基于二维结构熵的 CBTC 系统信息安全风险评估方法

董慧宇 [1] 唐 涛 [2] 王洪伟 [3]

摘 要 随着计算机技术、通信技术和控制技术在城市轨道交通列车运行控制系统中的应用, 城市轨道交通的自动化和信息化程度不断提升. 然而, 基于通信的列车运行控制 (Communication-based train control, CBTC) 技术采用的通用计算机设备和通信技术带来的信息安全漏洞, 给 CBTC 系统带来了日益严峻的信息安全风险, 因此, 对 CBTC 系统的信息安全风险进行量化、动态评估具有重要意义. 本文根据设备及通信链路的差异性构建了 CBTC 网络拓扑模型, 结合信息安全风险下线路列车运行性能变化导致的运能损失, 采用综合表征信息域和物理域特征的二维结构信息熵对 CBTC 系统信息安全风险进行建模分析. 最后, 基于城市轨道交通列控系统半实物仿真平台对评估方法进行验证, 表明所提方法对 CBTC 系统信息安全量化评估的有效性和准确性.

关键词 基于通信的列车运行控制, 信息安全风险评估, 结构信息熵, 列车运行性能, 半实物仿真平台

引用格式 董慧宇, 唐涛, 王洪伟. 基于二维结构熵的 CBTC 系统信息安全风险评估方法. 自动化学报, 2019, **45**(1): 153−162

DOI 10.16383/j.aas.c180374

A 2D Structure Entropy-based Approach to Security Assessment of Communication-based Train Control System

DONG Hui-Yu[1] TANG Tao[2] WANG Hong-Wei[3]

Abstract With the wide application of computer, communication and control technologies in train operation control system, the degree of automation and informatization of urban rail transit is continuously improved. However, universal computer equipment and communication technologies adopted by the method of CBTC (communication-based train control) bring serious security risks to the CBTC system. In view of this, it is of great significance to quantify and dynamically evaluate the information security risks of CBTC system. In this paper, a topology model of CBTC networks is built according to the characteristics of equipment and communication links. Combining the capacity loss from performance changes of train control under security risks, the 2D structural information entropy is constructed, which can comprehensively characterize the cyber space and physical space features, to model and evaluate the information security risks of CBTC system. Finally, with a hardware-in-the-loop simulation platform for urban rail transit CBTC security, the effectiveness and accuracy of the proposed approach are verified.

Key words Communication-based train control (CBTC), security risks assessment, structural information entropy, train operation performance, hardware-in-the-loop simulation platform

Citation Dong Hui-Yu, Tang Tao, Wang Hong-Wei. A 2D structure entropy-based approach to security assessment of communication-based train control system. *Acta Automatica Sinica*, 2019, **45**(1): 153−162

城市轨道交通具有安全、准时、快速、运量大等优点, 在解决城市拥堵、促进城市及其交通可持续发展方面发挥着重要作用[1]. 基于通信的列车运行控制 (Communication-based train control, CBTC) 是城市轨道交通信号系统的关键技术, 该技术使用无线通信实现列车与地面设备的实时、双向、连续信息交互, 控制列车的运行速度和方向, 在确保安全的前提下提高城市轨道交通的运行效率[2]. 为提升城市轨道交通的自动化和信息化水平, 通信、控制、计算机等信息技术在 CBTC 系统中得到了广泛应用. 与此同时, 来自系统外部或内部的信息攻击的威胁加大, 系统面临的挑战日益严峻[3], 信息安全事件频发. 2012 年 3 月, 上海申通地铁车站信息发布系统和运行调度系统的无线网络受到攻击; 2012 年 7 月, 深圳地铁受乘客随身 MIFI (Mobile WIFI) 干扰

收稿日期 2018-05-31 录用日期 2018-09-03
Manuscript received May 31, 2018; accepted September 3, 2018
北京市自然科学基金 (L161006, 4164094), 国家自然科学基金 (61603031, 61790575, 61790573), 国家重点实验室项目 (RCS2018K008, RCS2017ZZ003) 资助
Supported by Beijing Natural Science Foundation (L161006, 4164094), National Natural Science Foundation of China (61603031, 61790575, 61790573), and State Key Laboratory (RCS2018K008, RCS2017ZZ003)
本文责任编委 吕宜生
Recommended by Associate Editor LV Yi-Sheng
1. 北京交通大学电子信息工程学院 北京 100044 2. 轨道交通控制与安全国家重点实验室 北京 100044 3. 国家轨道交通安全评估研究中心 北京 100044
1. School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044 2. State Key Laboratory of Rail Traffic Control and Safety, Beijing 100044 3. National Research Center of Railway Safety Assessment, Beijing 100044

的影响导致车地通信中断, 致使多列列车紧急制动等. 这些事件均造成了不好的社会影响, 有的严重影响了城市轨道交通的行车秩序. CBTC 系统的信息安全已成为轨道交通领域的重要研究内容, 评估列控系统网络安全性、提高 CBTC 系统信息安全防护能力成为轨道交通事业健康、快速发展的关键[4].

然而, 国内外对轨道交通领域的信息安全研究处于起步阶段, 相关研究停留在列控系统信息安全存在的隐患及挑战等分析层面, 针对 CBTC 系统的信息安全评估方法匮乏. 文献 [5] 对欧洲铁路运输 (European railway traffic management system, ERTMS) 规范中的潜在漏洞进行分析, 并综合威胁来源、攻击能力以及影响等级几个方面定性地评估了英国实施的 ERTMS 的网络安全风险. 文献 [6] 采用基于贝叶斯攻击图的方法, 分析了列控系统最易发生的信息安全事件及系统的风险等级. 文献 [7] 分析了用于控制道岔转换、改变行车信号的先进列车控制系统 (Advanced train control systems, ATCS) 协议的脆弱性. 文献 [8−9] 分别从入侵检测和攻击防御的角度对列控系统信息安全进行研究.

鉴于 CBTC 系统与其他工业控制系统 (Industrial control system, ICS) 均属于典型的信息物理系统 (Cyber physical system, CPS)[10], 例如智能电网[11]、水利[12]、核能[13] 等, 加之这些领域对信息安全的研究相对成熟, 因此, CBTC 系统信息安全研究可参考 ICS 相关的研究方法及成果.

常见的信息安全评估方法有贝叶斯网络、攻击树、Petri 网、博弈论等. 贝叶斯网络[14−15] 是一种将定性分析转化为定量分析的概率网络, 文献 [16] 提出了一种基于贝叶斯网络的网络安全模型, 从管理和技术方面综合评估了核基础设施的安全性. 考虑到贝叶斯网络具有解决复杂依赖性问题的优势, 文献 [17] 利用贝叶斯网络计算结果作为事件树的输入, 分析网络攻击下核反应堆保护系统的故障率, 从而量化评估其信息安全能力. 该方法克服了常见的概率安全评估方法在工业控制系统信息安全评估中的局限性. 攻击树[18−19] 可以方便直接地显示系统中的资产或设备可能受到的攻击类型, 提供了一种以目标为导向的方法来描述多阶段攻击, 文献 [20] 基于攻击树对节点重新定义, 从各设备、攻击场景及系统的脆弱性的角度对 SCADA (Supervisory control and data acquisition) 系统的安全性进行评估, 但是, 该方法是一种静态的信息安全评估方法, 不能体现系统在网络攻击中状态的变化. Petri 网[21−22] 中的变迁是一个主动元素, 可以表示事件发生、状态改变等动态特性, Bouchti 等 [23] 提出了一种将静态的攻击树模型扩展为有色 Petri 网的方法, 利用有色 Petri 网[24−25] 的灵活性, 分析网络入侵的静态和动态特征. 信息安全攻防之间构成典型的博弈关系, 使用博弈论[26−27] 研究信息安全问题较为广泛, 加之许多信息安全评估方法只关注系统当前的安全状态, 没有考虑未来系统安全状态的变化趋势, 文献 [28] 提出了一种基于马尔科夫博弈理论的新型风险评估模型以衡量网络信息系统的安全性, 并且能自动生成防御方案以提高系统信息安全防护能力.

上述方法均从系统的执行流程出发, 基于功能和性能对信息安全防护能力进行评估. 然而, 信息安全风险总是从计算机网络发起, 然后在工业控制系统中演化, 最终作用于物理系统. 上述方法难以对风险传播过程中的系统性能进行综合刻画. Li 等[29] 提出了首个衡量网络结构信息的方法, 即二维结构熵, 并基于该方法提出了网络阻力的概念, 用以定量描述网络面对病毒传播时的抵抗能力[30], 克服了传统的 Shannon 信息熵无法充分反映网络结构信息的局限性[31].

本文基于二维结构熵提出衡量 CBTC 系统网络结构性能的方法, 再结合物理域列控系统的运行性能, 给出了 CBTC 系统信息安全的定量描述模型, 最后依托 CBTC 信息安全测试床对该方法的准确性和有效性进行验证.

1 CBTC 系统

1.1 CBTC 系统简介

典型的 CBTC 系统如图 1 所示, 核心装备包括列车自动监控 (Automatic train supervision, ATS)、区域控制器 (Zone controller, ZC)、计算机联锁 (Computer interlocking, CI)、车载控制器 (Vehicle on-board controller, VOBC)、数据存储单元 (Data storage unit, DSU) 和数据通信系统 (Data communication system, DCS).

列车运行过程中, VOBC 通过车载移动台 (Mobile station, MS) 不间断地将列车标识、实时位置、速度及运行方向等信息传输给 ZC. ZC 根据接收到的列车信息以及 CI 监测的线路信息实时动态计算后车可到达的最远距离, 即移动授权 (Movement authority, MA), 并发给后车, 后车根据接收到的 MA 计算列车运行曲线并按照该曲线行驶, 在这一过程中, 列车到 ZC 和 ZC 到列车之间的信息交互均通过车地无线通信实现.

1.2 CBTC 系统的信息安全问题

目前已投入运营的 CBTC 系统主要采用基于 IEEE 802.11 协议族的无线局域网作为车地通信的主要制式. 为提升信息化和自动化程度, CBTC 系统采用大量数字化和信息化组件, 包括 Windows 和

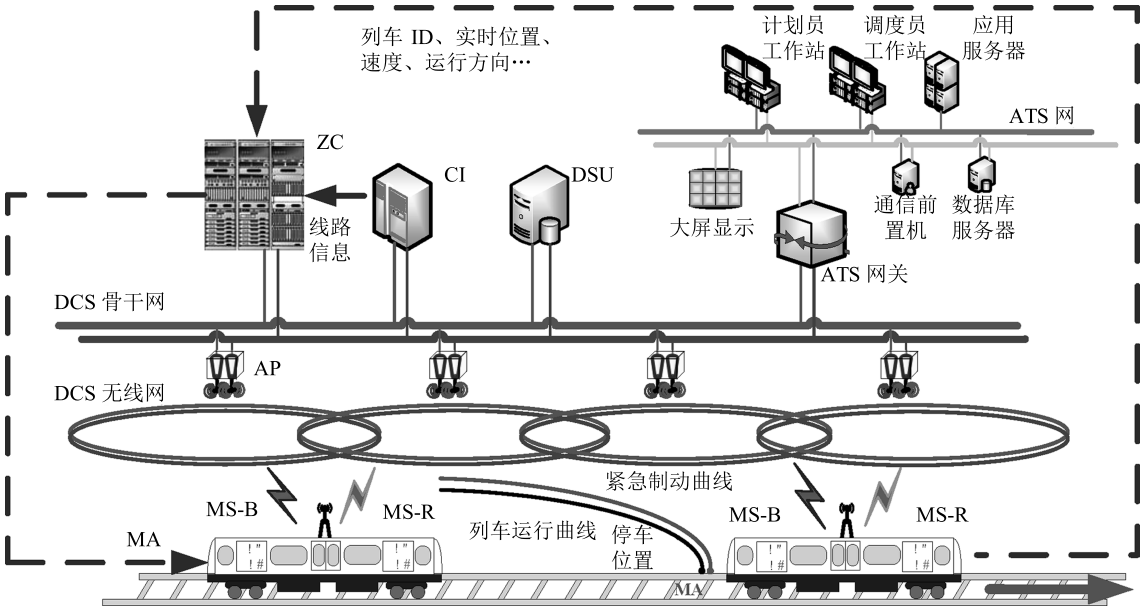


图 1　CBTC 系统结构

Fig. 1　CBTC systems

VxWorks 等操作系统、通用计算机、标准通信协议等. 然而, 随着系统组件漏洞的逐渐披露, CBTC 系统面临着日益严峻的信息安全风险. 一旦系统被恶意入侵, 漏洞被利用, 列车会被迫紧急制动, 降低系统运行效率, 影响正常行车秩序.

CBTC 系统的典型信息安全风险包括: 1) 网络设备的工作机制、配置等信息安全隐患可能被内部及外部威胁利用, 例如常用的防火墙设备的包过滤机制存在缺陷, 可导致防火墙被穿透; 2) 核心、汇聚交换机承载着极高的数据流量, 在突发异常数据或攻击时, 极易造成设备负载过重而宕机; 3) 操作系统漏洞会导致远程代码执行、缓冲区溢出、拒绝服务、信息泄露、未授权访问以及获取权限等, 均可给城市轨道交通的高效运营带来极大隐患; 4) WLAN 工作在 ISM 频段, 易受到干扰, 其认证、加密等关键技术相对陈旧, 车地信息的传输存在被窃听甚至篡改的风险, 对行车效率造成威胁.

实际上, CBTC 系统的安全苛求特征决定系统具有比较完善的安全功能防护措施, 包括故障导向安全机制、容错架构设计、冗余设置、安全协议等. 然而, 功能安全保障措施并非专为信息安全设计, 既有措施对信息安全风险的约束以及信息安全风险造成的影响仍需要精确、全面评估.

2　CBTC 系统信息安全评估方法

信息物理系统中, 信息安全威胁和系统漏洞组合作用于信息域的网络节点或链路, 进而会引起物理域列车运行状态的变化, 从而带来轨道交通运营服务性能的降低. 综合描述物理域和信息域的性能是对 CBTC 系统信息安全风险评估的核心, 本文引入结构信息熵对计算机网络在信息安全风险下的整体性能进行描述和分析, 继而充分考虑物理域列车控制性能, 实现对 CBTC 系统信息安全风险的综合评价.

2.1　二维结构熵

Shannon 提出的熵是关于不确定性的一种度量, 结构信息熵可用来描述复杂系统结构的属性. 网络的结构信息能够较好地定义网络交互、网络通信以及网络演变等网络结构的动态复杂性, 对网络理论的发展至关重要[32]. 因此, 借助于二维结构熵可描述计算机网络在信息安全风险下的状态变化.

2.1.1　二维结构熵的定义

给定一个由 n 个节点和 m 条边组成的连通的加权网络 $G=(V,E)$, V 和 E 分别是网络 G 中所有节点和所有边的集合, 将 V 划分为 L 个模块, 每个模块用 X_j 表示, 则 $P=\{X_1, X_2, \cdots, X_L\}$可看作 G 的划分. 由于 P 的存在, 确定 G 中任意一点 $v \in V$ 都需要确定 v 所在的模块的标识 j 和 v 在相应模块 X_j 中的节点标识 i. 基于划分 P, 给出网络 G 的二维结构熵的定义, 如下:

$$H^2(G)=\sum_{j=1}^{L}\frac{V_j}{vol(G)}\times H\left(\frac{d_1^{(j)}}{V_j},\cdots,\frac{d_{n_j}^{(j)}}{V_j}\right)-$$

$$\sum_{j=1}^{L}\frac{g_j}{vol(G)}\log_2\frac{V_j}{vol(G)}=$$
$$-\sum_{j=1}^{L}\frac{V_j}{vol(G)}\sum_{i=1}^{n_j}\frac{d_i^{(j)}}{V_j}\log_2\frac{d_i^{(j)}}{V_j}-$$
$$\sum_{j=1}^{L}\frac{g_j}{vol(G)}\log_2\frac{V_j}{vol(G)} \tag{1}$$

其中, $d_i^{(j)}$ 表示模块 X_j 中第 i 个节点的度, $vol(G)$ 和 V_j 分别表示网络 G 及模块 X_j 中所有节点的度之和, n_j 表示 X_j 包含的节点数, g_j 表示有且只有一个端点与 X_j 中节点相连的边数.

$H^2(G)$ 是一个二项式, 第 1 项表示在模块 X_j 中确定任意节点 v 所需要的信息量; 第 2 项表示在 G 中, 确定某一模块 X 所需的信息量. 其中, 每个模块可由与其相连的其他模块中的节点访问. 因此, 二维结构熵包含了各个模块内部节点的信息和各模块之间的信息, 反映了系统网络拓扑结构的特性.

2.1.2 CBTC 系统二维结构熵的特点

CBTC 系统的计算机设备和网络设备构成了典型的计算机网络, 设备之间存在复杂的数据交互. 由于城市轨道交通站间距离短, 所以 CBTC 装备分布密度高, 同时系统的冗余和容错设置也使得网络中的设备数量众多. 鉴于安全等级需求和工作模式的不同, 数据交互的承载方式有所不同, 传输协议和传输媒介存在差异.

二维结构熵定义中图的顶点和边均是一致的, 而 CBTC 网络中的节点和通信链路有一定的差异性, 因此对网络拓扑的顶点和边的属性的差异性需要针对性描述. 本文使用加权网络对 CBTC 网络拓扑的顶点和边进行加权处理.

1) 边权重

网络拓扑中的边即为通信链路, CBTC 系统中, 通信链路以有线和无线两种形式呈现. 有线网即为骨干网, 采用数字同步序列、弹性分组网或基于交换技术的环网, 地面设备通过骨干网基于 TCP/IP 通信协议交互数据; 无线是地面设备与车载设备的双向数据传输方式, 主要承载列车和地面控制中心的信息交互. 考虑到数据传输的安全需求不同, 不同通信链路采用不同的应用层传输协议. 典型的 CBTC 系统安全通信协议包括 RSSP-I、RSSP-II 以及私有协议等, 不同协议的安全防护能力不同, 各自的权重值也不同. 类似地, 考虑到通信链路的本质物理属性, 有线网和无线网的抗干扰能力及安全防护能力不同, 各自的权重值也不同.

2) 节点权重

CBTC 系统主要的通信节点有安全计算机、工控机、服务器、网络交换机、网关等, 根据功能定位的不同, 内置的操作系统也不同, 主要有 WindowsXP、Windows7、Windows Server 以及 VxWorks 等. 鉴于设备类型、设备配置及使用的操作系统等的多样性, 每个设备的安全隐患有所不同, 例如使用防火墙及强登录密码的设备的安全性要高于未设置防火墙及身份验证的设备; Windows 操作系统的漏洞一般远多于 VxWorks 系统; 相同操作系统的设备的漏洞数目、严重程度也可能不同等. 因此, 在构建 CBTC 网络拓扑图时, 需要考虑通信节点的安全性差异从而给各个顶点赋权重, 权值的大小取决于设备现有的安全措施、是否存在异常、漏洞情况等.

一般而言, 边的安全性越低, 与其连接的节点被入侵的可能性越高, 但是节点被入侵的可能性还取决于节点自身的特性. 如果节点本身安全性很高, 即便与其相连的边易被入侵, 该节点被攻击成功的可能性也会降低.

CBTC 加权网络与一般的加权网络相比, 除了边被赋予权重, 网络的节点也被赋予不同的权重, 因此, 各节点的度不能仅由边权重之和确定, 应具有其特殊性. 由此, 给出 CBTC 系统在节点度的新定义如下:

$$d_i^j=\sum_{k_i=1}^{E_i^j}we_{k_i}^j\times wn_i^j \tag{2}$$

其中, $we_{k_i}^j$ 表示第 j 个模块中与节点 i 相连的第 k 条边的权重, wn_i^j 表示第 j 个模块中节点 i 的权重, E_i^j 表示第 j 个模块中与节点 i 相连的总边数.

2.2 列车运行性能

二维结构熵衡量的是 CBTC 系统信息域网络拓扑在信息安全风险下的状态变化, 无法体现物理域列车的运营属性, 因此需要在式 (1) 的基础上增加列车运行性能的参数.

列车按计划正常行驶时, 线路的运营能力、列车的运行速度和运行距离等指标在一定范围内随时间规律变化. 基于故障导向安全原则, 为保证安全, 在信息安全风险作用下, 列车运行会导向安全侧, 即列车紧急停车. 为了保障列车运行的连续性和线路运营服务的弹性, 列车停车后会进行降级运行, CBTC 系统的冗余和容错架构设计会使得即使在某些情况下网络的拓扑性能发生改变, 列车运行仍不受影响. 因此在衡量 CBTC 系统的信息安全风险时, 需要综合考虑物理域的列控性能和信息域的网络性能.

以车地通信为例, ZC 与车载设备通过骨干网实现无线双向通信, 由于 ZC 采用 2 × 2 取 2 的架构,

当 ZC 主系故障时会自动切到备系以确保列车仍能收到 MA 并正常运行. 因此, 攻击者攻击 ZC 时, 列车运行状态在短时间内不会受到影响; 随着攻击的深入, ZC 备系也故障时, 列车则触发故障−安全机制, 紧急制动; 在制动过程中, 如果列车满足降级运行, 即通过一个用于定位的应答器时, 列车会重新启动, 由自动驾驶模式转换为点式运行模式. 如图 2 所示, 面临信息安全风险时, 冗余设计使得 CBTC 系统具备一定的抵抗力, 当主备系均被破坏后, 列车性能开始由最佳状态快速下降直至最低点, 在保障功能安全的前提下, 根据运营服务的需求, 列车性能开始缓慢恢复, 最终达到新的稳定状态. 由于网络攻击前后列车驾驶模式发生改变, 因此, 初始的列车运行性能状态优于缓慢恢复后的新的稳定状态.

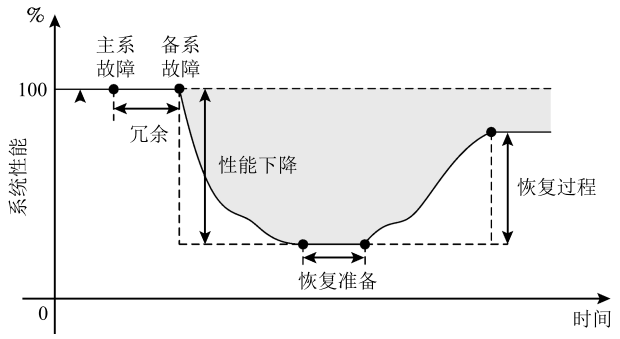


图 2　CBTC 系统故障时的列车性能变化

Fig. 2　Train performance under failures of CBTC

上述过程导致列车的实际运行曲线与计划运行曲线产生较大差异, 图 2 中的阴影部分是信息安全风险下系统性能的损失, 可由列车实际运行速度曲线计算得到.

$$P_{\text{loss}}(t)=\int_{t_0}^{t}(v_p-v_a)\mathrm{d}t \tag{3}$$

其中, $P_{\text{loss}}(t)$ 表示 t 时刻列车运行性能损失, t_0 表示初始时刻, v_p 和 v_a 分别表示列车计划和实际运行速度. 对式 (3) 进行归一化处理可得

$$P(t)=\int_{t_0}^{t}\frac{v_p-v_a}{v_p}\mathrm{d}t=\int_{t_0}^{t}\left(1-\frac{v_a}{v_p}\right)\mathrm{d}t \tag{4}$$

$P(t)$ 范围为 [0, 1], 值越小, 表示攻击对列车当前时刻造成的影响越大.

2.3　CBTC 系统信息安全模型

有效的网络攻击会对 CBTC 系统信息域的网络拓扑性能造成直接影响, 例如利用特定系统漏洞导致设备宕机继而节点从网络中移除, 利用协议漏洞导致设备通信中断继而使相应节点之间的边移除等. 但是 CBTC 系统采取双网冗余、双机热备等架构设计, 确保了列控系统在一定程度上具有抵抗网络攻击的能力, 即随着网络攻击致使系统的网络拓扑结构造发生变化, 但列车仍能在短时间内保持 CBTC 驾驶模式正常运行. 因此, 衡量 CBTC 系统的信息安全状态需要综合信息域网络拓扑性能及物理域列车运行性能, 继而得到衡量 CBTC 系统信息安全的模型.

考虑到网络攻击可能使子系统之间通信中断, 从而导致系统网络拓扑结构由连通状态变为非连通, 因此, 结合前面给出的 CBTC 系统在网络攻击过程中信息域及物理域的动态评估结果, 可得 CBTC 系统信息安全模型.

$$S(t)=H_t^2(G)\times P(t)=\frac{1}{vol(G)}\sum_{k=1}^{N}vol(G_k)H_t^2(G_k)P(t) \tag{5}$$

其中, N 表示当前网络结构中连通子图的个数, $vol(G_k)$ 表示 t 时刻系统网络结构中第 k 个连通子图中所有节点度之和, $H_t^2(G_k)$ 表示 t 时刻该连通子图的二维结构熵; $P(t)$ 表示 t 时刻列车运行情况.

3　CBTC 系统信息安全评估方法验证与分析

本节基于 CBTC 系统信息安全测试床, 利用系统的安全隐患模拟入侵者对其进行网络攻击. 根据信息安全评估模型, 构建 CBTC 系统的网络拓扑, 分析网络边和节点的权重并计算网络拓扑性能的变化, 根据列车运行状态计算列车性能的变化, 综合评估测试床的安全性.

3.1　CBTC 系统信息安全测试床

CBTC 系统信息安全测试床是基于北京地铁 7 号线搭建的列控系统半实物仿真平台, 由部分真实列控设备、仿真软件和真实线路参数组成, 模拟多列车在线路上的追踪.

每个 ZC 子系统包含 4 台使用 VxWorks 系统的处理单元 (Process unit, PU)、2 台通信控制器 (Communication controller, CC) 以及 1 台使用 Windows XP 系统的维护机, 构成 2×2 取 2 的容错架构. 当且仅当主系或备系中的 2 个 PU 处理结果相同时, 才能作为本系的最终结果, 此外, 每一系的 CC 承载着骨干网与 ZC 内网数据转发的功能, 一旦 CC 故障, 相应的骨干网将无法接收来自 ZC 的数据.

CBTC 测试床网络拓扑如图 3 所示. 按功能结构将拓扑图划分为 15 个子系统: 6 个 ZC 子系统, 1

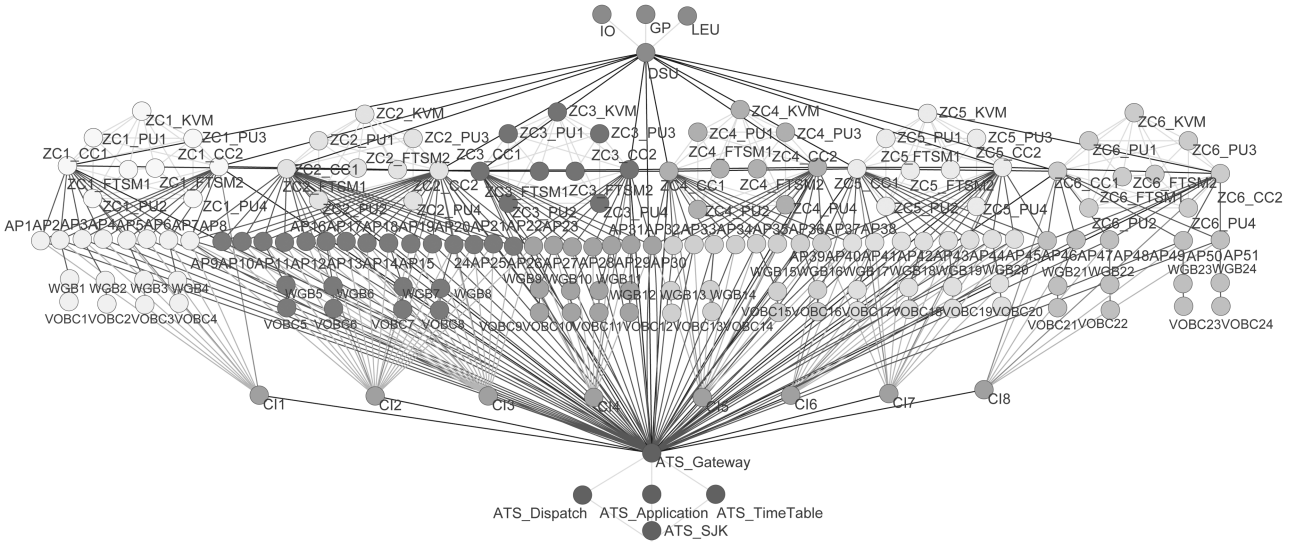


图 3 CBTC 系统测试床网络拓扑图

Fig. 3 The network topology of the CBTC test-bed

个 ATS 子系统, 每个 ZC 覆盖范围内的所有 AP, VOBC 及 MS, 各划分为 1 个子系统, 8 个 CI 设备作为 1 个子系统, 其他设备例如地面电子单元 (Lineside electronic unit, LEU) 和 DSU 等作为 1 个子系统.

3.2 攻击案例

为了验证上述方法的合理性, 本文将 ZC 子系统作为攻击目标进行仿真实验.

ZC 由主备两系组成, 每一系包括 1 台 CC 和 2 台 PU, CC 宕机后会自动重启, 若重启失败, 则整系宕机.

根据 ZC 的工作原理, 模拟以下攻击过程: 如图 4 所示, 首先攻击者通过暴力破解无线网密码侵入 DCS 红网, 通过网络分析获取网段信息, 随后利用 VxWorks 操作系统漏洞对 ZC1 主系的 CC1 发起攻击, 导致 CC1 宕机, 共耗时 20 min; 持续攻击 CC1, 使其重启失败, 则主系两个 PU 同时宕机, ZC1 切换到备系, 共耗时 10 min; 采用同样的方法接入蓝网, 攻击 ZC1 的备系, 直到整个 ZC1 子系统故障. 对 ZC2, ZC3 依次进行上述操作.

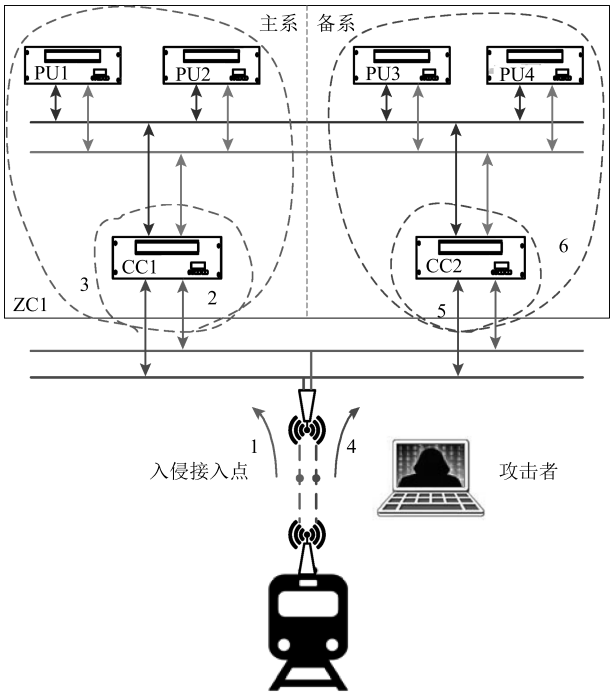


图 4 网络攻击过程

Fig. 4 The process of the network attack

3.3 CBTC 系统信息安全评估结果及分析

3.3.1 网络拓扑性能变化

系统的设备故障反映到网络拓扑中表现为相应的节点从拓扑中移除, 因此, 系统的网络拓扑随着上述攻击过程不断变化.

1) 节点权重

节点的权重使用文献 [33] 中基于攻击树的脆弱性评估的方法, 构建 CBTC 测试床的攻击树模型, 综合每台设备, 即每个节点的安全状态、设备漏洞情况、密码强度以及涉及的通信协议类型 4 个要素计算得到.

$$v(L) = \chi \times \max\{v_\alpha, v_\beta\} \times \mu \tag{6}$$

其中, χ 表示设备当前的安全状态, 由设备满足的网络安全条件 (是否存在异常、是否已采取防护措施、是否设置登录密码等) 个数确定; v_α 表示综合考虑

设备的固有漏洞类型、漏洞严重程度以及漏洞数目的端口审计结果; v_β 表示设备采取的密码策略的强度; μ 从不同通信协议类型可能造成设备安全程度不同的角度, 考虑了通信协议对节点安全的影响.

图 5 为 CBTC 测试床叶脆弱性指数的仿真结果, 即各节点被恶意入侵的可能性大小. 脆弱性指数越大, 相应设备的安全性越低, 节点权重则越小.

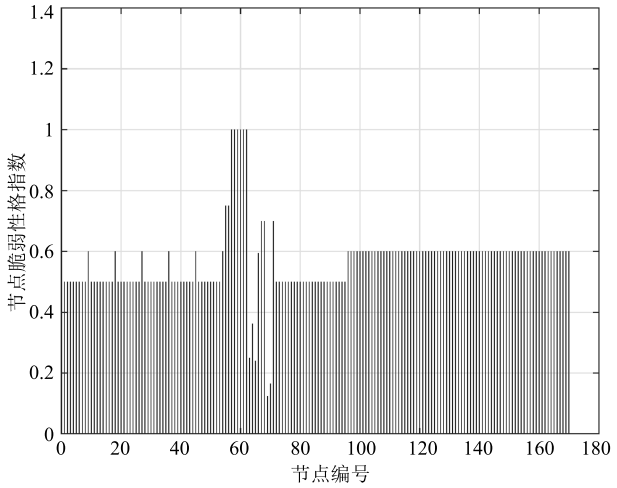


图 5　节点脆弱性指数

Fig. 5　Vulnerability indexes of nodes

2) 边权重

边的权重取决于设备之间的通信方式和通信协议的安全性, 表 1 从数据安全性、数据包被截获的难易程度两个方面对通信方式和通信协议进行量化, 并综合表征了通信链路的权重值.

表 1　通信链路的安全性

Table 1　Security of communication links between equipments

通信方式	通信协议	数据安全性	被截获的难易程度	综合评价	边权重
有线	RSSP-I	2	3	2.3	3
	私有协议	3	3	3	1
	明文	1	4	1.9	5
无线	RSSP-I	2	2	2	4
	私有协议	3	1	2.4	2

CBTC 系统使用的通信协议类型有 RSSP-I、私有协议以及明文, 其中, RSSP-I 是公开的铁路信号安全通信协议, 私有协议由厂家自定, 因此, 从数据安全性角度, 私有协议安全性最高, RSSP-I 次之, 明文最弱.

DCS 使用无线和有线两种通信方式, 其中, WLAN 工作在公开的 ISM 频段, 且认证、加密等关键技术相对陈旧, 易被恶意入侵者破解从而接入网络中, 而对于有线通信方式, 攻击者往往需要接触到相关的网络设备, 通过以太网接口、USB 接口等接入网络, 实施网络攻击的条件相对苛刻, 由此, 攻击者通过无线方式侵入 CBTC 系统较有线方式更容易实现. 另外, 使用不同通信协议的设备在网络中的结构、通信周期不同. 鉴于这些因素, 不同的通信方式下数据被截获的难易程度不同.

3) 二维结构熵

由边和节点的权重使用式 (2) 可得到网络拓扑中每个节点的度, 度越大, 表示攻击者入侵相应节点的难度越大, 系统越安全, 进而根据式 (1) 计算得到 CBTC 系统网络拓扑演变过程中二维结构熵随时间的变化, 结果如图 6 所示.

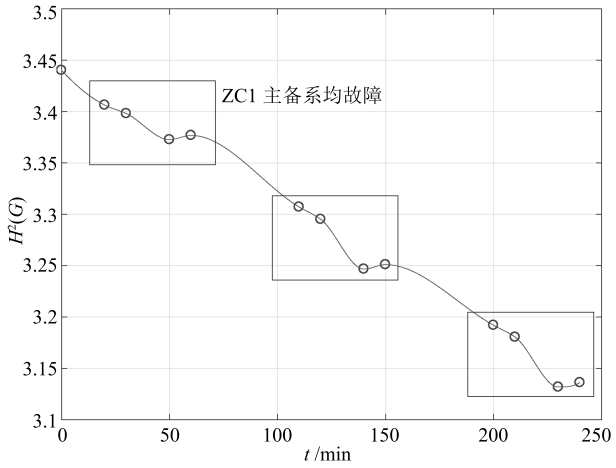


图 6　网络攻击下计算机网络二维结构熵的变化

Fig. 6　Two-dimensional structure entropy of computer network under the cyber attack

系统初始的二维结构熵为 3.4402, 点 A, B, C, D 分别表示 ZC1 的 CC1、主系其余设备、CC2、备系其余设备依次宕机后二维结构熵的计算结果. 其中, 当 ZC 子系统的主系以及备系的 CC2 故障, 即 ZC 成为孤立子系统时, 系统的二维结构熵下降明显, 当 ZC 子系统完全故障, 即相应 ZC 完全从网络拓扑中移除时, 二维结构熵反而增加. 这是由于在网络攻击的影响下, CBTC 系统由连通图演变为多个连通子图的集合, 二维结构熵定义为各连通子图的结构熵的加权平均值, 由于孤立的 ZC 子系统与系统其余部分没有关联, 各连通子图的节点无法通过其外部的节点确定, 因此, 孤立 ZC 的结构熵较小, 并且子系统内部使用明文通信, 设备的安全性也较低, 因此, 系统的结构熵明显下降; 而随着 ZC 完全故障, 整个 ZC 子系统从网络结构中移除, 系统的结构熵不再受 ZC 影响, 因而增大.

从图 6 中二维结构熵的整体变化趋势来看, 随着网络攻击逐渐深入, ZC1、ZC2 和 ZC3 相继故障, 系统的网络拓扑性能整体呈现下降趋势.

3.3.2 列车运行性能变化

图 7 是 ZC 主备两系均故障后其管辖范围内的单列车的速度变化曲线.

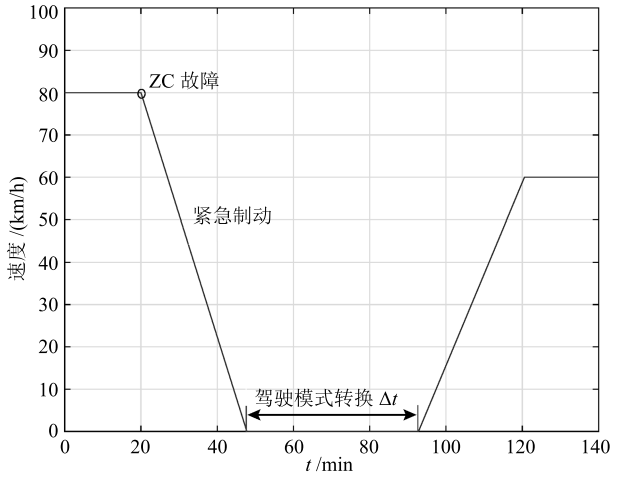


图 7 ZC 故障后的列车运行速度图

Fig. 7 The speed of a train within the range of a failed ZC sub-system

正常情况下, 列车以 80 km/h 的速度运行, 假设在 t_1 时刻, ZC 主备系均故障, 此时, 在该 ZC 范围内的列车将以 0.8 m/s^2 的减速度紧急制动, 随后经过 Δt 时间的降级准备后, 列车重新以 0.6 m/s^2 的加速度以点式模式运行, 直到 t_2 时刻达到最大运行速度 60 km/h. 根据式 (4) 可计算得到列车的性能变化.

正常工作状态下, ZC 覆盖范围内的各列车的运行性能均为 1, 不同 ZC 子系统故障对线路运行能力的影响程度不同, 该影响因子可由每个 ZC 线路覆盖范围的大小确定.

$$\eta = \frac{C_i}{L} \tag{7}$$

其中, C_i 表示第 i 个 ZC 的覆盖范围, L 表示整条线路全长. 因此, 6 个 ZC 的影响因子依次为 0.153, 0.314, 0.137, 0.165, 0.181, 0.050. 综合线路中所有列车的性能变化情况, 得到 CBTC 系统列车性能变化曲线, 如图 8 所示.

比较图 6 和图 8, 当 $t = 30$ min 时, 虽然 ZC1 主系故障, 系统的二维结构熵减小, 但是由于 ZC 的 2 × 2 取 2 架构, 系统切换备系确保车地正常通信, 列车运行性能不受影响, 直到 $t = 60$ min, ZC1 备系也故障后, 列车性能开始下降, 又因为系统具有故障安全机制, 故障 ZC 覆盖范围内的列车会紧急制动, 当满足降级运行条件时又会重新开始运行, 因此, 列车运行性能曲线呈现先急后缓的下降趋势.

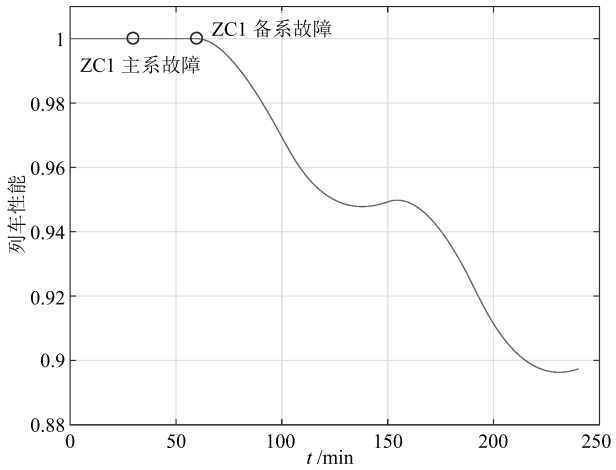


图 8 网络攻击下列车性能

Fig. 8 Operation performance of trains of CBTC test-bed under the cyber attack

3.3.3 信息安全状态评估结果

基于式 (5)、图 6 和图 8, 得到 CBTC 系统受攻击下整体性能的变化, 根据该结果可以判断列控系统当前的信息安全状态, 如图 9 所示.

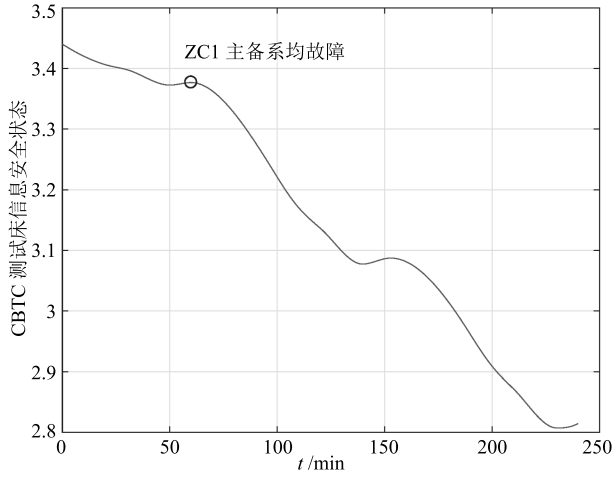


图 9 网络攻击下 CBTC 系统测试床的信息安全状态

Fig. 9 Security of CBTC test-bed under the cyber attack

随着 ZC 依次故障, CBTC 测试床安全程度逐渐下降, 仿真结果与预期基本相符. 特别地, 当某个 ZC 完全故障, 即整个 ZC 从网络中移除后, 系统的安全状态会略微提高, 这是由于每减少一个故障子系统, 通过该故障子系统入侵 CBTC 系统剩余部分的可能性变为 0, 因此, 系统的安全程度会有所提高.

3.4 CBTC 系统信息安全评估方法比较

文献 [5] 采用贝叶斯攻击图和 AHP – 模糊综合评价两种方法分别对 CBTC 系统进行信息安全风险评估. 其中, 贝叶斯攻击图从攻击者的角度结合系统架构、设备漏洞构建攻击图模型, 分析信息安全事件发生的概率及后果来衡量 CBTC 系统的风险值, 但是该方法只考虑了网络设备的漏洞, 没有考虑通信链路的特征; AHP 模糊综合评价, 运用模糊理论分析 AHP 层次模型, 并根据最大隶属度原则确定 CBTC 系统的风险等级, 该评估过程需要考虑具体的攻击类型, 且对专家经验、相关调研的依赖性强, 存在一定的主观性.

本文提出的基于二维结构熵的信息安全评估方法从攻击影响的角度, 将系统网络拓扑性能作为一个衡量 CBTC 系统信息安全状态的指标, 并结合攻击对列车运行性能造成的损失, 综合评估 CBTC 系统信息安全状态. 与贝叶斯攻击图相比, 本文方法不仅考虑了系统设计架构、设备漏洞, 还考虑了设备当前安全状态、密码策略以及通信方式、通信协议等特征, 评估过程简单, 可行性高; 与 AHP – 模糊综合评价方法相比, 本文只考虑攻击后果, 不针对特定攻击类型, 具有普适性, 且评估结果相对客观.

4 结论

本文提出了一种定量分析 CBTC 系统信息安全风险的方法. 对 CBTC 网络进行建模; 结合 CBTC 系统设备及设备间通信链路的特点, 以二维结构熵衡量信息安全攻击下网络拓扑性能的变化; 考虑到 CBTC 系统的功能安全设计, 综合列车运行性能与二维结构熵, 给出了 CBTC 系统信息安全状态的定量描述.

关于 CBTC 系统的信息安全状态与系统信息域及物理域性能变化的定量关系仍需做进一步的研究, 此外, 本文对列车运行性能的定义只考虑了列车的实际运行距离与理论运行距离之间的差异, 需要对该定义进行更深入的分析.

References

1 Zhang Xiao, Ding Zhi, Wu Yun-Shuang, Xie Zong-Xing. Analysis on present situation and prospects of city rail traffic development. *Modern City*, 2014, **9**(2): 17−19
(张霄, 丁智, 吴云双, 谢宗星. 城市轨道交通发展现状及前景浅析. 现代城市, 2014, **9**(2): 17−19)

2 Zheng Ying. Study on CBTC based on wireless communication. *Communications Technology*, 2011, **44**(12): 137−138, 141
(郑莹. 基于无线通信的 CBTC 研究综述. 通信技术, 2011, **44**(12): 137−138, 141)

3 Hong Xiang. Challenges and countermeasures for information security of rail transportation automation (excerpt). *Automation Panorama*, 2015, (2): 26
(洪翔. 轨道交通自动化信息安全面临的挑战与应对 (节选). 自动化博览, 2015, (2): 26)

4 Chen Deng-Ke. Network safety analysis of urban rail transit signaling system. *Railway Signalling and Communication Engineering*, 2012, **9**(5): 41−43
(陈登科. 城市轨道交通信号系统网络安全分析. 铁路通信信号工程技术, 2012, **9**(5): 41−43)

5 Bloomfield R, Bendele M, Bishop P, Stroud R, Tonks S. The risk assessment of ERTMS-based railway systems from a cyber security perspective: methodology and lessons learned. In: Proceedings of the 1st International Conference on Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. Paris, France: Springer, 2016. 3−19

6 Kuang Xiang-Qi. Research on Risk Assessment Method of Information Security in Communication-Based Train Control Systems [Master thesis], Beijing Jiaotong University, China, 2017.
(邝香琦. CBTC 系统信息安全风险评估方法研究 [硕士学位论文], 北京交通大学, 中国, 2017.)

7 Craven P V, Craven S. Security of ATCS wireless railway communications. In: Proceedings of the 2005 ASME/IEEE Joint Rail Conference. Pueblo, CO, USA: IEEE, 2005. 227−238

8 Yu Shu-Ya. Research on Information Security Detection Technology of Urban Rail Transit Control System [Master thesis], Beijing Jiaotong University, China, 2017.
(郁舒雅. 城市轨道交通列控系统信息安全检测技术研究 [硕士学位论文], 北京交通大学, 中国, 2017.)

9 Bao Zheng-Tang. Active Defense of Security Risk in Train Control System [Master thesis], Beijing Jiaotong University, China, 2017.
(包正堂. 列控系统信息安全风险主动防御研究 [硕士学位论文], 北京交通大学, 中国, 2017.)

10 Chen B B, Schmittner C, Ma Z D, Temple W G, Dong X S, Jones D L, et al. Security analysis of urban railway systems: the need for a cyber-physical perspective. In: Proceedings of the 2015 SAFECOMP Workshops on Computer Safety, Reliability, and Security. Delft, The Netherlands: Springer, 2014. 277−290

11 Li Wen-Wu, You Wen-Xia, Wang Xian-Pei. Survey of cyber security research in power system. *Power System Protection and Control*, 2011, **39**(10): 140−147
(李文武, 游文霞, 王先培. 电力系统信息安全研究综述. 电力系统保护与控制, 2011, **39**(10): 140−147)

12 Zhan Quan-Zhong, Chen Lan. A brief discuss on water resources network and information security system. *Water Resources Informatization*, 2010, (5): 31−33
(詹全忠, 陈岚. 浅谈水利网络与信息安全体系. 水利信息化, 2010, (5): 31−33)

13 Hu Jiang, Sun Guo-Chen, Zhang Jia-Jun, Hou Qin-Mai. The status quo and information security supervision of NPP from stuxnet attacks. *Chinese Journal of Nuclear Science and Engineering*, 2015, **35**(1): 181−185
(胡江, 孙国臣, 张加军, 侯秦脉. 由 “震网” 病毒事件浅议核电站信息安全现状及监管. 核科学与工程, 2015, **35**(1): 181−185)

14 Mendes E. Introduction to Bayesian networks. *Practitioners Knowledge Representation*. Berlin, Heidelberg: Springer, 2014. 67−71

15 Xie P, Li J H, Ou X M, Liu P, Levy R. Using Bayesian networks for cyber security analysis. In: Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Chicago, IL, USA: IEEE, 2010. 211−220

16 Shin J, Son H, Ur R K, Heo G. Development of a cyber security risk model using bayesian networks. *Reliability Engineering and System Safety*, 2015, **134**: 208−217

17 Shin J, Son H, Heo G. Cyber security risk evaluation of a nuclear I&C using BN and ET. *Nuclear Engineering and Technology*, 2016, **49**(3): 517−524

18 Schneier B. Attack trees. *Doctor Dobbs Journal*, 1999, **24**(12): 21−29

19 Mauw S, Oostdijk M. Foundations of attack trees. *Information Security and Cryptology — ICISC 2005*. Berlin, Heidelberg: Springer, 2006. 186−198

20 Ten C W, Liu C C, Govindarasu M. Vulnerability assessment of cybersecurity for SCADA systems using attack trees. In: Proceedings of the 2007 IEEE Power Engineering Society General Meeting. Tampa, FL, USA: IEEE, 2007. 1−8

21 Murata T. Petri nets: properties, analysis and applications. *Proceedings of the IEEE*, 1989, **77**(4): 541−580

22 Chen T M, Sanchez-Aarnoutse J C, Buford J. Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on Smart Grid*, 2011, **2**(4): 741−749

23 El Bouchti A, Haqiq A. Modeling cyber-attack for SCADA systems using CoPNet approach. In: Proceedings of the 2012 IEEE International Conference on Complex Systems (ICCS). San Agadir, Morocco: IEEE, 2012. 1−6

24 Jensen K, Rozenberg G. *High-Level Petri Nets: Theory and Application*. Berlin, New York: Springer, 1991.

25 Zhou S J, Qin Z G, Zhang F, Zhang X F, Chen W, Liu J D. Colored petri net based attack modeling. In: Proceedings of the 9th International Conference on Rough Sets, Fuzzy Sets, Data Mining, and Granular Computing. Chongqing, China: Springer, 2003. 715−718

26 Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu Q S. A survey of game theory as applied to network security. In: Proceedings of the 43rd Hawaii International Conference on System Sciences. Honolulu, HI, USA: IEEE, 2010. 1−10

27 Liang X N, Xiao Y. Game theory for network security. *IEEE Communications Surveys and Tutorials*, 2013, **15**(1): 472−486

28 Cui X L, Tan X B, Zhang Y, Xi H S. A Markov game theory-based risk assessment model for network information system. In: Proceedings of the 2008 International Conference on Computer Science and Software Engineering. Wuhan, China: IEEE, 2008. 1057−1061

29 Li A S, Pan Y C. Structural information and dynamical complexity of networks. *IEEE Transactions on Information Theory*, 2016, **62**(6): 3290−3339

30 Li A S, Hu Q F, Liu J, Pan Y C. Resistance and security index of networks: structural information perspective of network security. *Scientific Reports*, 2016, **6**: Article No. 26810

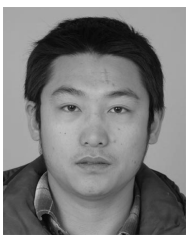
31 Shannon C E. A mathematical theory of communication. *Bell System Technical Journal*, 1948, **27**(3): 379−423

32 Anand K, Bianconi G. Entropy measures for networks: toward an information theory of complex topologies. *Physical Review E: Covering Statistical, Nonlinear, and Soft Matter Physics*, 2009, **80**(4): Article No. 045102

33 Dong H Y, Wang H W, Tang T. An attack tree-based approach for vulnerability assessment of communication-based train control systems. In: Proceedings of the 2017 Chinese Automation Congress (CAC). Ji′nan, China: IEEE, 2017. 6407−6412

董慧宇 北京交通大学电子信息工程学院硕士研究生. 2016 年获得北京交通大学电子信息工程学院学士学位. 主要研究方向为城市轨道交通列控系统信息安全. E-mail: 16120213@bjtu.edu.cn
(**DONG Hui-Yu** Master student at the School of Electronics and Information Engineering, Beijing Jiaotong University. She received her bachelor degree from Beijing Jiaotong University in 2016. Her research interest covers information security in communication-based train control systems.)

唐 涛 轨道交通控制与安全国家重点实验室教授. 1991 获得中国科学院博士学位. 主要研究方向为基于通信的列车运行控制, 高速列车控制系统和智能交通系统. E-mail: ttang@bjtu.edu.cn
(**TANG Tao** Professor at the State Key Laboratory of Rail Traffic Control and Safety. He received his Ph. D. degree from Chinese Academy of Sciences in 1991. His research interest covers communication-based train control, high-speed train control systems, and intelligent transportation systems.)



王洪伟 国家轨道交通安全评估研究中心副教授. 2014 年获得北京交通大学博士学位. 主要研究方向为基于通信的列车运行控制系统的车−地通信技术和地铁系统中的协作调度方法. 本文通信作者. E-mail: hwwang@bjtu.edu.cn
(**WANG Hong-Wei** Associate professor at the National Research Center of Railway Safety Assessment. He received his Ph. D. degree from Beijing Jiaotong University in 2014. His research interest covers train-ground communication technology in communication base train-ground communication systems and cooperative scheduling approaches in subway systems. Corresponding author of this paper.)