面向 6G 网络的可信需求与应用场景研究*

刘秋妍[1],李铭轩[1],吕 轩[2],李佳俊[3],张忠皓[1],李福昌[1],朱雪田[1]
(1.中国联合网络通信有限公司研究院,北京 100048;
2.中国联合网络通信有限公司北京分公司,北京 100031;3.中国联通华盛通信有限公司,北京 100031)

摘 要:基于 5G 网络应用现状及技术发展趋势分析,提出网络可信是 6G 网络重要发展趋势之一,并对比分析了网络可信与网络安全的概念内涵,阐述网络安全基于“有罪假设”的本质及其在下一代网络应用中面临的困境,提出基于“无罪假设”的网络可信在下一代网络应用中的必要性。最后面向 6G 网络工作频段提升、建设运维成本增加、天地一体化等发展趋势,对 6G 网络共建共享、天地互联、超大规模物联网中面向网络的可信需求进行系统分析。

关键词:无线通信;6G;网络可信;需求分析
中图分类号:TN929.5 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.211361

中文引用格式:刘秋妍,李铭轩,吕轩,等. 面向 6G 网络的可信需求与应用场景研究[J].电子技术应用,2021,47(3):5-7.
英文引用格式:Liu Qiuyan,Li Mingxuan,Lv Xuan,et al. Trustworthy requirements and application scenarios in 6G network[J]. Application of Electronic Technique,2021,47(3):5-7.

Trustworthy requirements and application scenarios in 6G network

Liu Qiuyan[1],Li Mingxuan[1],Lv Xuan[2],Li Jiajun[3],Zhang Zhonghao[1],Li Fuchang[1],Zhu Xuetian[1]
(1.China Unicom Research Institute,Beijing 100048,China;
2.China Unicom Beijing Branch,Beijing 100031,China;3.China Unicom Huasheng Co.,Ltd.,Beijing 100031,China)

Abstract: In this paper, trusted networking is proposed as one of the most important technologies trend in 6G network according to the status of services and applications in 5G network. In 6G network, network trust is proposed as a complementary concept of network security. Compared with network security based on the presumption of guilt, network trust is designed based on the presumption of innocence to prove itself without network attack of threat. Finally, trust requirements in next generation network are analyzed with the trend of higher frequency spectrum, capital expenditure, operational expenditure, and multi-domain integrated, including random access network sharing, space-ground integrated network and massive connection Internet of Things.
Key words: wireless network;6G;trusted network;requirement analysis

0 引言

6G 网络的演进趋势除了在现有 5G 网络的通信能力(如带宽、时延、可靠性、连接)和信息化水平(如云化水平、智能化水平、安全等级)的基础上进一步增强之外,还需要面向未来多方共建共享、天地融合三维立体泛在接入、超大规模分布式连接等典型场景需求提升网络可信能力。与面向攻防对抗的网络安全理念不同,网络可信是面向网络自身的自证清白能力。

1 6G 网络发展趋势

随着 5G 网络商用部署的逐渐展开,数以亿计的 5G 用户在体验 eMBB、uRLLC、mMTC 移动互联业务的同时,也对移动网络质量提出了更高的需求[1-5]。AR、VR、XR 以及全息等新媒体业务是视频图像类的热点业务,但是单用户百 Mb/s 级 5G 网络只能提供新媒体业务的初级体验,而 8 K~16 K 沉浸式 AR 业务则至少需要 0.5 Gb/s~1 Gb/s 的用户体验速率,如果是全息视频业务,其带宽需求将至少在 Tb/s 级。在泛在接入方面,虽然全球地面移动网络覆盖已经超过 90%,甚至部分国家已经超过 98%,但是目前移动用户仍然无法在飞机上实现泛在接入,而且少数尚未实现网络覆盖的偏远地区由于网络建设难度和成本收益的问题,短时间内也难以解决。在传输时延方面,无线信道的衰落特性导致时延抖动无法支撑工业机械手、自动驾驶等对时延和时延抖动要求严苛的精细化设备控制。因此,6G 技术发展趋势之一就是在 5G 网络大带宽、低时延、泛在接入能力的基础上进一步增强,为 6G 业务提供 Tb/s 级带宽、空天地一体泛在接入和面向极低时间超高可靠性的网络服务质量保障[6-9]。

除了带宽、时延、接入等传统的通信域(Communica-

*基金项目:国家重点研发计划“6G 网络架构及关键技术”项目(2020-YFB1806700)

tion Technology, CT)能力增强之外,6G 技术发展的另一个维度就是 IT 能力增强。6G 在继承 5G 核心网资源池化和架构服务化的基础上,不仅有将无线侧云化开源解耦的趋势,而且亟需通过更普及的算力部署将人工智能、大数据分析、安全防御等 IT 能力由外挂辅助式转化为内嵌式的内生能力,提升网络弹性至简、按需服务、自治运维和安全防御的智能化程度。

网络 CT 域能力提升的同时,伴随着频段提升、小区半径减小、网络建设运营成本提升以及三维立体泛在接入需求,多方参与网络共建共享模式将从地面网络共建共享逐步扩展到天地融合、公专融合、固移融合等领域,建立可信的网络信任体系则成为 6G 网络发展的重要趋势。网络 IT 域能力的提升是通过大部分软件能力和少部分新型硬件能力实现的,同时也引入了威胁网络信任体系的新型风险,如何在现有网络安全纵深防御体系的基础上建立能够自证清白的可信网络信任体系是支撑 6G 网络共建共享发展模式的核心基础。

2 网络可信与网络安全

2.1 网络安全

网络安全(Network Security)是指通过网络中的物理硬件、存储数据、网络连接、操作系统乃至应用软件等各层均受到有效的防御措施保护,不遭受因偶然误操作或者恶意攻击而导致的网络中存储或传输数据被破坏、更改、泄露,网络服务中断或系统无法连续可靠正常地运行等异常事件发生[10-11]。

网络安全的概念是与网络攻防息息相关的,因此,网络安全技术体系也是以网络攻防对抗为主线发展开来的,网络防御技术是以对抗网络攻击杀伤链为对抗目标的,如网络边界的漏洞威胁感知检测、自动实时安全隔离,网络层的深度协议解析,终端层的访问控制、智能动态防御响应,以及数据层的安全加固等防御技术都是面向网络攻击或者假设存在网络攻击,是从“有罪论”的角度进行防御设计的,最终实现使网络攻击“进不来、改不了、出不去、逃不掉”的纵深防御。

2.2 网络可信

网络可信(Trustworthy Network)是指网络的输出结果是符合预期[12-13]。与网络安全的“有罪论”逻辑不同,如图 1、图 2 所示,网络可信通过建立从底层数据到终端软硬件、网络传输和网络边界的信任链传递机制,实现基于“无罪逻辑”的自证清白。除了防御网络攻击之外,在没有发生网络攻击的大部分日常网络运营维护中,或存在攻击特征尚未被完全掌握的“0 日漏洞”和处于静默期的高级持续性威胁(Advanced Persistent Threat, APT)的场景中,物理世界对网络世界更多的需求是如何通过逻辑自洽,自证清白,向物理世界提供面向网络的可信体系,即网络可信。

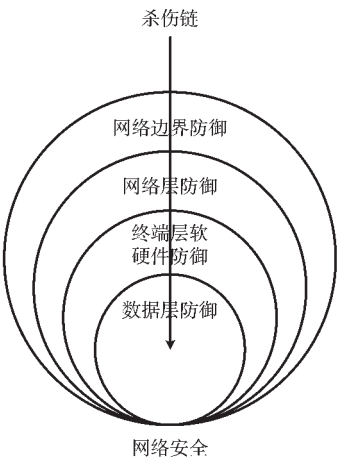

图 1 网络安全概念示意图

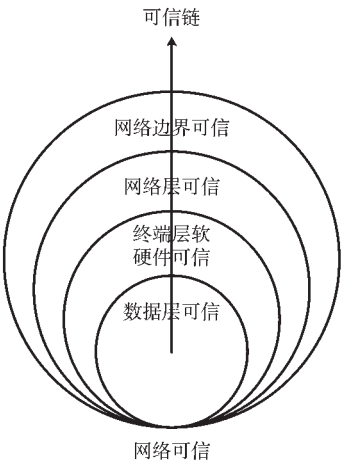

图 2 网络可信概念示意图

3 6G 网络可信需求分析

3.1 共建共享

随着移动通信网络工作频段不断向毫米波、太赫兹、可见光等高频段演进,新一代无线网络的小区覆盖半径将越来越小,网络建设成本也将大幅攀升,网络建设成本对于全球范围内的几个大型电信运营商而言,已经成为独难承受的重担,而对于众多小型电信运营商而言,未来独立建设运维一张完整的新一代无线通信网络已经成为不可能完成的任务。因此,运营商之间无线网络共建,共同分担不同地域的新一代无线网络建设运维成本;运营商与垂直行业基础设施共享,共建面向用户需求的边缘基础设施,既解决垂直行业用户运维难题,提升垂直行业云化基础设施利用率,又能改善垂直行业用户网络服务质量;运营商与个人/家庭用户设备共享,实现个人/家庭设备的低成本自主共享,都将成为新一代无线网络建设的重要趋势,不仅可以显著降低新一代无线网络建设、运营、维护成本,而且可以实现设备利旧与重复利用。

在网络共建,设备共享的新一代无线网络建设运维的过程中,公平、公开、可信地追溯网络及设备运用状态、工作效率和成本开销等数据,是维护多方网络共建良性可持续发展的基础。

建立包含多个运营商、垂直行业、个人/家庭用户的多方参与、多级维护的区块链网络,能够为新一代无线网络提供从建设阶段到运营阶段、从使用阶段到维护阶段的全周期的网络及设备状态数据,为参与网络共建的多方提供面向机器的网络信任。

3.2 天地融合

随着移动互联业务对大带宽、广覆盖需求的进一步提高,6G 无线网络除了向毫米波、太赫兹等更高频段的频谱搬移,还将向天地一体立体化组网架构等领域演进发展[14]。依据 ITU 频率划分规定,传统的卫星通信频段包括 C 波段(4~8 GHz)、X 波段(8~12 GHz)、Ku 波段(12~

18 GHz)、Ka 波段(18~27 GHz),与 5G、毫米波频段位于相同的区间。虽然卫星网络与新一代地面无线网络在工作频段上有很大的重叠区,但是在空间域存在一定的隔离度,因此,频域隔离对新一代天地一体无线网络而言并不是最理想的解决方案,动态频率共享将是新一代天地一体无线网络融合发展的重要趋势。同样,如何保证天地一体融合网络频率动态可信共享是未来网络亟待解决的问题。另外,新一代立体化无线网络架构中,天地一体融合网络不是地面网络与卫星网络两个网络域的松耦合互联,而将支持网络功能的弹性重构与灵活迁移,因此,如何保证天地资源可信动态共享亦是支撑天地一体融合网络可持续良性发展的基础。

3.3 超大规模连接物联网

随着物联网应用日益推广,无线网络连接密度成为衡量网络能力的关键指标之一[15]。目前,基于对新一代无线网络应用场景、业务需求的分析,业界认为新一代无线网络在物联网领域除了现有的工业互联网、智慧城市、车联网等典型业务之外,还将支持立体化泛在接入、满足视听触嗅闻的感知互联、数字孪生等新生应用需求,连接密度也将比 5G 网络提升一个数量级,即约 $10^7/km^2$。面对种类繁多、制式各异、数量庞大、安全基础薄弱的新一代无线网络物联网应用,亟需基于具有分布式特性的区块链技术体系,建立面向网络的安全信任体系,将安全可信能力由终端迁移至网络侧,降低物联网终端的能源、体积、成本等消耗,实现超大规模异构物联网设备立体泛在可信接入,使物联网具备免疫能力,不仅能被动抵御恶意攻击,还能主动对抗各种安全风险,在不牺牲终端设备性能的前提下,确保新一代无线网络物联网应用的安全与隐私保护。

4 结论

本文网络安全是面向网络攻防对抗行为,基于“有罪假设”的技术体系,而网络可信是面向网络自身,基于“无罪假设”的技术体系。网络安全技术是实现网络可信的前提条件,但建立面向网络的可信体系是解决网络可信的核心。在工作频谱更高、网络建设运维成本更大、参与方更多、网络架构更弹性立体灵活多变、网络资源更分散云化的下一代移动通信网络中,在多方共建共享、天地一体融合互联、超大规模物联网等典型场景中,都存在对参与网络建设、运营、维护、使用的多方提供面向网络的可信能力的需求。

参考文献

[1] YOU X H, WANG C X, HUANG J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts[J]. Science China, Information Sciences, 2020, 64(1): 1-76.
[2] RAJATHEVA N, ATZENI I, BJORNSON E, et al. Whiter paper on broadband connectivity in 6G[R]. 2020.
[3] FARSI M, DANESHKHAH A, HOSSEINIAN F A, et al. Digital twin technologies and smart cities[M]. Springer, 2020.
[4] SAAD W, BENNIS M, CHEN M. A vision of 6G wireless systems: applications, trends, technologies, and open research problems[J]. IEEE Network, 2019, 2: 10265v2.
[5] ZHANG Z Q, XIAO Y, MA Z, et al. 6G wireless networks: vision, requirements, architecture, and key technologies[J]. IEEE Vehicular Technology Magazine, 2019, 14(3): 28-41.
[6] YOAMTTOLA M, KANTOLA R, GURTOV, et al. 6G whiter paper: research challenges for trust, security and privacy[R]. 2020.
[7] DANG S, AMIN O, SHIHADA B, et al. What should 6G be? [J]. Nature Electronics, 2020, 3(1): 20-29.
[8] MOURAD A, YANG R, LEHNE P H, et al. A baseline roadmap for advanced wireless research beyond 5G[J]. Electronics, 2020, 9(2): 351-355.
[9] LETAIEF K B, CHEN W, SHI Y, et al. The roadmap to 6G: AI-empowered wireless networks[J]. IEEE Communications Magazine, 2019, 57(8): 84-90.
[10] 3GPP TS 33.501 v16.1.0. 5G security specifications RL16[S]. 2019.
[11] AHMAD I, SHAHABUDDIN S, KUMAR T, et al. Security for 5G and beyond[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3682-3722.
[12] ITU-T, Y.3052. Overview of trust provisioning in information and communication technology infrastructures and services[S]. 2017.
[13] ITU-T, Y.3053. Framework of trustworthy networking with trust-centric network domains[S]. 2018.
[14] LIU J, SHI Y, FADLULLAH Z, et al. Space-air-ground integrated network: a survey[J]. IEEE Communications Surveys & Tutorials, 2018, 20(4): 2714-2741.
[15] XIAO Y, KRUNZ M, Shu T. Multi-operator network sharing for Massive IoT[J]. IEEE Communication Magazine, 2019, 57(4): 96-101.

(收稿日期:2021-02-02)

作者简介:

刘秋妍(1984-),女,博士,高级工程师,主要研究方向:B5G/6G 无线通信技术。

李铭轩(1980-),男,硕士,高级工程师,主要研究方向:大数据、云计算及业务平台和 IT 支撑系统开发。

吕轩(1983-),男,硕士,高级工程师,主要研究方向:无线通信解决方案与新业务创新应用。

版权声明