

· 专题:5G移动通信基础理论与关键技术 ·

智能移动通信新架构探索

葛宁* 陈旭 冯伟

北京信息科学与技术国家研究中心 清华大学电子工程系,北京 100084

[摘要] 围绕移动通信网络发展面临的效率与安全问题,探讨构建智能移动通信架构的思路和技术发展途径。针对无线环境、移动业务等复杂不确定性挑战,新架构通过引入网络知识,利用知识的积累演进,不断适应多样变化的应用场景与要求;通过构建分布式全局优化方法,优化完善信息服务体系,形成网络通信服务能力增长新机制。在此基础上,进一步建立移动网络与互联网服务协同途径,构建“服务商—运营商—用户”多方博弈框架,丰富网络安全经济模型,发展通信入口管控方法,为变革网络安全格局提供新机制。

[关键词] 移动网络;智能通信;协同优化;用户行为;入口管控

4G、5G等移动通信网络的迅速发展,为移动互联网、物联网等提供了坚实的底层通信支撑。同时,复杂多变的应用场景,也对移动通信网络的安全和效率提出了全新挑战^[1,2]。一方面,传统通信能力增长严重依赖基础设施和资源投入,如从2G到5G,基站密度不断增加,单小区覆盖半径已达百米极限,通信效率提升亟待开拓新维度^[3,4];另一方面,恶意流量泛滥,网络安全形式日益严峻,如恶意流量在机器流量中的占比已超过50%^[5],亟待建立新型通信安全机制。

为了突破无线网络安全与效率瓶颈,探索将智能技术引入通信领域,构建智能与通信相融合的新型网络架构,一方面能够灵活适应复杂变化的通信环境与业务形态;另一方面有望解决万物互联及通信网络自身发展面临的高效组织、学习演进、安全可靠问题。

1 以智能协同应对复杂不确定性

现有网络以互联互通为目的,服务主要由云中心提供。云—网分立框架导致网络与信息服务割裂,整体信息服务能力提升遭遇边际效应递减。未来智能通信新架构应以构建网络信息秩序、协调网络行为为目的,将网络与信息服务融合,分布式共享



葛宁 清华大学研究员、博士生导师、电子工程系通信所所长。主要从事通信片上系统、短距离无线通信、宽带无线网络等方面的研究工作。先后负责国家科技重大专项、863目标导向、973课题和国家自然科学基金重点项目等。发表SCI论文40余篇,申请专利20余项,获得集成电路布图设计专有权2项。获得2017年通信学会科学技术奖一等奖、2014及2017年吴文俊人工智能科学技术进步奖一等奖、2016年电子学会创新团队奖。

传输、处理、存储资源,面向多样化用户的大规模信息体系组织,由网络提供信息基础服务能力。在此新框架下,云中心将向信息体系高层次演化,面向多样化应用进行管控与优化。新型框架通过网络化的知识运用,大幅减轻底层数据汇聚带来的带宽、处理压力,逐步向更大规模、更加自主的信息服务体系发展。

新架构也要为解决网络容量增长面临的电磁环境和业务需求的复杂不确定性难题提供新途径^[6]。传统理论以简化模型应对复杂不确定性,造成大量数据开销和资源利用的瓶颈^[7,8]。在新架构下可以通过智能方法构建知识库,以层次化模型表征环境和业务中的复杂不确定性,大幅提升模型准确性,以模型开销代替数据开销,解决资源效率提升的瓶颈问题。此外,可将知识引入移动通信网络的优化,建

收稿日期:2020-04-06;修回日期:2020-04-10

* 通信作者,Email:gening@tsinghua.edu.cn

本文受科技部变革性技术关键科学问题“智能通信架构与可信协议基础”重点专项(2018YFA0701601)资助。

立“环境—通信”和“内容—通信”的闭环控制架构，通过知识的增长与闭环运用将不断提升资源利用的程度和范围，形成网络通信容量增长新机制。

具体地，高效提升通信容量须另辟蹊径：着眼于通信的载体，可建立基于区域无线环境学习、自主适应的通信框架；着眼于通信的对象，可建立基于网络相关内容、面向感知质量优化的服务新框架；立足通信构筑新的安全架构，可建立安全监测与恶意行为管控协同的新框架。一种可能的智能移动通信新架构如图 1 所示。为引入智能，设计智能协同优化平台；针对无线环境、媒体内容和通信行为，通过归纳学习构建相应的知识库。新架构的突出特点体现在：① 利用知识库刻画复杂干扰、业务内容特性，通过智能优化与代理服务大幅提升资源效率；② 构建基于身份的可信协议，减少通信行为的不确定性；进而，分析恶意行为来源，大幅降低移动接入端的恶意流量。

从信息通信产业现状来看，首先，现有基站组网覆盖技术对站址选择要求苛刻，需经过繁冗的网络规划来适应环境。可基于新架构发展无线环境感知与按需覆盖技术，使基站具有学习与适应环境的能力，从而极大拓展站址资源选择范围，变革移动网络的规划与部署模式。其次，现有移动通信网络难以支持个性化服务需求。可基于新架构发展智能通信服务技术，通过引入个性化知识库，一方面可实现“窄带通信、宽带体验”，另一方面可为个人提供基础信息服务，打破互联网巨头对用户信息的垄断。此外，现有网络安全缺乏行为级管控技术，可基于新架构发展可信协议与恶意通信行为监控技术，从而在网络接入端形成恶意通信行为管控新能力。

2 从入口管控探索安全与效率共赢的新机制

在智能移动通信新架构下解决网络安全问题，需要考虑网络对用户通信行为的影响，应当充分发挥移动通信网络接近用户终端的区位优势，着眼安全与效率共赢的目标，基于用户身份识别信息，实施

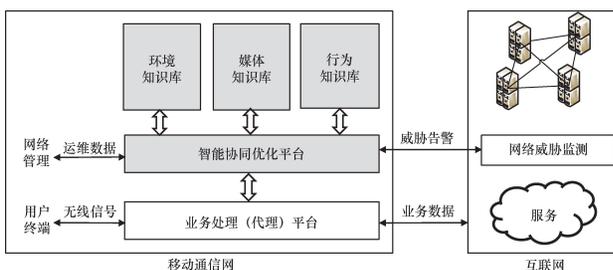


图 1 智能移动通信网络新架构

恶意用户行为级监测和入口管控，遏止恶意流量蔓延势头，进一步提升网络整体通信效能。

经济模型是网络安全体系重构的基础^[9]。构建移动网络与互联网安全协同，需要首先考虑移动网络运营商实施用户行为入口管控的成本收益问题，强化运营商参与网络安全治理意愿^[10]，建立运营商、服务商和用户三方博弈框架。运营商提供安全服务，实施用户管控，努力提升网络效能，用户通信行为接受运营商监管并获得高质量互联网服务，服务商提供用户服务，同时订购安全服务以保证业务安全运作。各方成本收益情况如表 1 所示。

三方博弈系统结构如图 2 所示，虚线表示需要加强部分。一方面，服务商与运营商相互协作，运营商为服务商提供业务安全保障，同时恶意流量的减少能够提升网络通信效能，增加运营商效益，促使运营商提高安全管控能力。另一方面，运营商网络安全管控能力的提升，能够增加恶意用户的攻击成本，提升正常用户获得互联网服务的安全品质，进而保护服务商的安全利益，最终形成良性互动安全博弈格局。

在此安全经济模型基础上分析当前网络安全体系架构，容易发现，当前网络安全问题难以得到彻底解决，主要原因在以下两个方面。

首先，在横向上，移动通信网络安全与互联网安全割裂，如图 3 所示。端对端的业务安全涉及终端与应用服务双方，横跨移动网络与互联网两个网域。

表 1 网络安全博弈三方成本收益结构

博弈者	成本	收益
运营商	网络安全监管服务投入	安全服务收益，网络效能提升
服务商	订购安全服务的成本	业务正常运转，不必自建安全系统
用户	通信行为接受运营商监管	良好的互联网服务质量

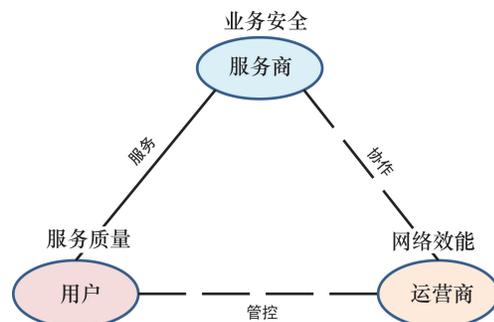


图 2 网络安全三方博弈框架图

以往的移动通信网络和互联网安全体系,独立研究、分立建设,互不协同,而移动网络接入端源发的安全问题往往在互联网服务端才能体现出危害性,因此网络安全问题不能仅依靠移动网络或互联网任何一方单独解决,需要建立跨网协同机制。

其次,在纵向上,底层网络安全与上层应用服务安全割裂。网络信息服务体系包括用户、网络与应用服务三大要素,当前移动网络安全架构主要按照底层数据传输安全和上层应用安全的逻辑划分^[11](如图4所示),导致网络难以监管通信服务,给恶意用户留下可乘之机。因此,只有底层网络与上层服务协同,才有望实现更加高效的安全管控体系^[12]。

综合上述分析,网络安全问题的有效解决,需要基于智能协同优化平台,建立以用户为中心的信誉评估系统和以行为知识库为支撑的恶意行为检测识别系统,构建上下联动、跨域协同的行为级网络入口安全管控体系。

依托移动通信网络的身份标识和地址分配机制,建立终端用户身份与网络IP地址的关联映射,通过地址检验机制,在移动网入口遏止IP地址仿冒等恶意行为。通过让网络适度掌握应用服务类型等信息,使得网络能够更深入地了解和掌握应用服务,进而理解用户行为特征,建立用户信誉评价系统,为用户行为意图分析奠定基础。

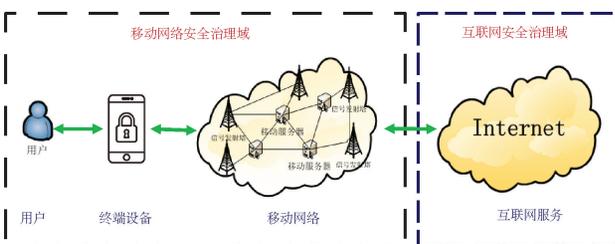


图3 网络安全治理的横向划分

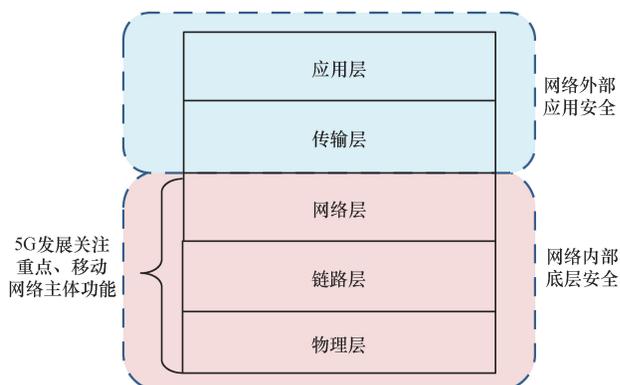


图4 网络安全风险的纵向层次划分

通过打通移动通信网络与互联网安全体系的分立局面,将互联网威胁告警数据引入用户行为知识库,经过深度挖掘运用,提取恶意行为特征模型,建立恶意行为监测识别方法。对网络用户的通信行为进行实时监测和分析。恶意行为一经判定,立即在移动通信网络入口处实施管控或阻断。通过建立跨域协同的网络安全行为管控机制,能够有效控制互联网恶意流量规模,进一步提升网络资源利用效率。

机制上,安全管控技术发展要引入风险度量策略和奖惩机制,以遏制攻击者从事恶意行为的动机,将事后处理转变为事先预防,根据安全风险概率,动态调整对用户通信行为的抽检程度,在确保有效威慑的同时降低管控成本,实现安全与效率共赢。

3 结论与展望

在移动通信网络技术发展和代际演进中,复杂不确定性导致的安全与效率问题难以通过简单的网络设备规模增长解决。网络化知识和博弈论经济模型的引入,为提升移动通信网络效能开辟了潜在发展空间。移动通信跨越式发展需突破面向稳态分解的技术思路,发展面向适变体系的理论,借助交叉学科研究,围绕降低不确定性的本质问题,揭示网络宏观运作与演进的规律,为物联网、工业互联网等新兴需求发展提供理论技术途径。

致谢 特别感谢陆建华院士对本文研究工作的指导,以及周华春、金石、张文逸教授等课题负责人对本文研究工作的帮助。

参 考 文 献

- [1] Feng W, Wang JC, Chen YF, et al. UAV-aided MIMO communications for 5G internet of things. *IEEE Internet of Things Journal*, 2019, 6(2):1731—1740.
- [2] Chen X, Feng W, Ge N, et al. Defending link flooding attacks under incomplete information: a Bayesian game approach. *Proc. IEEE ICC'2020, Dublin, Ireland*, 2020.
- [3] FG-NET-2030. A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond, Network 2030, ITU-T, 2019.
- [4] 6G Flagship research program. Key drivers and research challenges for 6G ubiquitous wireless intelligence, University of Oulu, 2019.
- [5] Distil Networks. 2018 Bad Bot Report, <https://resources.distilnetworks.com/whitepapers/2018-bad-bot-report>, 2019.
- [6] 陆建华, 葛宁, 杜冰. 复杂性与不确定性: 无线通信面临的双重挑战. *中国科学: 信息科学*, 2013, 43(12): 1563—1577.

- [7] Feng W, Wang Y, Ge N, et al. Virtual MIMO in multi-cell distributed antenna systems: coordinated transmissions with large-scale CSIT. *IEEE Journal on Selected Areas in Communications*, 2013, 31(10):2067—2081.
- [8] Feng W, Wang Y, Lin D, et al. When mm Wave communications meet network densification: a scalable interference coordination perspective. *IEEE Journal on Selected Areas in Communications*, 2017, 35 (7): 1459—1471
- [9] Anderson R, Moore T. *The Economics of Information Security*. Science, 2006, 314(5799): 610—613.
- [10] Osterweil E, Stavrou A, Zhang LX. 20 Years of DDoS: a Call to Action. <https://arxiv.org/pdf/1904.02739.pdf>, 2019.
- [11] Ericsson. A guide to 5G network security. <https://www.ericsson.com/en/security/a-guide-to-5g-network-security>. 2019.
- [12] Huawei White Paper. 5G Security: Forward Thinking. Huawei Technologies Co., Ltd. 2015.

New Network Architecture for Intelligent Mobile Communications

Ge Ning* Chen Xu Feng Wei

Beijing National Research Center for Information Science And Technology,

Department of Electronic Engineering, Tsinghua University, Beijing, 100084

Abstract Focusing on the efficiency and security issues faced by the development of mobile communication networks, we discuss the ideas and technical development approaches for building an intelligent mobile communication architecture. Aiming at the complex and uncertain challenges of wireless environment and mobile services, the new architecture adapts to various application scenarios and requirements by introducing network knowledge and its evolution mechanisms. Through building a distributed global optimization method, the new architecture optimizes and developsthe information service system, to form new growth mechanism of network communication service capability. On this basis, a further collaborative approach is established between the mobile network and Internet services, creating a multi-party game framework consists of operators, service providers and malicious users which enriches the economic model of network security. It enables a user access control method at communication entrance, which provides a potential mechanism for reforming network security pattern.

Keywords mobile network; intelligent communication; collaborate optimization; user behavior; entrance management

(责任编辑 姜钧译 吴妹)

* Corresponding Author, Email: gening@tsinghua.edu.cn