数字城市安全测评研究

Study on Security Assessment of Digital City

宋　畅[1]，夏俊杰[1]，邓成明[1]，刘　晓[2]（1. 中国联通智能城市研究院，北京 100048；2. 北京通和实益电信科学技术研究所有限公司，北京 100191）

Song Chang[1], Xia Junjie[1], Deng Chengming[1], Liu Xiao[2]（1. China Unicom Smart City Research Institute, Beijing 100048, China; 2. Beijing Tongheshiyi Telecommunication Science&Technology Research Institute Co., Ltd., Beijing 100191, China）

摘　要：

随着数字城市的发展，物联网、大数据、边缘计算等多技术融合应用于数字城市带来新的安全问题，为应对多技术融合带来的潜在、未知的安全风险，实现数字城市安全测评能力互通，亟需构建跨领域、跨专业、技术融合的安全测评体系。城市级安全测评体系以“安全共生基座先行到位，根据基座规划安全测评平台，依托平台提供安全测评服务”原则为指引，构建城市级“安全基座+平台+服务”的安全测评体系。城市级安全测评体系的提出有效解决多技术融合带来的安全问题，实现数字城市全域测评、数据协同、报告协同、通报协同、能力协同。

关键词：

城市级安全测评体系；数字城市；安全共生系统；安全测评；IPDR

doi：10.12045/j.issn.1007-3043.2022.05.003

文章编号：1007-3043（2022）05-0010-06

中图分类号：TN919

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

With the development of digital city, the integration of Internet of things, big data, edge computing and other technologies in digital city brings new security problems. In order to deal with the potential and unknown security risks brought by multi technology integration and realize the interoperability of security evaluation capabilities of digital cities, a cross domain, cross professional and technology integrated security evaluation system is urgently needed. The city-level security evaluation system adopts the form of "the foundation is in place first, design the security assessment platform according to the foundation, relying on the platform to provide security assessment services", so as to build a city-level security evaluation system of "Foundation + Platform + Service". The proposal of city-level security evaluation system effectively solves the security problems caused by multi technology integration, and realizes the global evaluation, data collaboration, report collaboration, notification collaboration and capability collaboration of digital cities.

Keywords：

City-level security assessment system; Digital city; Secure symbiotic system; Security assessment; IPDR

引用格式：宋畅，夏俊杰，邓成明，等. 数字城市安全测评研究[J]. 邮电设计技术，2022(5)：10-15.

1 概述

1.1 背景

近年来，我国高度重视网络安全测评能力的建设，国家层面出台系列法律法规、政策文件，指导网络安全测评能力建设发展。2017年6月1日施行的《中华人民共和国网络安全法》指出“网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供；关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估”。2021年9月1日施行的《中华人民共和国数据安全法》指出“国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动”。2020年8月，工信部发布《互联网新技术新业务安全评估指南》[1]，对互联网新技术新业务安全评估的工作要求、组织流程、评估内容和方法进行了规范。2021年7月，工信部等十部门发布的《5G应用“扬帆”行动计划（2021—2023年）》[2]指出：

收稿日期：2022-03-07

“加强5G应用安全风险评估，构建5G应用全生命周期安全管理机制，指导企业将5G应用安全风险评估机制纳入5G应用研发推广工作流程，同步规划建设运行安全管理和技术措施，并与5G应用同步实施”。

各监管机构和主管部门积极响应国家政策，从工作要求、组织流程、评估内容和方法等各方面为安全测评提供保障和支撑。

1.2 国内安全测评现状

国家层面，重点针对计算机信息系统、网络关键设备和网络安全专用产品、新闻信息服务、APP等开展安全测评工作。计算机信息系统安全测评方面，自1994年《中华人民共和国计算机信息系统安全保护条例》（国务院令147号）发布，国家要求计算机信息系统实行安全等级保护工作。网络关键设备和网络安全专用产品安全测评方面，根据《中华人民共和国网络安全法》要求，国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全测评结果互认。2018年6月国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室四部门发布首批承担网络关键设备和网络安全专用产品安全认证和安全测评任务的机构名录[3]。新闻信息服务安全测评方面，国家网信办于2017年10月发布《互联网新闻信息服务新技术新应用安全评估管理规定》[4]，规范开展互联网新闻信息服务新技术新应用安全评估工作。APP安全测评方面，2019年1月，中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展APP违法违规收集使用个人信息专项治理的公告》，全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会成立APP违法违规收集使用个人信息专项治理工作组[5]。同年3月，国家市场监管总局、中央网信办联合发布《关于开展APP安全认证工作的公告》[6]，标志着APP认证工作正式启动。

行业层面，工业和信息化部重点开展网络安全、信息安全、数据安全3个方面安全测评工作，并将安全测评工作纳入行业主管部门考核，要求各企业常态化开展。网络安全测评方面，根据《通信网络安全防护管理办法》（工业和信息化部令第11号），要求境内通信网络运行单位开展通信网络安全防护工作。信息安全方面，2016年行业标准《互联网新技术新业务安全评估指南》发布，指导各企业开展新技术新业务安全评估工作。此后，中国互联网协会于2019年发布《互联网新技术新业务安全评估第三方服务自律公约》，推动行业自律工作的落地。数据安全方面，2019年工信部发布《电信和互联网行业提升网络数据安全保护能力专项行动方案》，明确开展数据安全合规性评估工作，并于2021年开展基础电信企业行业数据安全标准贯标工作，进一步推进企业数据安全合规能力建设。

当前，安全测评工作以国家、行业政策要求为背景推动，各项安全测评工作独立开展，不同安全测评工作中，测评对象、测评内容可能存在交叉和重复，且由于各项工作主管部门职责划分，安全测评工作相对分散。

2 城市级安全测评体系建设意义

数字城市涉及政府部门、基础设施、通信产业、IT产业等多个领域，同时充分运用物联网、互联网、5G通信、云/超计算、边缘计算、区块链、大数据、人工智能、IPv6等新一代ICT技术，行业和领域的多样性和交错性，使得安全与多个行业、领域相融合，安全问题更加复杂，现有单一的、分散型的安全测试不足以应对多技术融合带来的潜在、未知的安全风险[7]。因此，需要建立城市级的全域、全时、全局、全程、全要素的统一安全测评与处置平台，与城市安全基座、应急处置、情报数据、态势感知等进行联动，方可实现“一盘棋”的城市级安全测评体系。

城市级安全测评体系可为城市级公共服务、通信、金融、电力、能源、交通等部门、行业提供全域的安全测评服务；为政府部门、基础设施、通信产业、IT产业等领域提供全域测评、数据协同、报告协同、通报协同、能力协同；为区块链、车联网、工业互联网等基础设施及应用提供安全测评能力。实现安全测评能力、安全测评数据的互通，能够应对多技术融合带来的潜在、未知的安全风险，为城市级安全提供保障。

城市级安全测评能力建设，能够通过安全测评能力统筹规划，规避传统安全测评对象和测评内容的交叉、重复性问题。此外，搭建基于主动风险识别和风险动态预警的安全测评能力平台，可实现跨行业、跨领域、全域覆盖的安全测评能力，打造可信安全共生生态环境，促进共生安全能力提升。

3 城市级安全测评体系架构

3.1 总体思路

基于数字城市技术架构，构建“基座+平台+服务”的城市级安全测评体系，基座先行到位，根据基座规划安全测评平台，依托平台提供安全测评服务（见图1）。

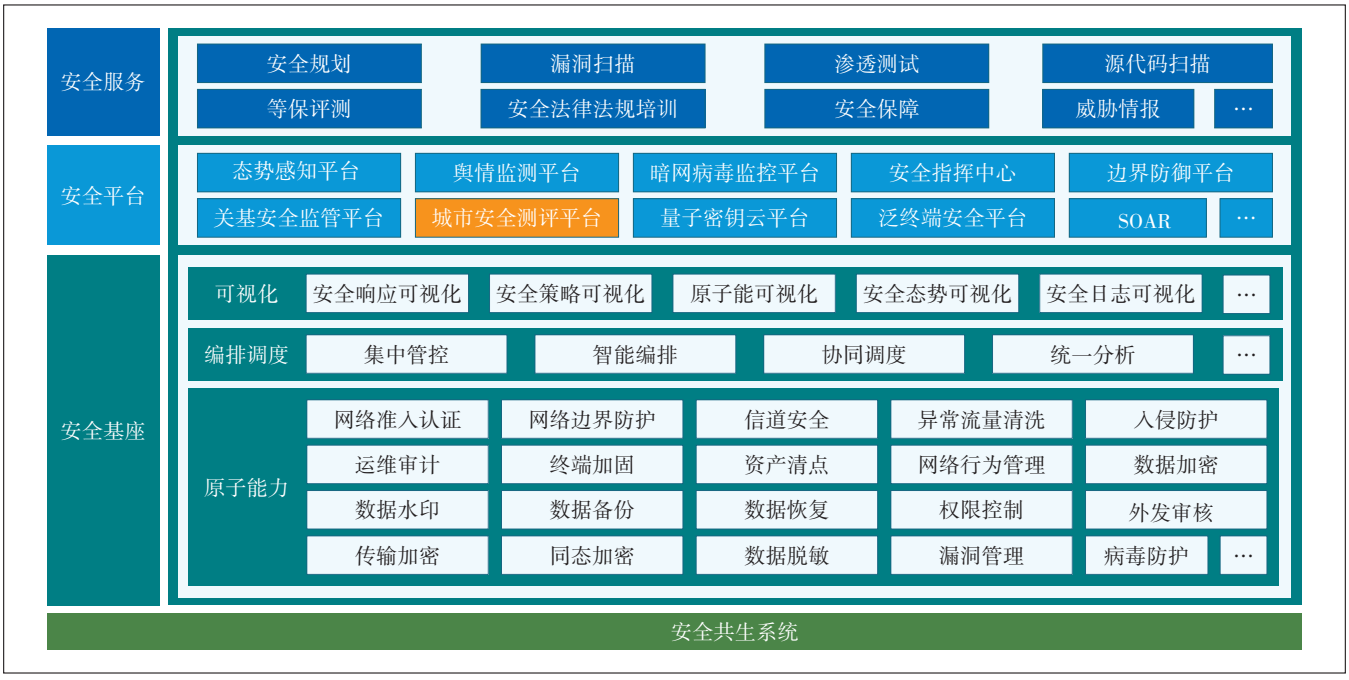

图1　城市级安全共生系统架构

a）基座：以共生理论[8]为基础，打造城市级安全共生系统。城市级安全共生系统作为汇聚安全数据、智能化分析、连接各类安全设备的网络与信息安全一体化交互中心，为数字城市建设输出原子化安全能力。

b）平台：基于共生系统安全能力，建设城市级安全测评平台。城市级安全测评平台与城市级安全共生系统相连接，汇聚城市的系统安全测评数据，作为感知城市的网络空间安全态势关键参数，全方位、自动感知智能城市的安全测评状态，实现城市级安全测评能力，提供城市级安全风险监测和安全态势展示。

c）服务：依托城市级安全测评平台，提供城市级全域覆盖、按需可定制的安全测评能力与服务。结合城市级安全测评跨行业、跨领域特性，以及安全测评需求分散化特点，借助城市级安全测评平台功能模块低耦合方式，提供按需定制的安全测评能力与服务。

3.2 设计原则

城市级安全测评体系设计遵循城市级、兼容性、可扩展性三大原则。

a）城市级。依托数字城市建设城市级安全测评体系，提供城市级全域覆盖、协同联动、按需定制的安全测评能力与服务。

b）兼容性。城市级安全测评体系具备极高兼容性，提供通用接口及多方能力集成。一方面，实现体系内必要工具、能力的对接，提高安全测评与分析能力集成度与重用度，完善城市安全测评体系；另一方面，可实现城市全域系统对接，为其提供网络与信息安全实时监测、风险分析、态势预警等能力。

c）可扩展性。城市级安全测评体系中各能力模块间采用低耦合方式，实现体系高扩展性，便于安全测评数据、安全测评能力、安全管理机制等内容的扩增及管理，满足按需的安全测评需求。

3.3 体系架构

“基座+平台+服务”的城市级安全测评体系架构如图2所示。

a）安全共生基座。基座是指城市级原子化安全能力库，提供终端安全、网络安全、数据安全、应用安全、基础设施安全等多项原子安全能力，并将原子能力的安全策略配置、日志传输等接口标准化，使其具备协同调度和统一分析基础。

b）城市级安全测评平台。城市级安全测评平台划分为能力支撑层、核心功能层和展示层。

（a）能力支撑层。能力支撑层集成各类数据处理、分析模型和功能引擎，向上提供数据分析与处理能力。针对设备安全测评模块，提供数据模型、状态

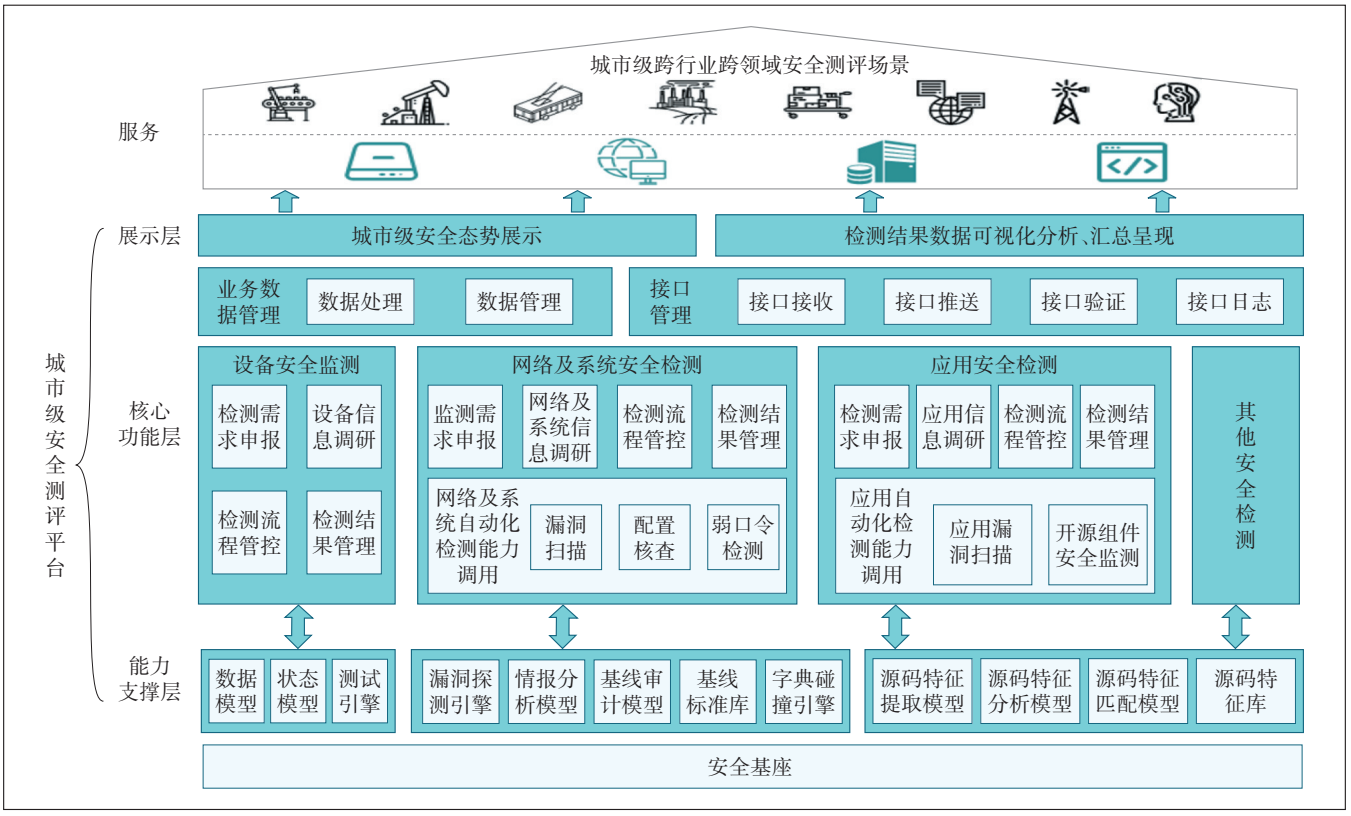

图2　城市级安全测评体系架构

模型和测试引擎集成；针对网络与系统安全测评模块，提供漏洞探测引擎、情报分析模型、基线审计模型、基线标准库和字典碰撞引擎集成；针对应用安全测评，提供源码特征提取模型、源码特征分析模型、源码特征匹配模型和源码特征库集成。

（b）核心功能层。核心功能层主要包括安全测评、业务数据处理、接口管理三大功能模块。安全测评功能模块，结合不同测评场景划分为设备安全测评、网络与系统安全测评、应用安全测评等，主要提供各场景安全测评能力及安全测评全流程管控。业务数据处理模块，一是实现各安全测评场景数据的聚合分析，二是实现城市级安全测评平台与其他系统间交互数据的分析处理，实现系统间数据联动。接口管理模块，主要实现与其他系统、工具间接口，以及对外服务能力调用接口的配置与安全管理。

（c）展示层。展示层主要提供测评结果数据可视化分析与汇总呈现，以及城市级安全态势展示。

c）城市级安全测评能力与服务。基于数字城市全域链接基础，以及城市级安全测评平台多场景测评功能集成和对外通用接口，面向城市不同行业、领域提供基于设备、网络、系统、应用等场景的安全测评能力调用与服务输出。

3.4 运营流程

基于城市级安全测评体系架构，建立IPDR的安全运营模式。

a）识别（Identify）。将风险识别作为安全运营基础，将体系中各场景安全测评作为风险识别手段。

b）防护（Protect）。将安全防护作为安全运营核心，基于风险识别结果，提出管理、技术方面安全防护建议，促进城市级安全防护能力建设。

c）测评（Detect）。将安全测评作为持续安全运营的关键，通过实时安全测评和安全威胁预警分析，生成城市级安全风险态势，提供数字城市全域安全感知和安全预警。

d）响应（Response）。将安全响应作为安全运营闭环保障，面向城市政府、企事业单位、行业用户提供网络与信息安全事件决策与应对处置支撑服务，形成闭环管理。

4 城市级安全测评典型场景

4.1 城市级安全测评场景需求分析

结合现有数据统计，2020年全球失陷主机约有

6 431 498台,国内约有880 607台,约为全球的1/8左右,云服务、VPN、移动设备、IOT设备等仍是攻击者的主要攻击对象[9]。2021年我国国家信息安全漏洞共享平台(CNVD)收录通用型安全漏洞13 083个,同比增长18.2%,按影响对象分类统计,排名前3的是应用程序漏洞、Web应用漏洞、操作系统漏洞。2021年上半年,CNVD验证和处置涉及政府机构、重要信息系统等网络安全漏洞事件近1.8万起。根据CNCERT监测发现,境内大量暴露在互联网的工业控制设备和系统存在高危漏洞的系统涉及煤炭、石油、电力、城市轨道交通、机械等重点行业,覆盖企业生产管理、企业经营管理、政府监管、工业云平台等[10]。根据CNCERT监测数据,2021年第3季度,CNVD共收录联网智能设备漏洞2 792个,覆盖通用型漏洞1 413个和事件型漏洞1 379个,监测到联网智能设备恶意程序样本579.29万个,发现恶意程序传播源IP地址40.18万个,境内僵尸网络受控端IP地址4 309.39万个。

基于以上安全测评、监测成果统计,提出设备安全测评、网络及系统安全测评、应用安全测评3类典型城市级安全测评场景。

4.2 城市级安全测评场景

4.2.1 城市级设备安全测评

数字城市中各类智能控制及采集设备、网络连接设备、信息系统支撑设备等作为城市数字化基础,其安全能力是城市级安全保障的基础。

城市级设备安全测评旨在为政府、企事业单位、行业用户提供设备安全采购和城市入网测评能力。城市级设备安全测评重点关注设备是否存在安全漏洞缺陷、安全功能缺失,以及是否符合国家安全合规相关的能力要求。通过城市级设备安全测评,一方面能够确保采购设备具备所需安全能力;另一方面,不会因新设备引入而导致城市网络、系统等产生新的安全风险,确保各类设备安全准入。

城市级安全测评体系中,通过测评平台集成Fuzz测试引擎等能力模块,可自动创建覆盖协议测试空间的测试包序列,从而能够及时挖掘、发现、记录被测设备及应用系统在组装、解析网络协议过程中存在的脆弱性,从而实现对设备所使用的协议健壮性安全进行自动化无人值守测试。针对设备协议安全方面,模糊协议测试功能如图3所示。

4.2.2 城市级网络及系统安全测评

网络及系统作为数字城市全域链接、数字化平面的核心,其安全能力是城市级安全保障的重点。

城市级网络及系统安全测评旨在为城市管理者提供网络及系统安全风险识别能力,并基于风险研判结果,提供网络及系统安全能力提升与加固指导。城市级网络及系统安全测评通过对网络及系统中各类资产识别、威胁分析和脆弱性分析,分析网络及系统从细节到整体的安全风险情况,覆盖网络及系统安全管理薄弱环节和技术缺陷各方面,提出针对性整改建议,从而提升网络及系统风险防护能力,降低安全隐患发生的可能性和安全事件造成的损失。通过城市级网络及系统安全测评,一方面能够为城市网络及系统安全验收提供支撑,确保新建网络及系统达到所需安全防护能力水平;另一方面,能够提供网络及系统动态、可持续的风险监测和预警能力。

城市级安全测评体系中,通过测评平台集成漏洞探测引擎、情报分析引擎等能力模块,提供全局资产细粒度自动化扫描分析和整体安全风险管理能力。此外,通过安全隐患一键通报、修复指导、快速复核可实现城市网络及系统的安全隐患闭环管理。针对网络及系统资产脆弱性分析方面,城市级安全测评体系具备漏洞扫描功能和配置核查功能。

4.2.3 城市级应用安全测评能力

应用作为数字城市中重要的人机交互节点,在提供数字空间便捷交互功能的同时,也增加了城市安全风险暴露面,其安全能力缺陷容易成为城市安全防护的短板。

城市级应用安全测评旨在为城市管理者、应用开发者、应用运营者提供应用安全风险识别能力和加固指导。城市级应用安全测评重点关注应用安全漏洞、开源代码使用、应用数据处理不合规等方面的安全隐患。通过城市级应用安全测评,一方面能够提供应用上线安全风险管控,确保新上线应用不存在安全风险隐患;另一方面,能够提供应用动态、可持续的风险监测、预警能力,降低应用运营过程中安全风险的发生。

城市级安全测评体系中,通过测评平台集成源码特征提取模型、源码特征分析模型等能力模块,提供应用安全漏洞识别,以及开源代码可能存在的传染性、兼容性等开源合规风险识别,通过与权威安全漏洞库披露信息实时匹配,可获取最新应用安全漏洞信息并进行实时预警,为城市应用安全加固提供解决方案。针对应用开源代码使用安全方面,城市级安全测评体系具备开源代码安全检测功能。

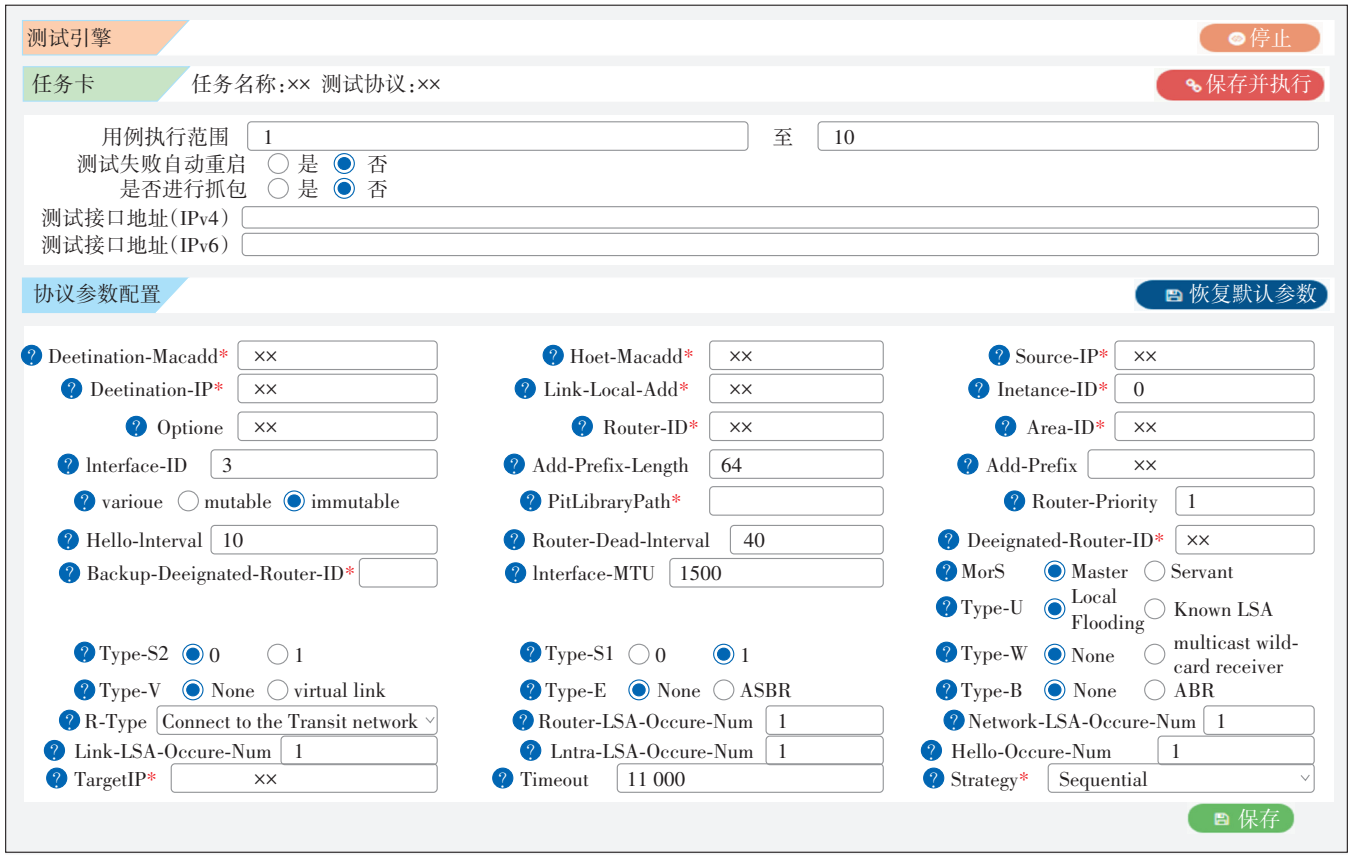

图3　模糊协议测试功能

5 总结

本研究提出一套城市级安全测评体系，依托城市安全共生系统为安全底座能力，构建一套城市级的全域、全时、全局、全程、全要素的统一安全测评、处置平台，面向城市不同行业、领域提供按需定制的安全测评能力调用与服务输出。此外，研究中结合城市安全测评需求和体系架构，提出城市级安全测评体系运营模式和测评典型场景建议，希望为城市级安全测评体系建设者和使用者提供指导和借鉴，协助城市管理者快速构建一个集安全测试、监控预警、响应和分析等于一体的集中化、标准化的持续管理过程，为城市安全筑牢屏障。

参考文献：

[1] 中华人民共和国工业和信息化部. 互联网新技术新业务安全评估指南：YD/T 3169-2020[S]. 北京：人民邮电出版社，2020.
[2] 佚名.《5G应用“扬帆”行动计划（2021—2023年）》印发[J]. 河南科技，2021，40(21)：1.
[3] 佚名. 首批承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录公布[J]. 自动化博览，2018，35(7)：4.
[4] 佚名. 网信办公布《互联网新闻信息服务新技术新应用安全评估管理规定》[J]. 传媒，2017(21)：6.
[5] 佚名. 公安部等四部门 专项治理App违法违规收集使用个人信息[J]. 中国防伪报道，2019(2)：38.
[6] 佚名. 中央网信办、国家网信办会同国家市场监管总局联合开展App安全认证工作[J]. 中国信息安全，2019(4)：22.
[7] 数字孪生供应链白皮书[R/OL]. [2022-03-15]. https://max.book118.com/html/2022/0131/6231241023004114.shtm.
[8] 潘垚辰. 基于共生理论的城市更新研究[J]. 智能建筑与智慧城市，2021(9)：38-39.
[9] 2020年网络安全威胁信息研究报告（2021年）[R/OL]. [2022-03-15]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202112/t20211203_393541.htm.
[10] 2021年上半年我国互联网网络安全监测数据分析报告[R/OL]. [2022-03-17]. https://www.cert.org.cn/publish/main/upload/File/first-half%20%20year%20cyberseurity%20report%202021.pdf.

作者简介：
宋畅，工程师，主要从事网络与信息安全研究工作；夏俊杰，中国联通智能城市研究院副院长，教授级高级工程师，主要研究方向包括移动通信网安全、信息安全、应用安全等；邓成明，高级工程师，主要从事数字经济、智慧城市及新技术、新业务的研究与市场拓展工作；刘晓，工程师，主要从事网络与信息安全研究工作。