·自动化技术·

具有数据包丢失的NCS反馈调度研究

何坚强，张焕春，经亚枝

(南京航空航天大学自动化学院 南京 210016)

【摘要】网络化控制系统数据包丢失会导致控制系统性能下降与网络资源利用率降低。该文分析了网络化控制系统的数据包丢失问题，基于网络利用率，采用反馈调度方法，动态调整网络化控制系统控制任务周期，在线分配网络资源，实现调度与控制的集成，提高了网络资源的利用率与控制系统性能，仿真结果表明该方法的有效性。

关 键 词 数据包丢失; 反馈调度; 网络利用率; 实时控制

中图分类号 TP273 文献标识码 A

Study on Feedback Scheduling for NCS with Packet Losses

HE Jian-qiang，ZHANG Huan-chun，JING Ya-zhi

(College of Automation Engineering, Nanjing University of Aeronautics and Astronautics Nanjing 210016)

Abstract The data packet dropout degrades the performance and network utilization of networked control system. Based on network utilization, a feedback scheduler is used to adjust the sampling periods for tasks of NCS and network resources. The integrated control-scheduling is realized and the total control performance is optimized. The emulation result shows its effective.

Key words packet losses; network utilization rate; feedback scheduling; real-time control

网络化控制系统(Networked Control Systems，NCS)的控制信息通过网络传输，由于网络阻塞、连接中断以及数据传输超时等原因，造成控制数据传输具有不确定性，使数据包在网络中传输产生时延与丢失，最终导致控制系统性能下降，甚至不稳定。网络化控制系统中各子系统控制数据以不同的周期通过网络传输，为了保证各子系统的控制性能，有效地利用控制网络，必须对各子系统实时控制任务进行调度。网络控制系统是一个涉及控制与调度的复杂系统，需要实现两者的集成。文献[1]对具有数据包丢失的NCS稳定性进行了分析，对网络调度采用了静态调度方法，尽管静态调度可以解决一些复杂特征的实时任务调度，但它们是开环的调度算法，不能根据系统的实际状态与性能动态地调整实时任务，而具有数据包丢失的实时控制系统具有随机性与不可预见性，因此开环调度用于时变和数据包丢失的NCS具有局限性。

为了得到好的控制系统性能，需要根据系统当前的状态动态调整调度策略，在线进行资源调度，因此反馈调度被引入实时调度系统中[2-4]。文献[4]研究了具有网络时延的实时系统的反馈调度问题，而数据包丢失是NCS的一个重要现象，目前对具有数据包丢失的网络调度方法少见报道。本文采用反馈调度方法对具有数据包丢失的网络化控制系统进行研究，通过在线调整实时控制任务周期，将系统资源利用率与控制系统性能有机结合，同时提高NCS的控制性能质量(Quality of Control，QoC)和网络服务质量(Quality of Service，QoS)，实现NCS的调度与控制集成。

1 数据包丢失的NCS模型

图1所示为一个具有数据包丢失的NCS结构示意图[1]。图中将NCS中的网络作为一种速率开关S_i，当S_i关闭时(S_i=1)，控制信息传输；当S_i打开时(S_i=0)，数据丢失。一个由n个子控制系统组成的NCS的集合为$L_{\text{Loop}}=\{L_{\text{Loop}_1},L_{\text{Loop}_2},\cdots,L_{\text{Loop}_n}\}$，其中子系统$L_{\text{Loop}_i}$表示为：

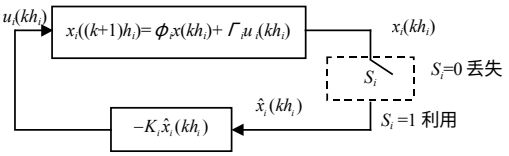

图1 数据包丢失的NCS

收稿日期：2004 - 04 - 15

作者简介：何坚强(1964 -)，男，博士生，副教授，主要从事计算机测控、实时控制、分布式控制系统方面的研究.

$$x_i((k+1)h_i)=\Phi_i x_i(kh_i)+\Gamma_i u_i(kh_i) \tag{1}$$

假设数据包的丢失率为α，则网络的关闭速率β=1−α，NCS中数据以β速率在网络中传输。

设 $\boldsymbol{z}_i(kh_i)$ 为扩展状态向量，具有数据包丢失的网络化控制系统可表示为：

$$\boldsymbol{z}_i((k+1)h_i)=\begin{bmatrix}x_i((k+1)h_i)\\ \hat{x}_i((k+1)h_i)\end{bmatrix}=\hat{\Phi}_{i,S_i}\begin{bmatrix}x_i(kh_i)\\ \hat{x}_i(kh_i)\end{bmatrix} \tag{2}$$

式中 $s_i=0,1$；$\hat{\Phi}_{i,0}=\begin{bmatrix}\Phi_i & -\Gamma_i K_i\\ \Phi_i & -\Gamma_i K_i\end{bmatrix}$；$\hat{\Phi}_{i,1}=\begin{bmatrix}\Phi_i & -\Gamma_i K_i\\ 0 & I\end{bmatrix}$。

设网络控制系统L_{Loop}扩展状态向量 $\boldsymbol{z}(k)=\left[z_1(kh_1),z_2(kh_2),\cdots,z_n(kh_n)\right]^{\mathrm{T}}$，则数据包丢失的NCS模型为：

$$z(k+1)=\hat{\Phi}(k)\cdot z(k)\ ,\ \ \hat{\Phi}(k)=\ \mathrm{diag}(\hat{\Phi}_{1,s_1},\hat{\Phi}_{2,s_2},\cdots,\hat{\Phi}_{n,s_n}) \tag{3}$$

控制子系统 L_{Loop_i} 性能指标采用时间连续二次函数表示[5]：

$$J_i=\frac{1}{h_i}E\int_0^{h_i}\left[Z_i^T(t)\quad u_i^T(t)\right]\boldsymbol{Q}_i\begin{bmatrix}Z_i(t)\\ u_i(t)\end{bmatrix}\mathrm{d}t \tag{4}$$

式中 $\boldsymbol{Q}_i$ 为正半定矩阵。网络控制系统总体性能指标 $J=\sum_{i=1}^{n}J_i=J(h_i,\alpha_i)$，NCS的性能与采样周期$h_i$和数据包丢失率$\alpha_i$有关。图2给出了一个NCS线性子系统性能指标$J_i$与$h_i$和$\alpha_i$的关系示意曲线。显然，$h_i$与$\alpha_i$增加将导致 L_{Loop_i} 系统性能下降。文献[1]分析了导致系统不稳定的数据包丢失率的限制条件，系统采用了非强占单调速率调度来实现网络调度。由于RMS是一种开环调度，不能够对数据包丢失的系统进行动态调度调整，所以，文献[1]没有对如何改善系统性能进行研究，本文采用反馈调度算法对数据包丢失的NCS进行研究。

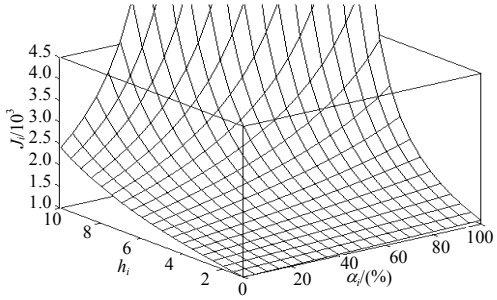

图2 J_i与h_i、α_i 的关系示意图

2 NCS的反馈调度

2.1 反馈调度结构

本文设计了图3所示的NCS反馈调度结构。该系统是在NCS的基础上，增加一个外环回路，实现对网络中数据传输信息的监控。反馈调度系统包括网络监控器、QoS控制器、调度器。反馈调度作为一个周期任务与QoC控制系统并行运行，采样周期为h_s，大于控制任务周期，具有更高的优先级。

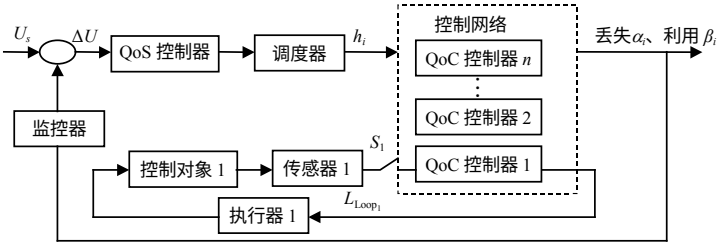

图 3 NCS 反馈调度结构

对于一组周期性控制任务的网络化控制系统，每个控制子系统的任务模型表示为 L_{Loop_i} (h_i，D_i，C_i，B_i)，其中，h_i为控制任务的传输周期；D_i为相对时限；C_i为任务传输时间；B_i为传输的阻塞时间。为了实现NCS反馈调度，对网络中传输数据进行实时监控，需要确定数据包丢失率与网络利用率。本文选用网络利用率U_s作为给定值，利用率U_s依赖于数据包的丢失率α_i与通过率β_i，数据包丢失率α_i在每个反馈调度采样周期中测出，在[(k−1)h_s，kh_s]内，$\alpha_i=\dfrac{\text{丢失数据包数}}{\text{丢失数据包数}+\text{传输数据包数}}\times 100\%$，网络的利用率 $U_i=\sum_{i=1}^{n}[(1-\alpha_i)\overline{C}_i]/h_i$。由于网络传输采用非强占方式，$\overline{C}_i$ 为包括B_i的数据平均传输时间。反馈调度选择控制任务传输周期作为操纵变量，用于在线调节各个控制任务周期，调节控制系统采样周期，同时改善NCS的QoC和QoS。网络监控器将网络传输信息反馈到控制器与给定值U_s进行比较，根据偏差对控制任务的传输周期进行调整，控制

任务新周期调整为 $h_i' = h_i(U_i / U_s)$，实时任务调度通过基本调度器实现。

2.2　反馈调度方法

基于网络利用率的反馈调度系统，网络利用率的设定必须满足可调度条件。对于采用单调速率调度的网络：$U_s = \sum_{i=1}^{n} \overline{C}_i / h_i \le i(2^{1/i} - 1)$。为了对传输时间进行快速评估，引入了遗忘因素$\lambda$[5]，则实时任务传输时间为：

$$\hat{C}(kh_s) = \lambda \hat{C}((k-1)h_s) + (1-\lambda)\overline{C}(kh_s)$$

当α_i=0时，网络无数据包丢失，控制信息100%传输，网络利用率 $U = \sum_{i=1}^{n} \hat{C}_i / h_i$，$\Delta U$=0，反馈调度器保持原调度参数不变，NCS各子系统采样周期为h_i。当$\alpha_i \neq 0$，由于部分控制信息丢失，对应于每个反馈调度周期h_s，网络的利用率为：

$$U(kh_s) = \sum_{i=1}^{n} [(1-\alpha_i)\hat{C}_i(kh_s)] / [h_i((k-1)h_s)] \tag{5}$$

式中　$h_i(kh_s)$ 为分配到控制任务i的采样周期；$\hat{C}_i(kh_s)$ 为每个周期控制任务的传输时间。由于$U \neq U_s$，QoS控制器对控制任务周期进行重新分配，新控制任务周期为：

$$h_i' = h_i((k-1)h_s)\frac{U(kh_s)}{U_s} \tag{6}$$

调度器根据新任务周期对NCS各个控制子系统进行重新调整分配。数据包丢失率α_i的增加导致网络利用率降低，动态调整相应控制任务周期，使得 h_i' 减少，从而提高了网络利用率 $U(kh_s)$，优化了网络化控制系统性能，新控制任务周期的调整必须满足网络可调度条件。

3　仿真研究

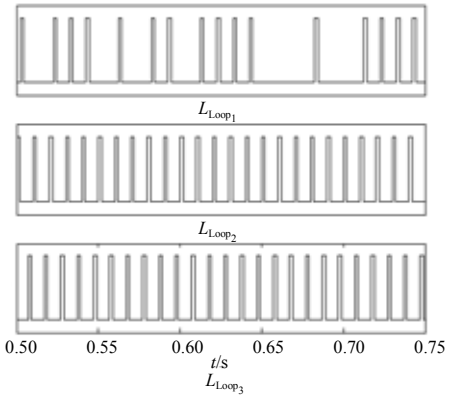

图4　数据包丢失的NCS调度(α_1=30%)

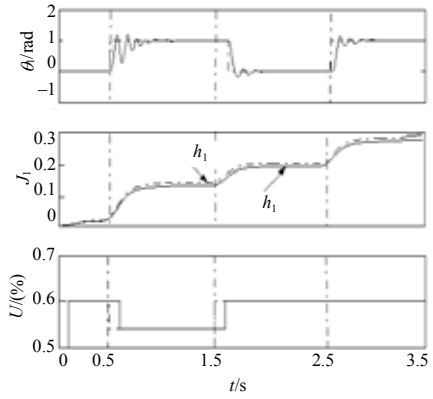

图5　反馈调度结果

仿真以三个直流伺服电动机控制系统构成的网络控制系统为例，在有、无数据包丢失状态下分别对周期性控制任务进行仿真研究。伺服电动机控制对象描述为 $G(s) = k/(s^2 + s)$，k为1 000，三个控制子系统相互独立，控制任务采用单数据包方式传输。假设每个控制任务数据包平均传输时间为2 ms，三个子系统周期性控制任务的传输周期h_i (i=1,2,3)分别为10、12和12 ms，反馈调度周期为120 ms，控制回路采用PID控制方法，设定网络控制系统控制网络资源网络利用率为60%。

仿真采用Truetime工具箱，分别对有、无数据包丢失的网络控制系统进行实验。无数据包丢失时，网络化控制系统保持系统原有性能不变。当任务执行到0.5 s时，设控制回路 L_{Loop_1} 数据包丢失率α_1=30%，则控制网络利用率降低为54%，反馈调度器根据式(6)重新调整控制系统任务周期，控制系统新的任务周期 h_i' (i=1,2,3)分别为9、10.8和10.8 ms，图4为NCS的网络调度曲线，图5分别给出了控制回路 L_{Loop_1} 伺服电机角位移输出响应曲线、控制回路 L_{Loop_1} 反馈调度性能比较与控制网络资源利用率变化曲线，实验结果表明反馈调度可以改善系统性能。

(下转第822页)

洞间推理关系建立该主机的有色加权有向图G_A，如图3所示。依据E_A的漏洞日志关联矩阵$\boldsymbol{M}$，利用forensic算法遍历G_A中的漏洞并进行日志信息查找，得日志信息支持度矩阵$\boldsymbol{D}$，计算 $\chi_i = |\boldsymbol{\varphi}_i \times \boldsymbol{d}_i|$，与根据经验值设置的阈值比较后对图$G_A$进行剪枝得图 C'_A，如图4所示。从 C'_A 得漏洞攻击链(e_1,e_5,e_6,e_7)，其中e_1属于远程操作类型，查找e_1相关网络日志，可知内网Linux攻击者主机存在远程操作嫌疑。分析SUNOS和Solaris，可得相同结论。(2) 检查内网Linux攻击者，构建其有色加权有向图并分析得其漏洞攻击链，可有效地分析出外网Linux攻击者主机存在远程攻击嫌疑，且该主机即为攻击机。实验结果符合实验预期。

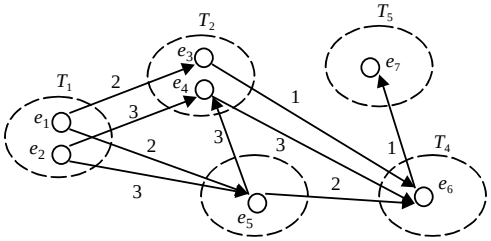

图3 主机B有色加权有向图G_A

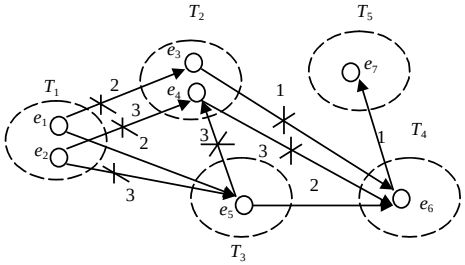

图4 剪枝后的主机B有色加权有向图 G'_A

4 结 束 语

目前，针对网络攻击过程的分析多集中于对攻击过程的某些具体问题的研究，如文献[2]采用静态漏洞链构造分析攻击过程，漏洞链数目庞大，冗余操作多，降低了分析效率；文献[3]采用因果推理入侵检测报警信息重构攻击过程，依赖存在漏报和误报的入侵检测系统，信息源缺乏准确性；文献[4]采用程序性推理，通过与攻击过程模板相匹配建立整个网络的攻击过程，缺乏对新的未知攻击的分析和识别。与以上方法相比，本文提出的动态漏洞链构造推理分析方法执行效率高，采用多信息源信息查找、分析攻击过程，准确、完整，且插件的运用使该方法具有良好的可扩展性，可对大规模网络攻击过程进行分析、识别和取证。

参 考 文 献

[1] MIT Lincoln Lab. 2000 DARPA intrusion detection scenario specific datasets[DB/OL]. http://www.11.mit.edu/IST/ideval/data/2000/2000_data_index.html, 2004-09-30.
[2] Sheyner O, Haines J, Somesh J, et al. Automated generation and analysis of attack graphs[C]// Proceddings of the 2002 IEEE symposium on security and privacy, Oakland, 2002.
[3] Peng Ning, Yun Cui, Douglas S R, et al. Constructing attack scenarios through correlation of intrusion alerts[C]// 9th ASM Conference on Computer & Communications Security, Washington, D.C., 2002.
[4] Douglas B M, Marbry T, Pauline B, et al. Diagnosis, explanation and recovery from computer break-ins[DB/OL]. http://www.ai.sri.com/~derbi/, 2004-09-30.

编 辑 熊思亮

(上接第793页)

4 结 束 语

反馈调度可以实现数据包丢失与网络时延等不确定环境的在线调度，本文利用实时控制任务周期与QoC周期的一致性特点，动态调整控制任务周期，实现控制与调度集成，同时提高了网络资源的利用率与控制系统性能。为了改善反馈调度性能，网络资源利用率的准确评估有待于进一步研究，如何将网络化控制系统中QoS回路与QoC控制回路有机地结合，还需要深入研究。

参 考 文 献

[1] Branicky M S, Phillips S M, Zhang Wei. Scheduling and feedback co-design for networked control systems[C]//Proc. IEEE on Decision and Control, Las Vegas, 2002, 2: 1211-1217.
[2] Stankovic J A, He Tian, Abdelzaher T F, et al. Feedback control scheduling in distributed real-time systems[C]// IEEE Real-Time Systems Symposium, London, UK, 2001: 712:724.
[3] Eker J, Hagander P, Årzén K E. A feedback scheduler for real-time control tasks[J]//Control Engineering Practice, 2000, 8(12): 1369-1378.
[4] Sename O, Simon D, Robert D. Feedback scheduling for real-time control of systems with communication delays[C]//9th IEEE International Conference on Emerging Technologies and Factory Automation, Lisbonne, 2003: 375-383.
[5] Cervin A. Integrated control and real-time scheduling[D]. Sweden: Lund Institute of Technology, 2003.

编 辑 漆 蓉