

城市轨道交通通信系统网络攻击分析与检测

高思凡 胡立强

(石家庄铁道大学电气与电子工程学院, 050043, 石家庄//第一作者, 本科生)

摘要 针对城市轨道交通通信系统面临的网络安全现状, 分析了网络安全需求, 深入阐述了现有的可能攻击手段, 厘清了网络安全威胁及风险, 并梳理了相应的检测方法, 并对不同检测方法进行了比较和分析。

关键词 城市轨道交通; 通信系统; 网络空间安全

中图分类号 U231.7

DOI:10.16037/j.1007-869x.2022.08.021

Analysis and Detection of Urban Rail Transit Communication System Network Attack

GAO Sifan, HU Liqiang

Abstract Targeting current network safety situation faced by urban rail transit communication system, network safety demand is analyzed, and existing possible attack and defense measures are expounded in depth. The network safety threats and risks are summarized, and corresponding detection methods are sorted. Different detection methods are compared and analyzed.

Key words urban rail transit; communication system; network space safety

Author's address Shijiazhuang Tiedao University, 050043, Shijiazhuang, China

如果城市轨道交通(以下简称“城轨”)通信系统被别有用心黑客控制^[1], 或城轨网络空间中的信息流被恶意监听抓取, 则会严重威胁到列车安全与乘客的生命安全。可见, 城轨通信系统的网络安全能力现已成为城轨发展的底线能力与保障基石。

近年来, 城轨领域的功能安全和网络空间安全一体化的问题受到了国内外学者的高度关注。现有的研究主要借鉴 CPS(信息物理系统)和工控系统的风险管控方法, 能够在一定程度上解决城市轨道交通网络安全风险与挑战。本文旨在研究城轨列车运行控制系统所面临的网络安全问题, 针对城市轨道交通可能遭遇的网络安全梳理了当前的检测方法。为城轨构建信息安全基石, 助力轨道交通行业从业者贯彻执行“系统自保、平台统保、边界

防护、等保达标、安全确保”的策略, 确保城轨云平台的全面支撑和城轨的安全发展。

城轨系统每天承载着上千万人的出行, 一旦发生网络安全事故, 后果十分严重。而列车控制系统的通信系统具有结构庞大、地理位置分散、互联系统多、网络边界不明确, 以及防护薄弱等特点。这些特点导致其容易被不法分子入侵和破坏。本文将分析城轨网络空间安全的各个方面, 如安全性需求、可能的攻击^[2]及现有的应对措施^[3-4]。

1 城轨网络空间的安全性需求

1) 增加容错性。当城轨列车运行于桥梁、隧道及洞窟等复杂环境中时, 不仅列车的行驶速度不同, 而且网络条件变化迅速, 故网络质量并不稳定。不稳定的网络质量与有限的带宽会严重影响城轨的实时通信效率。在低容错性系统中, 任何微小的时延和错误都会增大城轨网络空间安全的风险。故增加容错性是重要的城轨网络空间安全性需求。

2) 高移动性。为保证通信的高效和安全, 列车的通信数据包必须及时发送、传递与解析, 且在传递的过程中不可被修改。但在城轨列车运行控制系统的网络动态拓扑结构下, 列车的高移动性会影响列车通信的安全性, 难以保证通信数据包不被修改^[5]。因此要提高城轨网络空间安全性, 就必须在高移动性的前提下保证通信的高效和安全。

3) 隐私性与安全性的均衡。如果城轨网络空间系统被入侵, 则列车很容易被不法攻击者控制, 进而导致列车的功能安全被破坏。因此, 城轨安全系统建设必不可少。由于安全系统的海量数据采集会将居民个人的日常数据纳入数据库, 故城轨安全系统的增多又会增大居民个人隐私的泄漏风险, 从而产生隐私性问题的威胁。可见, 实现安全性和隐私性的均衡是城轨网络空间安全的一个主要挑战^[6-7]。

4) 云平台及其数据传输的安全性需求。现阶段

段的城轨系统入侵检测功能都是基于大数据技术和高性能计算来实现的,其在数据存储方面依赖于云平台的服务,故云平台自身的稳定性至关重要^[8]。此外,云平台与列车之间需进行精准的数据交互,而二者间的数据传输过程存在潜在的风险。为了保护隐私性,需要在数据传输和存储两方面都实现高效的加密算法。在数据的安全性方面,应能有效检测识别恶意节点或中间人,以避免危险数据注入时的严重后果。

2 城轨的网络空间攻击

城轨网络的复杂环境使得列车及列车通信环境暴露于各类攻击和威胁当中^[9]。在发生网络空间入侵时,不法进攻者的恶意行为会对城轨系统功能安全造成威胁或对城轨系统网络空间安全造成威胁,进而影响城轨运行的功能安全。

为保障城轨网络的安全,针对不法攻击者的入侵行为实现有效的预防与反制,应了解影响城轨网络空间安全的各种攻击,掌握其攻击特点。城轨网络空间安全攻击可分为主动攻击与被动攻击。主动攻击是指攻击者或恶意用户为了从网络中提取敏感信息而主动参与攻击的行为,可分为信息收集攻击、系统入侵攻击、数据欺骗攻击、拒绝服务攻击和物理破坏攻击等^[10]。被动攻击,指攻击者被动地收集网络信息,而不对网络进行实际篡改或注入任何信息。ID(身份标识号)泄漏攻击就属于被动攻击。常见的城轨通信系统网络空间攻击分类见表1。

表 1 常见的城轨通信系统网络空间安全攻击分类	
Tab.1 Classification of common security attacks in urban rail transit network space	
类型	细分类别
主动攻击	系统入侵攻击(如女巫攻击等),信息收集攻击(如中间人攻击等),数据欺骗攻击(如虚假信息注入攻击等),拒绝服务攻击(如 DoS(拒绝服务)攻击等),物理破坏攻击(如位置操控攻击)
被动攻击	虫洞攻击,ID 泄漏攻击,窥探攻击,否定攻击,黑洞攻击

2.1 女巫攻击

女巫攻击是一种主动攻击,在城轨安全系统中属于较为严重的威胁,在其他安全要求较高的系统中也是最危险、最难解决的攻击之一。在1个单纯的分布式P2P(对等计算机)网络中,任何节点只需

对外暴露其在P2P网络中的唯一标识,即可随意地加入和退出P2P网络,不受任何限制。女巫攻击利用了P2P网络的这一特性,将1个节点伪装成多个节点,并将这多个伪装节点(也称“Sybil节点”)广播到整个P2P网络中,即可实现获得网络控制权、拒绝响应或干扰查询等的操作^[11]。

在女巫攻击中,由于恶意攻击者具有多个身份,故很难确定接收到的信息是否来自伪装节点。有恶意行为的伪装节点或车辆被称为女巫节点。来自女巫节点的信息可误导调度中心及线路上的其他列车进行错误操作,甚至造成交通事故。其实现方式为:恶意攻击者可在线路上创建1个虚假的车辆或冒用合法车辆的身份,通过发送虚假的堵塞或到站等信息,或是提供错误的行驶路线,来欺骗城轨调度中心与其他列车。可见,女巫节点的破坏行为能对整个城轨网络空间造成干扰,严重影响车辆功能安全与乘客生命安全^[12-14]。

如图1所示,按通信方式、参与方式和身份来源,女巫攻击可分为通信类型(Communication type)、参与类型(Participation type)和身份类型(Sybil identity type)。

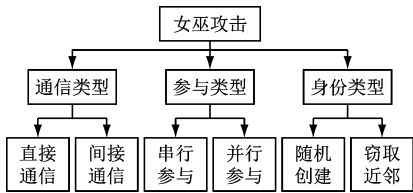


图 1 女巫攻击的分类
Fig.1 Classification of witch attacks

2.2 中间人攻击

中间人攻击是城轨网络空间中的重要攻击。在有线网络中,中间人攻击是通过ARP(地址解析协议)实现的。在无线网络中,攻击者在与原始接收者的通信中扮演“虚假发送者”角色,并在与原始发送者的通信中扮演“虚假接收者”角色,从而实现拦截和篡改通信数据。如图2所示,攻击者在同时窃取2列列车的通信数据,并向2列列车传出错误信息,进而发动攻击。在城轨列控系统中,通信数据用于传输重要的控制命令,一旦被攻击者篡改,则会影响列车运行的安全性。中间人攻击违反了安全需求的数据完整性和隐私性目标,会对传输信息的真实性造成负面影响,危及网络安全^[15-16]。

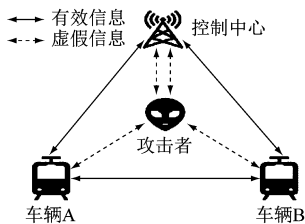


图2 中间人攻击示意图

Fig. 2 Diagram of man-in-the-middle attack

3 网络空间入侵的检测

为避免网络空间入侵带来的安全危害,有必要采取入侵检测技术,通过收集和分析城轨网络空间中关键数据的特征信息,来检测网络空间中的攻击行为。对于城轨通信网络来说,入侵检测技术作为防火墙之外的网络空间安全保障,能不影响城轨正常运行的情况下,实时监测网络状态,还能分析网络中的通信行为和数据流量,针对网络攻击及时给出告警,并为防御响应提供重要依据。对于不同的攻击,入侵检测方案有所不同。

3.1 女巫攻击的入侵检测

从女巫攻击的基本流程可知,简单的密钥检测已不再安全有效。恶意攻击者通过窃取或伪造正常运行列车的身份,可破解密钥,并发送错误信息,进而影响列车的运行效率或造成相邻列车的追尾等严重事故。

对女巫攻击入侵检测的常用方法有:

1) 时间戳与临时认证方法^[17]。时间戳认证基于以下事实:极少有2列列车会几乎同时发出信息。故当信息中包含一系列极为相近的时间戳时,可判定受到了女巫攻击。临时认证:给每列列车分配唯一的临时认证密钥,即1列列车只能拥有1对有效的临时密钥。这可有效避免女巫攻击。

2) 车辆运行的真实轨迹方法^[18]。设定2个路边单元时间不能少于最短可能时间等限定条件,判断只有符合限定条件的车辆轨迹才是真实的车辆轨迹,其余车辆运行轨迹均为女巫攻击的虚假信息。

3) 本地安全认证方法^[19]。基于LTE-T2T(长期演进-车车通信)的城轨列车中心无线通信系统,提出了在用户链路建立时用于列车安全认证的本地安全认证方案,再以本地安全认证方案为基础,进一步提出了用户防御女巫攻击的协作式信息安全检测方法。

上述方法的利弊分析:

1) 时间戳与临时认证方法可行性较强,对网络数据传输的要求较低,可以判别大多数情况,但相比于另外两种方法其认证方法的效率较低。

2) 车辆运行的真实轨迹方法虽能有效检测女巫攻击,但针对不同的路况环境,其限定条件往往难以统一。尤其对于重庆等路况复杂的地域而言,其确认合理限定条件的复杂度会大大增加。

3) 就现阶段而言,本地安全认证方法的实现较为困难。相比于另外两种方法,该方法对列车与列车之间、列车与控制中心之间数据传输的速度和准确度要求较高。

3.2 中间人攻击的入侵检测

目前常见的中间人攻击方法主要有ARP(地址解析协议)欺骗、DNS(域名系统)欺骗和SSL(安全套接字协议)欺骗。

对于中间人攻击入侵检测的常用方法有:

1) 认证、申请状态模型检测方法^[20]。参照802.1X-2004认证和申请状态模型基础,从RSNA(强健安全网络关联)建立过程角度判断RSN(强健安全网络)中的中间人攻击,RSN会利用RSNA过程完成STA(发放-触发平均方法)和网络间的双向认证,如果此过程异常中断则断定受到了中间人攻击。

2) 端口重定向和证书链检测方法^[21]。大型网络系统大多采用SSL协议保护用户的敏感数据,但是由于存在浏览器证书验证隐患、用户的疏忽以及网站服务器架设方式缺陷等问题,攻击者仍然可以借此发动中间人攻击。其攻击主要体现在端口非正常变化、非正常安装证书以及ARP缓存改变。

3) 基于贝叶斯博弈的检测和防御方法^[22]。从博弈和控制角度检测中间人攻击,当发生中间人攻击时会产生信息的博弈对局,而从博弈对局的角度看双方的信息都将不完全,地面系统的信息集将会较大程度缩小,由此可以检验出中间人攻击。

上述检测方法分析:

1) 认证、申请状态模型检测方法对于中间人攻击识别度较高,但局限于RSNA的建立,对于其他类型的中间人攻击无法检测。

2) 端口重定向和证书链检测方法较为简单,但需要频繁进行ARP查询来验证是否遭到攻击,在实际应用中可行性较低。

3) 基于贝叶斯博弈的检测和防御方法可以较好地实现对多种中间人攻击的检测和防御,从而降

低其攻击造成的城轨系统损失,但对数据传输的速度和准确度要求较高。

4 结语

本文研究并探索了城轨网络空间安全的安全性需求;分析了网络空间中不同类型攻击行为的模型与其对城轨功能安全的影响机理;归纳梳理了典型城轨攻击行为的网络空间安全入侵检测方案。通过对攻击模型以及入侵检测方案的研究,可以为未来城轨网络空间管理系统的发展与更新提供新思路,加强对城轨新技术发展的研究,使其技术更加成熟,便于推广和应用。这不仅有利于形成整体性的、全局性的安全管理体系,符合时代发展需求,而且能为智慧城轨的实现奠定扎实的基础,具有重要意义。

参考文献

- [1] 李祥,步兵,朱力.城市轨道交通列控系统主动防御方法研究[J].中国安全科学学报,2019(增刊2):62.
LI Xiang, BU Bing, ZHU Li. Research on proactive defense-method in train control system for urban rail transit[J]. Chinese Safety Science Journal, 2019(S2): 62.
- [2] ALI I, HASSAN A, LI F. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey[J]. Vehicular Communications, 2019, 16:45.
- [3] ISAAC J T, ZEADALLY S, CAMARA J S. Security attacks and solutions for vehicular ad hoc networks[J]. IET Communications, 2010, 4(7):894.
- [4] FAROOQ J, SOLER J. Radio communication for communications-based train control (CBTC): a tutorial and survey[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3):1377.
- [5] QU F, WU Z, WANG F, et al. A security and privacy review of VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(6):2985.
- [6] MALIK V, BISHNOI S. Security threats in VANETS: a review, 2014[J]. International Journal of Recent Research Aspects, 2015, 2(1):2349.
- [7] WU W, YANG Z, LI K. Internet of vehicles and applications[J]. Internet of Things, 2016:299.
- [8] SUN Y, ZHANG J, XIONG Y, et al. Data security and privacy in cloud computing[J]. International Journal of Distributed Sensor Networks, 2014(7):9.
- [9] MANVI S S, TANGADE S. A survey on authentication schemes in VANETs for secured communication[J]. Vehicular Communications, 2017, 9:19.
- [10] 林瑜筠.城市轨道交通信号[M].3版.北京:中国铁道出版社有限公司,2015.
LIN Yuyun. Urban rail transit signal[M]. 3ed. Beijing: China Railway Publishing House, 2015.
- [11] BARIAH L, SHEHADA D, SALAHAT E, et al. Recent advances in VANET security: a survey[C]//2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), September 6-9, 2015. Boston, MA, USA. New York: IEEE, 2015:1.
- [12] SAKIZ F, SEN S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV[J]. Ad Hoc Networks, 2017, 61:33.
- [13] IWENDIC O, UDDIN M, ANSEREJ A, et al. On detection of Sybil attack in large-scale VANETs using Spider-Monkey technique[J]. IEEE Access, 2018, 6:1.
- [14] SUMRA I A, AHMAD I, HASBULLAH H, et al. Classes of attacks in VANET[C]//2011 Saudi International Electronics, Communications and Photonics Conference (SIEPCP), Riyadh, Saudi Arabia. New York: IEEE, 2011:1.
- [15] LIPINSKI B, MAZURCZYK W, SZCZYPIORSKI K, et al. Towards effective security framework for vehicular ad-hoc networks[J]. Journal of Advances in Computer Networks, 2015, 3(2):134.
- [16] KUMAR A, SINHA M. Overview on vehicular ad hoc network and its security issues[C]//2014 International Conference on Computing for Sustainable Global Development (INDIACom), March 5-7, 2014. New Delhi, India. New York: IEEE, 2014:792.
- [17] PARK S, ASLAMB, TURGUTD, et al. Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support[J]. Security & Communication Networks, 2013, 6(4):523.
- [18] CHANG S, QI Y, ZHU H, et al. Footprint: detecting Sybil attacks in urban vehicular networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(6):1103.
- [19] 王晓轩.城市轨道交通 CBTC 无线通信系统可信性分析及优化[D].北京:北京交通大学,2020.
WANG Xiaoxuan. Dependability analysis and optimization of CBTC wireless communication systems in urban rail transit systems[D]. Beijing: Beijing Jiaotong University, 2020.
- [20] 汪定,马春光,翁臣,等.强健安全网络中的中间人攻击研究[J].计算机应用,2012(1):42.
WANG Ding, MA Chunguang, WENG Chen, et al. Research of man-in-the-middle attack in robust security network[J]. Journal of Computer Applications, 2012(1):42.
- [21] 贾静,薛质. SSL 中间人攻击原理与防范[J].信息安全与通信保密,2007(4):103.
JIA Jing, XUE Zhi. The principle and prevention of SSL man-in-the-middle attack[J]. Information Security and Communication Privacy, 2007(4):103.
- [22] 彭亚枫.城轨 CBTC 系统中间人攻击检测与防御方法研究[D].北京:北京交通大学,2018.
PENG Yafeng. Research on detection and defense of urban rail CBTC system man-in-the-middle attack[D]. Beijing: Beijing Jiaotong University, 2018.

(收稿日期:2021-09-25)