区块链底层是一种基于投票机制的 Hashgraph 算法，理论上每秒能够处理数十万笔交易。IOTA 提出了一种面向物联网环境下的区块链——Tangle^[6]，这种区块链无须支付交易手续费，其基于有向无环图的结构使交易吞吐量得到巨大突破。

在企业领域，Factom 公司基于区块链设计了一套完整的、不可更改的审计流程与方法，帮助审计师实现高效低成本审计。IBM 公司致力于打造企业级区块链平台，其 Hyperledger Fabric 区块链网络应用场景包括：供应链、食品信托、政企身份管理。Gen 公司与飞利浦区块链实验室合作研发了 Gen Health 区块链系统，优化了药品供应链和医疗数据的安全管理。

国内对于区块链的研究较国外稍晚，但是中

国对区块链的技术研究却是处于全球领先水平，中国区块链专利申请数量占比超过半数，居全球第一。国内许多学者对区块链进行了理论研究。例如，面向无线网络的区块链共识算法设计，优化和改善现有共识算法性能；面向物联网的区块链系统建模，理论分析吞吐量、确认时延、恶意节点攻击概率等各项性能指标及安全性问题^[7-8]。

高校方面，我国有 10 多所顶尖大学开设了区块链课程，并且成立了区块链实验室。清华大学正式成立区块链教育与产业联盟“青藤联盟”，并且创立区块链创新实验平台“青藤链”。北京大学区块链研究中心和 FutureNet 签约，合作成立区块链联合实验室。浙江大学汇聚浙江大学计算机学院、软件学院等相关优势学科研究力量，成立方图区块链研究中心。

在产业界，百度采取可插拔的共识机制、DAG 并行网络，用于突破当前区块链的技术瓶颈，打造 XuperChain，以此来提升网络的吞吐量。阿里巴巴蚂蚁区块链团队致力于研究区块链中的共识协议、跨链协议等，总计发明区块链专利约 1 000 件。腾讯公司打造腾讯云区块链 TBass 平台，服务众多政务、医疗、金融等行业用户，为解决机构、部门之间的数据可信共享提供了解决方案。

5 未来挑战

目前，区块链技术处在未成熟阶段，行业标准尚未建立，在诸多方面存在着问题与挑战。

首先，共识机制决定了区块链系统的性能，但是目前的共识机制都存在不同的缺陷，3 种主流的共识算法性能比较见表 1。PoW 机制消耗大量计算资源且吞吐量极低；PoS 虽降低了计算资源消耗、提高了交易吞吐量，却会带来寡头垄断的风险，与去中心化背道而驰；PBFT 面临广播带来的通信开销过大问题，系统的扩展性被大大限制。因此，共识机制设计将是未来区块链技术面临的一大技术挑战。

表1 共识算法性能比较

共识算法	PoW	PoS	PBFT
类型	公有链	公有链	联盟链
拜占庭容错	<51%算力	<33%的总资产	<33%的投票
交易费	有	有	无
交易吞吐量	7 Tbit/s	100 Tbit/s	200~2 000 Tbit/s
交易时延	高	低	低

其次,在实际区块链网络中,共识节点的能力存在差异,安全防护等级层次不齐^[9],使得分布式体系架构与区块链共识难以匹配,系统的安全性与稳定性难以得到保障。区块链技术与实际网络的匹配和联合优化,还需要进一步研究。

区块链技术面临着诸多问题和挑战,未来还需要实现无线通信、边缘/雾计算、安全技术^[10]的深度融合,相关的基础理论和关键技术需要进一步突破,以便推动区块链技术在6G中的应用与可持续发展。

6 结束语

区块链技术与6G深度融合,实现6G分布式节点间的智能共识,会面临新架构、新技术等全新挑战,对其也有了新的要求。一方面,就区块链技术本身而言,其基础理论和关键技术应当进一步完善与突破,为其融入6G做好充足的技术理论铺垫;另一方面要从设计规划入手,结合6G的特点与架构,形成适用于6G的区块链技术,以支撑人机物高效安全便捷互联的需求。

参考文献:

- [1] ASTRO M, LISKOV B. Practical Byzantine fault tolerance[Z]. 1999.
- [2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB]. 2018.
- [3] YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
- [4] CAO B, LI Y X, ZHANG L, et al. When internet of things meets blockchain: challenges in distributed consensus[J]. IEEE Network, 2019(7): 1-7.
- [5] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain technology: architecture and progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.
- [6] SERGUEI P. White paper of IOTA[R]. 2018.
- [7] LI Y X, CAO B, PENG M G, et al. Direct acyclic graph based blockchain for internet of things: performance and security analysis[J]. 2019.
- [8] SUN Y, ZHANG L, FENG G, et al. Blockchain-enabled wireless internet of things: performance analysis and optimal communication node deployment[J]. IEEE Internet of Things Journal, 2019, 6(3): 5791-5802.
- [9] 韩璇, 袁勇, 王飞跃. 区块链安全问题研究现状与展望[J]. 自动化学报, 2019, 45(1): 206-225.
HAN X, YUAN Y, WANG F Y. Research status and prospect of blockchain security [J]. Journal of Automation, 2019, 45(1): 206-225.
- [10] 李聪, 雷波, 解冲锋, 等. 基于区块链技术的可信网络[J]. 电信科学, 2019, 35(10): 60-68.
LI C, LEI B, XIE C F, et al. Trusted network based on blockchain technology [J]. Telecommunications Science, 2019, 35(10): 60-68.

[作者简介]



聂凯君 (1996-), 男, 北京邮电大学硕士生, 主要研究方向为区块链技术。



曹宾 (1983-), 男, 博士, 北京邮电大学网络技术研究院副研究员, 主要研究方向为区块链系统、物联网和移动边缘计算。



彭木根 (1978-), 男, IEEE Fellow, 教育部“长江学者”特聘教授, 国家杰出青年科学基金获得者, 入选“万人计划”科技创新领军人才、科睿唯安2019年度ESI全球高被引科学家和2019年首都科技盛典十大科技人物, 网络与交换技术国家重点实验室副主任, 中国通信学会青年工作委员会主任, 北京市科技人才研究会副理事长。长期从事移动通信智能组网理论及关键技术研究工作。累计发表IEEE期刊论文100余篇, 其中ESI高被引用论文累计19篇, 谷歌学术引用近万次。获得IEEE通信学会海因里希·赫兹奖、IEEE通信学会亚太区杰出青年学者奖等。受邀担任IEEE IoT-J、IEEE Communications Magazine等国际期刊指导委员会委员或编委等。以第一完成人身份获得国家技术发明奖二等奖(2018年)、北京市科学技术奖一等奖(2017年)、中国通信学会科学技术奖一等奖(2015年)、求是杰出青年成果转化奖(2018年)等。