doi:10.3969/j.issn.1001-893x.2014.02.016
引用格式:谢文军,付 晓,于振华,等.信息物理融合系统软件可信性演化动力学建模[J].电讯技术,2014,54(2):201-205.[XIE Wen-jun, FU Xiao, YU Zhen-hua, et al. Modeling Software Trustworthiness Evolution of Cyber-Physical Systems Using Nonlinear Dynamics[J]. Telecommunication Engineering, 2014, 54(2):201-205.]

信息物理融合系统软件可信性演化动力学建模*

谢文军,付 晓,于振华**,韩 林

(空军工程大学 信息与导航学院,西安 710077)

摘 要:信息物理融合系统(CPS)软件可信性建模是 CPS 可信软件开发过程中至关重要的一环,现有的形式化方法、软件验证技术并不适合对 CPS 软件可信性动态演化进行描述和分析。在深入分析 CPS 可信软件动态演化过程的基础上,结合非线性动力学的基本理论和方法,研究 CPS 软件可信性演化的动力学机制,对 CPS 软件在内外双重因素影响下的可信性演化过程进行建模,并分析其可信性演化规律,为 CPS 软件可信性研究提供了一种新手段。通过对一个工业控制领域中 CPS 软件的建模与分析,验证了该方法的可行性。

关键词:信息物理融合系统;非线性动力学;可信软件;建模与分析
中图分类号:TP311.5 **文献标志码**:A **文章编号**:1001-893X(2014)02-0201-05

Modeling Software Trustworthiness Evolution of Cyber-Physical Systems Using Nonlinear Dynamics

XIE Wen-jun, FU Xiao, YU Zhen-hua, HAN Lin

(School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China)

Abstract: Software trustworthiness is critical to assure the safety and effectiveness of Cyber-Physical Systems (CPS). The formal methods and software verification technologies are not suitable for describing and analyzing the software trustworthiness dynamic evolution of CPS. Based on the in-depth analysis of the software trustworthiness dynamic evolution of CPS, the dynamics characteristics for software trustworthiness of CPS are analyzed by using nonlinear dynamics. The software trustworthiness evolution model of CPS under internal and external factors is proposed, and the trustworthiness evolution law is analyzed. By an example of industry control systems, the feasibility of the proposed software trustworthiness evolution model of CPS is demonstrated using numerical simulations and theoretical analysis.

Key words: cyber-physical system; nonlinear dynamics; trustworthy software; modeling and analysis

1 引 言

信息物理融合系统(Cyber-Physical System, CPS)是一种集成计算、通信与控制功能的新型智能嵌入式系统,系统中计算进程和物理进程在开放环境下持续交互、深度融合,从而实现大规模物理系统的实时感知、远程精确控制和信息服务[1],并在国

* **收稿日期**:2013-10-10;**修回日期**:2014-01-07 Received date:2013-10-10;Revised date:2014-01-07
基金项目:国家自然科学基金资助项目(61202128);航空科学基金资助项目(20125896020);陕西省自然科学基金资助项目(2011JQ8011)
Foundation: The National Natural Science Foundation of China (No. 61202128); The Aviation Science Funds of China (No. 20125896020); The Natural Science Foundation of Shaanxi Province(2011JQ8011)
** **通讯作者**:zhenhua_yu@163.com **Corresponding author**: zhenhua_yu@163.com

防安全、航空航天、智能电网、医疗设备等多个领域得到了广泛应用。

不同于传统的计算机控制系统和传感器网络,首先,CPS 是动态、自治、异构的复杂系统;其次,CPS 包含传感器节点(Sensors)、执行器节点(Actuators)和控制器节点(Controllers),各节点间通过有线或无线网络连接实现节点间的高效协作、精确控制、资源的动态组织与协调分配、体系结构重配置等功能[2]。CPS 的最终目标是实现信息世界和物理世界的完全融合,构建一个可控、可信、可扩展且安全高效的 CPS 网络,进而改变人与物理世界交互的方式[3]。

软件是 CPS 的灵魂,其在 CPS 中所起的作用也越来越大。由于 CPS 主要应用于安全关键系统中,生存环境恶劣,极易遭受感染与攻击,且其功能需求也在不断增加,导致 CPS 软件日趋庞大化、复杂化,并不可避免地产生了越来越多的缺陷及漏洞,这也使得 CPS 愈发脆弱,一旦系统失效或发生故障,将造成难以挽回的巨大损失。2010 年爆发的“震网”病毒是首例针对工业控制系统的恶意代码,可突破 CPS 的物理域限制直接对物理世界中的工业设施造成破坏,伊朗核电站便因遭受“震网”攻击而被迫推迟发电;2012 年,“火焰”(Flame)爆发,“火焰”能够使用服务器远程控制受感染的计算机,并通过录音、截图及记录网络消息等手段来盗取机密文件、联系人数据等重要信息[4]。因此,我们必须提高 CPS 软件的可信性,防止软件漏洞及系统内部缺陷被恶意攻击所利用,这对 CPS 的安全性和有效性至关重要[5]。虽然目前采用了防火墙技术、主动防御技术、入侵检测技术等多种防护手段来保障软件的运行安全,但这些传统的安全防护技术只能较好地对抗外部入侵,而从内部发起的攻击与窃密仍旧防不胜防。为了解决这一问题,美国国家自然科学基金自 2005 年起便组织了一系列关于 CPS 可信软件的研讨会及国际会议[6],探讨了 CPS 在航空、汽车、铁路等安全关键系统的应用、构建高可信软件的方法与技术及所面临的挑战。我国学术界也对此展开了研究,文献[7]对网络时代的软件可信演化进行了研究,提出了可信软件演化论;文献[8]建立了基于软件行为可信性的软件动态可信理论模型,并用于软件动态可信评测。

由于 CPS 软件通常在恶劣环境中长期运行,这一过程中其可信性持续演化,不断变化,这往往导致原本可信的软件不再可信,因此需要对其可信性演化规律进行研究和分析。然而现有的形式化方法、软件验证技术[5,9]等仅在描述静态 CPS 软件时表现良好,并不适合对 CPS 软件可信性动态演化规律进行描述和分析。通过研究可发现,CPS 软件在复杂环境中动态行为演化的统计特性与软件可信性特征属性存在对应关系[10]。综合这些统计特性,本文利用非线性动力学理论与方法建立 CPS 软件行为演化动力学模型,为 CPS 软件可信性的判定提供一定参考。

2 信息物理融合系统软件可信性及其动态演化

2.1 信息物理融合系统软件可信性研究

可信性是在可靠性、正确性、安全性、时效性、可用性、可预测性、可控性、私密性、高效性、可生存性等概念基础上发展而来的一个新概念。目前,学术界对于软件可信性的定义仍有争议,一个被广泛认可的定义是:所谓“可信软件”,通常是指那些运行行为及其结果总是符合人们预期,并在受到干扰时仍能提供连续服务的软件[11]。本文认为 CPS 可信软件应具备一定的抗病毒、抗攻击能力,即在恶意攻击下能够保持稳定运行、异常状态可控、行为符合预测,可得到预期结果。

文献[12]从资源共享、资源能力提供、局部性能和整体性能这 3 个角度出发将可信研究划分为身份可信问题、能力可信问题和行为可信问题,在此基础上,本文根据 CPS 软件的特点,将 CPS 软件可信研究进一步分为功能可信、能力可信、身份可信、数据可信、行为可信。其中,功能可信着眼于用户需求,保证 CPS 软件能够满足用户所提出的要求;能力可信着眼于 CPS 软件实现其功能的能力,强调了 CPS 软件执行任务能力的可靠性及高效性;身份可信对 CPS 软件进行约束以确保 CPS 软件总是在规则允许的范围之内对相应资源进行访问和利用;数据可信立足于数据,从数据层面来保证 CPS 软件的可信性,数据是软件执行任务的基础,只有确保数据安全,防止数据泄露,才能保证 CPS 软件的安全可信;行为可信则确保 CPS 软件在其行为演化过程中的可信性,是 CPS 软件可信性的核心问题,也是本文研究的重点所在。

在 CPS 软件数据完整的前提下,如何确保 CPS 软件的行为总是以预期的方式朝着预期的目标运行,这就是 CPS 软件动态行为可信问题[13],CPS 软

件的动态行为可信性是衡量其可信与否的重要依据,是行为可信的核心问题。若 CPS 软件的动态行为可信性无法得到保证,会引发如软件失效、运行异常、数据泄露、远程操控等问题,甚至引发重大安全事故。

2.2　信息物理融合系统软件可信性动态演化

随着 CPS 软件需求进一步多样化、新技术的不断出现、新功能的不断拓展以及人们对 CPS 软件生存性的要求进一步提高,其在内部因素及外部因素的双重作用下不断演化,可将处于开放、复杂环境中的 CPS 软件视为一个动力学系统。

在持续运行过程中,即使 CPS 软件不受任何外部因素影响,其内部缺陷也会随着时间推移不断增加,并导致其性能衰退、功能失效甚至崩溃;为了延长软件的生命周期,不但要在软件研发阶段进行严格的测试,而且需要不断地对软件进行维护、数据更新、版本升级。此外,由于 CPS 软件一般应用于安全关键系统,对可能引发事故的重大软件缺陷应为“零容忍”,反映在其可信性演化曲线上即是 CPS 软件的可信性不低于人为设置的临界点,一旦其可信性低于安全线,将自动切换为安全模式以满足最低限度的安全需求。

根据以上分析,结合非线性动力学理论,我们将 CPS 软件自身演化过程称为自然演化,将其受人为因素影响的演化过程称为人为演化,将其处于安全模式下的演化过程称为生存演化[10]。

在自然演化过程中,给定 CPS 软件的初始状态,这也就确立了一个动力系统的初态。随着时间推移,CPS 软件的可信性演化过程可用其特征属性随时间变化而形成的轨道[14]进行描述。

在人为演化过程中,加入人为因素如发布补丁、更新软件数据库等,这通常使得软件可信程度发生一个明显的变化,此种情况下,其可信性演化曲线将是一个由多个局部自然演化曲线组成的具有阶跃特性的演化曲线,人为演化对应着“类动力系统”。

在生存演化过程中,CPS 软件内部发生严重错误或遭遇高强度恶意攻击,为了保证安全关键系统最低限度的安全需求,CPS 软件将自动切换为安全模式。此模式下,CPS 软件仅实现核心功能,可信性大幅增强并能在较长时间内处于一个较稳定的状态,此时可对 CPS 软件进行人工维护、升级等操作,以提升其可信性。将这些严重影响 CPS 软件可信性的因素表示为控制参量,其可信性演化曲线将在这些控制参量的作用下出现分支(Bifurcation),这对应着动力系统中的分支理论。

3　信息物理融合系统软件可信性演化非线性动力学建模与分析

CPS 可信软件的行为演化轨迹应是有规律、可预测的。由于 CPS 软件行为难以直接观测,但其行为变化会引起与其直接相关的特征量发生相应变化,因此我们通过选取 CPS 软件的特征属性及影响 CPS 软件运行的外部因素来刻画 CPS 软件的演化规律。将所选的 CPS 软件可信性特征属性与相应外部因素作为参数[10],可以建立起与之对应的动力学模型,便于对 CPS 软件可信性的演化特性进行分析。

下面以一个应用于工业控制系统的 CPS 软件为例说明其非线性动力学建模与分析过程,该 CPS 软件同时受内部因素(终端连接数)及外部因素(病毒攻击)综合影响。

假设 i 时刻该 CPS 软件占用的网络带宽为 $x(i)$,终端连接数为 $y(i)$。软件稳定运行时,所占用的网络带宽应与上一时刻所占用的网络带宽大致相同,即 $x(i+1)\approx x(i)$;若有病毒入侵,由于入侵该软件的病毒间存在相互竞争,致使抵消的网络带宽占用量正比于 $x(i)$ 的平方,其比例系数为 a;该软件的终端用户也需占用一定的网络带宽,终端连接数与占用的网络带宽大小间的比例系数为 b,并设终端连接数与上一时刻的网络带宽占用量成正比,比例系数为 c。

由上述假设,根据非线性动力学理论与方法,结合生物模型中著名的 Logistic 映射[15],可列出相应的微分方程对该模型进行描述。为了便于计算机仿真,将该微分方程离散化,得到的模型如下:

$$\begin{cases} x(i+1)=x(i)(1-ax(i))+by(i) \\ y(i+1)=cx(i) \end{cases} \tag{1}$$

在 CPS 软件动态行为演化过程中,可通过较少次数的测试得到终端连接数与网络带宽占用量间的比例系数 b、c,而病毒间的竞争系数 a 也可通过类似方法测得。确定了参加测试的病毒及软件后,a、c 也随之确定。下面以 $a=1.6$、$c=1.5$ 为例,对上述模型进行分析。

(1)当 $0.332<b<0.346$ 时,CPS 软件行为演化趋于一个确定状态,其网络带宽占用量与终端连接数的关系较为明确,其可信性也是可以预测的,如图

1 所示;

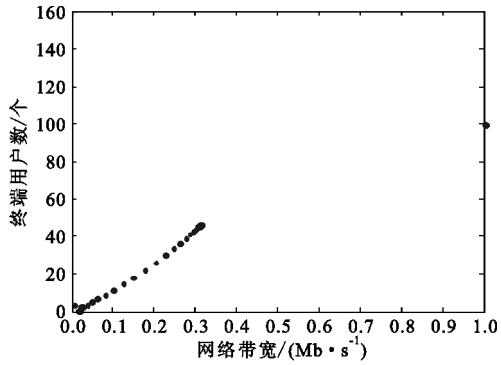

图 1 参数取 $a=1.6$、$b=0.334$、$c=1.5$ 时系统相轨图
Fig. 1 Bandwidth versus number of users when $a=1.6, b=0.334, c=1.5$

(2)当 $0.346<b<0.446$ 时,CPS 软件行为演化曲线出现分支,这意味着相关特征属性在若干状态间跳动,演化特性趋于复杂化,CPS 软件的不可信度也随之增高;

(3)当 $0.446<b<0.578$ 时,CPS 软件行为演化曲线进入了混沌状态,这意味着 CPS 软件的行为演化完全不可预测,软件行为充满了不确定性,即软件不再可信,如图 2 所示。

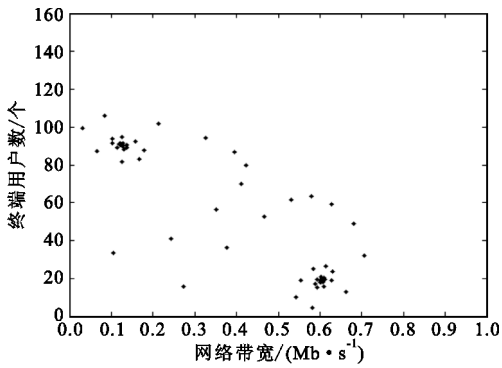

图 2 参数取 $a=1.6$、$b=0.556$、$c=1.5$ 时的系统相轨图
Fig. 2 Bandwidth versus number of users when $a=1.6, b=0.556, c=1.5$

由图 1 和图 2 可知,通过分析终端连接数与软件所占用网络带宽间的关系,该模型能够准确反映出 CPS 软件运行过程中的动态演化过程并形象地展示出来,有利于分析 CPS 软件当前状态,为 CPS 软件可信性研究提供了一种新手段。

4 总 结

本文在 CPS 可信软件相关技术的基础上,结合非线性动力学的思想与相关方法,针对 CPS 软件行为演化特性进行建模与分析,并从中导出相应判定机制:动力系统的轨道对应着 CPS 软件的行为演化过程;其分支现象则表示 CPS 软件在控制因素影响下的行为演化。利用这一方法,可通过提取 CPS 软件特征属性对其行为演化过程进行模拟仿真,为人们判断 CPS 软件是否可信提供重要支撑。

目前本文所做的仅限于 CPS 软件可信性演化分析,在实际应用中存在只能分析而无法控制的问题,接下来将进一步研究 CPS 软件可信性演化动力学模型的稳定性并着重分析在内部、外部因素影响下模型的分支现象及分支类型。

参考文献:

[1] National Science Foundation of the United States. Cyber-physical system (CPS) program solicitation [EB/OL]. [2013-10-10]. http://www.nsf.gov/pubs/2010/nsf10515/htm.

[2] 王中杰, 谢璐璐. 信息物理融合系统研究综述[J]. 自动化学报, 2011, 37(10): 1157-1166.
WANG Zhong-jie, XIE Lu-lu. Cyber-physical Systems: A Survey [J]. Acta Automatica Sinica, 2011, 37(10): 1157-1166. (in Chinese)

[3] Rajkumar R, Lee I, Sha L, et al. Cyber-Physical Systems: the Next Computing Revolution [C]//Proceedings of the 47th ACM/IEEE Conference on Design Automation. Anaheim, California, USA: IEEE, 2010: 731-736.

[4] 蒋建春, 文伟平, 张云泉. "震网"、"火焰"恶意代码警示—信息物理系统安全问题与挑战[J]. 中国计算机学会通讯, 2012, 8(7): 75-78.
JIANG Jian-chun, WEN Wei-ping, ZHANG Yun-quan. The Warning of "Stuxnet" and "flames"—Cyber-Physical Systems' Safety and Challenge [J]. Communications of the CCF, 2012, 8(7): 75-78. (in Chinese)

[5] Lee I, Sokolsky O, Chen S, et al. Challenges and Research Directions in Medical Cyber-Physical Systems [J]. Proceedings of the IEEE, 2012, 100(1): 75-90.

[6] National Workshop on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation and Rail [EB/OL]. [2013-10-10]. http://www.ee.washington.edu/reserach/nsl/aar-cps/NOC_June_2009.pdf, 2009.

[7] 王怀民, 尹刚. 网络时代的软件可信演化[J]. 中国计算机学会通讯, 2010(2): 28-35.
WANG Huai-min, YIN Gang. Software Trustworthiness Evolution in Network Era [J]. Communications of the CCF, 2010(2): 28-35. (in Chinese)

[8] 杨晓晖. 软件行为动态可信理论模型研究[D]. 合肥: 中国科学技术大学, 2010.
YANG Xiao-hui. Researches on Dynamic Trusted Theories and Models of Software Behavior [D]. Hefei: University of Science and Technology of China, 2010. (in Chinese)

[9] Bruce R A, McMillin M. Mode-Checking BNDC Properties in Cyber Physical Systems [C]//Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference. Seattle, WA, USA: IEEE, 2009: 660-663.

[10] 郑志明, 马世龙, 李未, 等. 软件可信性动力学特征及其演化复杂性[J]. 中国科学 E 辑:信息科学, 2009,39(9):946-950.
ZHENG Zhi-ming, MA Shi-long, LI Wei, et al. The Dynamic Characteristics and Complexity of Software Trustworthiness Evolution [J]. Science China (Series E), 2009, 39(9): 946-950. (in Chinese)

[11] 刘克,单志广,王戟,等."可信软件基础研究"重大研究计划综述[J]. 中国科学基金,2008(3):145-151.
LIU Ke, SHAN Zhi-guang, WANG Ji, et al, Overview on Major Research Plan of Trustworthy Software [J]. Bulletin of National Natural Science Foundation of China,2008(3):145-151. (in Chinese)

[12] 王怀民, 唐扬斌, 尹刚, 等. 互联网软件的可信机理[J]. 中国科学 E 辑:信息科学,2006,36(10):1156-1169.
WANG Huai-min, TANG Yang-bin, YIN Gang, et al. The Trustworthiness Mechanism of Network Software [J]. Science China (Series E),2006,36(10):1156-1169. (in Chinese)

[13] 张焕国, 赵波. 可信计算[M]. 武汉:武汉大学出版社, 2011.
ZHANG Huan-guo, ZHAO Bo. Trusted Computing [M]. Wuhan: Wuhan University Press,2011. (in Chinese)

[14] Smale S. Differentiable Dynamical Systems [J]. Bulletin of the American Mathematical Society, 1967, 73(6): 747-817.

[15] Benedicks M, Carleson L. On Iterations of 1 - ax2 on (-1,1)[J]. Annals of Mathematics,1985,122(1):1-25.

作者简介:

谢文军(1991—),男,江西上饶人,2012 年于长沙理工大学获工学学士学位,现为硕士研究生,主要研究方向为信息物理融合系统、可信软件;

XIE Wen-jun was born in Shangrao, Jiangxi Province, in 1991. He received the B. S. degree from Changsha University of Science and Technology in 2012. He is now a graduate student. His research concerns cyber-physical systems and trusted software.

付　晓(1975—),女,湖南临澧人,硕士,讲师,主要研究方向为信息物理融合系统;

FU xiao was born in Linli, Hunan Province, in 1975. She is now a lecturer with ths M. S. degree. Her research concerns cyber-physical systems.

于振华(1977—),男,山东乳山人,2006 年于西安交通大学获博士学位,现为副教授,主要研究方向为信息物理融合系统、可信软件;

YU Zhen-hua was born in Rushan, Shandong Province, in 1977. He received the Ph. D. degree from Xi'an Jiaotong University in 2006. He is now an associate professor. His research concerns cyber-physical systems and trusted software.

Email:zhenhua_yu@163.com

韩　林(1953—),男,河北蠡县人,教授,主要研究方向为通信指挥。

HAN Lin was born in Lixian, Hebei Province, in 1953. He is now a professor. His research concerns communication command.