

新型入侵检测技术在城市轨道交通 信号系统中的应用研究*

王俊彦¹ 衣 然² 张 斌² 车聪聪¹ 马 超¹

(1. 中车青岛四方机车车辆股份有限公司, 266111, 青岛; 2. 华北计算机系统工程研究所, 100083, 北京//第一作者, 高级工程师)

摘 要 城市轨道交通作为城市的关键基础设施,其网络安全问题尤为重要。尽管传统的防护安全机制已经应用到城市轨道交通系统的各个子系统中,但仍应进一步监视 CBTC (基于通信的列车控制)系统更底层的进程级活动。提出了一种针对 CBTC 系统底层信号的新型入侵检测技术,分析了其与传统入侵检测方法之间的区别,阐述了该新型技术的工作原理和工作过程。通过对某条城市轨道交通线路 CBTC 系统采集得到的真实数据进行仿真试验,验证了该新型入侵检测技术的有效性。

关键词 城市轨道交通; 信号系统; 入侵检测; 网络安全
中图分类号 U231.7

DOI:10.16037/j.1007-869x.2022.07.009

Research on Application of New Intrusion Detection Technology in Urban Rail Transit Signaling System

WANG Junyan, YI Ran, ZHANG Bin, CHE
Congcong, MA Chao

Abstract Urban rail transit is the key infrastructure of city, the network security of which is particularly important. Although the conventional protection safety mechanism has been applied to each subsystem of the urban rail transit system, the lower-level process-level activities of CBTC should be further monitored. A new intrusion detection technology for the underlying signal of CBTC system is proposed, and the difference between this and the conventional intrusion detection method is analyzed. The working principle and process of the new technology are expounded. The effectiveness of the new intrusion detection technology is verified by simulation experiments on the real data collected by the CBTC system of an urban rail transit line.

Key words urban rail transit; signaling system; intrusion detection; network security

First-author's address CRRC Qingdao Sifang Co., Ltd., 266111, Qingdao, China

《中华人民共和国网络安全法》明确了对于涉及公共利益的关键信息基础设施,在网络安全等级保护制度的基础上,实行重点保护^[1]。CBTC(基于通信的列车控制)是城市轨道交通的核心系统之一,包括 ATS(列车自动监控)、MSS(维护支持系统)等多个子系统^[2]。随着工业互联网时代的到来,CBTC 各个子系统互联互通的程度越来越高,各子系统间的信息安全也逐渐开始受到行业和相关管理部门(包括中共中央网络安全和信息化委员会办公室、公安部、工业和信息化部等)的高度重视。传统的安全防护设备往往关注的是信号系统的流量安全,而忽视了更底层的信号采集端的安全,因此,及时检测出信号采集过程中的恶意流量并进行报警,对于城市轨道交通信号系统来说尤为重要。

1 入侵检测技术概念

近年来,针对 CBTC 系统这类关键基础设施的攻击大多为 APT(高级可持续攻击)。攻击者通过注入大量虚假数据来隐藏自己的攻击^[3],同时控制受损的传感器值,使其大致保持在噪声水平之内。这样,对噪声不敏感的故障检测装置或本身性能存在异常的检测装置就很难检测到这种隐藏在噪声中的恶意攻击。

入侵检测是实时监测网络中的流量,在出现异常问题时进行相应处理的一种网络安全技术^[4]。如图 1 所示,传统入侵检测主要分为信息收集、系统辨识、威胁处理 3 个步骤^[5],在完成信息收集后,通过模式匹配、统计与完整性分析等系统辨识方式,建立物理过程的线性动态状态空间模型,经过预测

* 国家重点研发计划先进轨道交通重点专项(2017YFB1201103)

和更新这两个计算过程来判断系统是否含有恶意攻击流量。虽然这样的方法可能会检测到异常行为,但其检测模型很难建立,需要在初始阶段付出大量的人力,而且建立的物理模型并不一定适用于城市轨道交通系统。因此,本文尝试使用一种新的入侵检测方法,不需要建立线性动态状态空间模型,而是只关注 CBTC 系统中现场传感器的采样状态变化,通过检测传感器当前的读数是否因生成机制的变化而偏离了过去的读数,来判断 CBTC 系统中是否有异常行为。

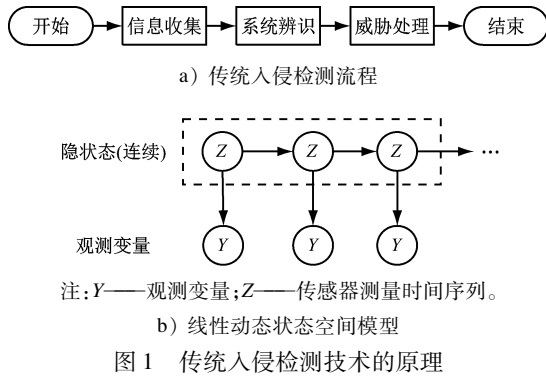


图1 传统入侵检测技术的原理

Fig. 1 Principle of traditional intrusion detection technology

本文提出的新型入侵检测技术是一种轻量、快速、无模型的进程级检测技术,能够检测传感器信号中的细微变化,大大增加了检测出策略性攻击者的可能性。其工作机制是:首先通过一个训练阶段学习传感器测量时间序列中记录的正常行为,再从正常工作的传感器测量时间序列中提取降噪信号信息,最后主动检查当前提取的信号是否与历史值产生偏离,从而判断系统中是否混合了恶意流量。为了提取信号信息,新型入侵检测技术借鉴了 SSA (奇异谱分析) 概念来提取信号信息^[6],通过识别 1 个信号子空间并进行计算,然后将计算结果与预估的结果进行对比,如果结果不一致,则表明生成时间序列的机制可能发生了变化,被测系统可能受到攻击。

2 新型入侵检测技术工作过程

如图 2 所示,在 CBTC 系统信号提取过程中经过了嵌入、奇异值分解、分组、重构 4 个步骤。具体工作过程如下:第一步,将传感器测量的时间序列嵌入到欧几里得空间中^[7];第二步,对从时间序列数据得出的特殊矩阵进行频谱分解,以提取系统行为的确定性部分;第三步,识别信号子空间,并将与正常操作条件下的传感器测量值相对应的矢量投

影到该子空间上,以获得正常过程行为的表示;第四步,系统会跟踪偏离分数,以确定该过程是否偏离正常状态。

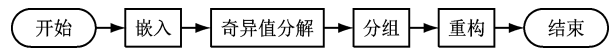


图2 SSA 技术流程图

Fig. 2 Technical flowchart of SSA

2.1 嵌入

设 x_i 为滞后向量。 L 为整数,作为 x_i 的滞后参数,然后通过形成 K 个长度为 N 的滞后向量 T ,使之作为初始子序列,嵌入 L 维欧几里得空间 R_L 中, $T \in L$,则有:

$$x_i = [x_i, x_{i+1}, \dots, x_{i+L-1}]^T \quad (1)$$

式(1)中, $1 \leq i \leq K, K = N - L + 1$ 。构造轨迹矩阵 X , X 的每一列均是滞后向量:

$$X = \begin{bmatrix} x_1 & x_2 & \dots & x_K \\ x_2 & x_3 & \dots & x_{K+1} \\ \vdots & \vdots & & \vdots \\ x_L & x_{L+1} & \dots & x_N \end{bmatrix} \quad (2)$$

2.2 奇异值分解

为了提取用以描述 CBTC 系统确定性行为的降噪信号信息,对 X 进行奇异值分解后可得到 l 个特征向量 u_1, u_2, \dots, u_l , 组成滞后协方差矩阵 XX^T 。然后,计算时间序列的统计个数 r , 判断确定性与变异性的自由度数。

2.3 信号子空间上的投影

在获得信号信息之后,在第三个步骤中,识别正常过程行为的数学表示。设有 r 个前导特征值, U 是 $l \times r$ 矩阵,其列是 r 个特征向量 u_1, u_2, \dots, u_r 。由此可知, l' 是 U 的列向量所跨越的子空间。计算 x_i 的样本均值 c :

$$c = \frac{1}{k} \sum_{i=1}^k x_i \quad (3)$$

在 l' 中形成簇的质心 \bar{c} , 其计算式为:

$$\bar{c} = Pc \quad (4)$$

其中, P 为投影矩阵, $P = U(U^T U)^{-1} U^T = UU^T$ 。

2.4 距离追踪

为了检测系统行为结构变化的攻击,需计算每个传感器观测得到的偏离分数。对于每个测试向量 $x_j (j > k)$, 计算 l' 中到质心 \bar{c} 的欧几里德距离的平方值 D_j :

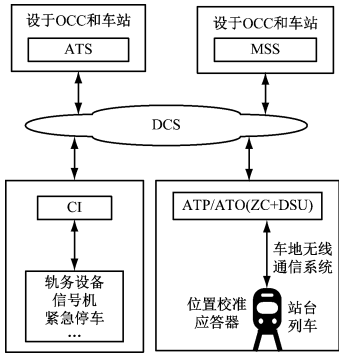
$$D_j = \|\bar{c} - Px_j\|^2 \quad (5)$$

设 θ 为系统设置的报警阈值。当 $D_j \geq \theta$ 时,将生成报警信息。设 τ 是恶意流量攻击的开始时间,

则在 $(n+1, \tau-1)$ 这个时间段内,通过对比正常状态下观测值和攻击开始前的观测值,可计算得到正常流量下偏离分数的最大值,以有效避免正常流量扰动产生的误报。

3 CBTC 系统入侵检测仿真试验

如图3所示,CBTC被广泛运用于城市轨道交通系统中,可以实现车-地之间的双向通信^[8]。CBTC的核心为ATP(列车自动防护)、ATO(列车自动运行)两个子系统,这两个子系统分别用以处理列车超速防护、车门开关、列车制动等列车运行控制,确保列车安全、高效运行^[9]。



注:OCC——运营控制中心;DCS——数据通信子系统;CI——计算机联锁;ZC——区域控制器;DSU——数据存储器单元。

图3 CBTC 系统结构图

Fig. 3 Diagram of CBTC system structure

3.1 搭建试验环境

如图4所示,本次试验中使用的硬件设备包括2台计算机(PC1、PC2)、1个具有镜像功能的交换机和1台路由器。其中:PC1用于安装科莱数据重放软件,模拟CBTC系统运行,产生运行数据;PC2作为安全管理终端,运行入侵检测程序,采集并检测数据。

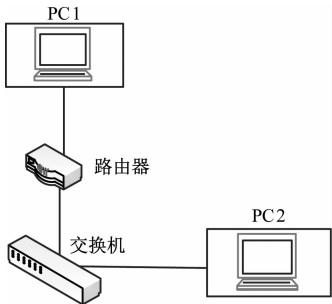


图4 试验环境网络拓扑图

Fig. 4 Network topology of test environment

3.2 试验过程

本次试验中,使用某地铁线路CBTC系统采集到的真实镜像数据,数据采集耗时10 d。作为仿真

试验的数据,在数据重放之前,先对流量数据进行检测和处理,并将数据分为3个部分。其中:第一部分数据为正常流量数据;第二部分数据为攻击流量数据,即在正常流量数据中混合的APT数据包,但该数据包只保留漏洞验证程序,不会对系统产生影响;第三部分数据为混合流量,正常流量数据中插入了APT流量,以此进行试验验证。这些数据均存放在PC1中,由PC1进行数据包的重放。PC2通过交换机的镜像口采集试验数据,并运行新型入侵检测程序。

具体的试验过程包括两个部分:

1) 试验一。PC1进行正常流量数据重放,PC2进行系统监控,重放时间为24 h;

2) 试验二。PC1进行攻击流量和混合流量数据重放,PC2进行系统监控,重放时间为24 h。

3.3 试验结果

根据试验的设定值 θ ,观测入侵检测程序的输出值。在正常流量数据通过时,检测到 $D_j < \theta$,系统未生成告警;在攻击流量数据通过时, $D_j \geq \theta$,系统立即生成告警;在混合流量数据通过时, $D_j \geq \theta$,系统也生成告警,试验达到了预期效果。重放最终监测结果如表1所示,为方便计算,所有数值均已取整。

表1 试验参数设定及其仿真输出值

Tab.1 Test parameter setting and simulation output value

试验序号	$n/\text{个}$	$l/\text{行}$	$r/\text{列}$	D_j	θ
试验一	1 000	500	13	8	10
试验二	2 000	1 000	16	22	10

4 结语

与传统的IT(信息技术)系统相比,城市轨道交通CBTC系统这类工业控制系统若受到网络攻击,可能会造成更为严重的损失和影响。本文提出了一种新型入侵检测技术,对CBTC系统的底层数据进行实时监测,可精准识别隐藏在正常流量中的恶意攻击,这对于CBTC系统网络的安全防护具有重大意义^[10]。如果在底层网络设置该新型入侵检测系统,在上层网络部署其他安全设备和安全策略,CBTC系统的安全防护水平将会大大提高。

参考文献

[1] 于臣军. 从等级保护角度浅谈公安视频网安全建设[J]. 中国公共安全,2018(7):178.
YU Chenjun. Discussion on the public security video network safety construction from the perspective of hierarchical protection [J]. China Public Security, 2018(7):178.

- [2] 李风华. 城市轨道交通 CBTC 系统区域控制器的研究与仿真[D]. 兰州:兰州交通大学,2011.
LI Fenghua. Research and simulation on zone controller of the CBTC system for urban rail transit[D]. Lanzhou: Lanzhou Jiaotong University, 2011.
- [3] 吴晓琴, 黄文培. Hadoop 安全及攻击检测方法[J]. 计算机应用, 2020(增刊1):118.
WU Xiaojin, HUANG Wenpei. Hadoop security and attack detection methods[J]. Journal of Computer Application, 2020(S1):118.
- [4] 李剑. 信息安全产品与方案[M]. 北京:北京邮电大学出版社, 2008:267.
LI Jian. Information security products and solutions[M]. Beijing: Beijing University of Posts and Telecommunications Publishing House, 2008:267.
- [5] 杨茂云. 信息与网络安全实用教程[M]. 北京:电子工业出版社, 2007:200.
YANG Maoyun. Practical course of information and network security[M]. Beijing: Publishing House of Electronics Industry, 2007:200.
- [6] 刘帅, 李智, 龚建村, 等. 基于奇异谱分析的空间环境数据插补方法[J]. 北京航空航天大学学报, 2016(4):829.
LIU Shuai, LI Zhi, GONG Jiancun, et al. Gap filling method for

space environment data based on singular spectrum analysis[J]. Journal of Beijing University of Aeronautics and Astronautics, 2016(4):829.

- [7] 王林鸿. 数控工作台非线性动态特性的辨识研究[D]. 武汉:华中科技大学,2009.
WANG Linhong. Research on nonlinear dynamic characteristics identification of NC table[D]. Wuhan: Huazhong University of Science and Technology, 2009.
- [8] 刘攀峰. 安全相关软件的设计方法研究及应用[D]. 杭州:浙江大学,2012.
LIU Panfeng. Research and application of the safety-related software design method[D]. Hangzhou: Zhejiang University, 2012.
- [9] 徐万里. 城市轨道交通列车控制系统集成项目的风险管理[D]. 北京:北京交通大学,2014.
XU Wanli. Risk management of urban transit train control system integration project[D]. Beijing: Beijing Jiaotong University, 2014.
- [10] 巩林明, 张振国. 入侵检测 ID 技术的探讨[J]. 南北桥, 2008(11):25.
GONG Linming, ZHANG Zhenguo. Discussion on ID technology of intrusion detection[J]. South North Bridge, 2008(11):25.

(收稿日期:2021-05-21)

(上接第 42 页)

注浆、缓慢变化和趋于稳定 4 个阶段。围岩压力整体表现为上下大、左右小的“鸭蛋”形不均匀分布,在管片设计时应应对隧道上下方进行局部加强。

2)管片轴力均为负值,即管片处于受压状态,其中左拱腰处的轴力最大。管片轴力整体呈现左上方大、右下方小的不均匀分布规律,在管片拼装施工时应可能减少左上部管片错台。

3)衬砌环弯矩均为正值,即管片外侧受拉,其弯矩最大值位于拱底处,衬砌环弯矩呈现为上下大、左右小的分布规律,在施工与后续运营中应密切关注隧道上下方管片结构挤压破损等病害。

参考文献

- [1] 林荣安, 刘伯莹. 富水淤泥质软土地层盾构隧道管片受力特征研究[J]. 中国公路学报, 2018(9):112.
LIN Rongan, LIU Boying. Mechanical characteristic investigation of shield tunnel segment in water-rich mucky soft stratum[J]. China Journal of Highway and Transport, 2018(9):112.
- [2] 张君禄, 段峰虎, 廖文来, 等. 湛江湾跨海盾构隧道管片现场监测试验研究[J]. 岩石力学与工程学报, 2014(增刊1):2878.
ZHANG Junlu, DUAN Fenghu, LIAO Wenlai, et al. Field monitoring experimental study of sea-crossing shield tunnel segment in Zhanjiang Bay[J]. Chinese Journal of Rock Mechanics and Engineering, 2014(S1):2878.
- [3] 周济民, 何川, 肖明清, 等. 狮子洋水下盾构隧道衬砌结构受力

的现场测试与计算分析[J]. 铁道学报, 2012(7):115.

- ZHOU Jimin, HE Chuan, XIAO Mingqing, et al. Field test and numerical simulation of mechanics of segment lining of Shiziyang underwater shield tunnel[J]. Journal of the China Railway Society, 2012(7):115.
- [4] 梁禹, 苏文辉, 方理刚, 等. 大直径江底盾构隧道衬砌结构受力现场测试与分析[J]. 隧道建设, 2014(7):637.
LIANG Yu, SU Wenhui, FANG Ligang, et al. Field test and analysis on stress of lining of large-diameter river-crossing shield tunnel[J]. Tunnel Construction, 2014(7):637.
- [5] 唐孟雄, 陈如桂, 陈伟. 广州地铁盾构隧道施工中管片受力监测与分析[J]. 土木工程学报, 2009(3):118.
TANG Mengxiong, CHEN Rugui, CHEN Wei. Stress monitoring and internal force analysis of Guangzhou metro shield tunnel segment during construction[J]. China Civil Engineering Journal, 2009(3):118.
- [6] 叶冠林, 王吉云, 王建华, 等. 超大断面盾构隧道管片施工荷载现场监测研究[J]. 现代隧道技术, 2010(5):85.
YE Guanlin, WANG Jiyun, WANG Jianhua, et al. In-situ monitoring of construction loading acting upon segments of a super large shield tunnel[J]. Modern Tunnelling Technology, 2010(5):85.
- [7] 张恒, 陈寿根, 谭信荣, 等. 不同地层盾构隧道管片力学行为研究[J]. 地下空间与工程学报, 2015(4):845.
ZHANG Heng, CHEN Shougen, TAN Xinrong, et al. Research on mechanical behaviour of segmental structure of shield tunnel in different strata[J]. Chinese Journal of Underground Space and Engineering, 2015(4):845.

(收稿日期:2020-12-08)