航 空 学 报
Acta Aeronautica et Astronautica Sinica
Aug. 25 2011 Vol. 32 No. 8 1461-1468
ISSN 1000-6893 CN 11-1929/V
http://hkxb.buaa.edu.cn hkxb@buaa.edu.cn
文章编号:1000-6893(2011)08-1461-08

基于传输性能降级约束的机载网络可靠性研究

张勇涛, 黄臻, 熊华钢*
北京航空航天大学 电子信息工程学院, 北京 100191

摘 要:为提高因出现故障而导致网络设备资源不足时机载网络的可靠性,定义了两种机载网络传输性能降级约束,降级约束使用3个参数精确描述机载网络中消息实例传输成功或失败的数量及其分布。提出动态失效、关键函数和最小确定性将来序列等概念来对网络传输性能降级约束进行理论分析:通过计算关键函数值预先确定下一条消息实例传输失败是否会产生动态失效;使用最小确定性将来序列确定在不发生动态失效时将来消息实例传输成功的最少数量。给出两种实施约束的策略:消息源节点静态过滤和网络动态仲裁。提出一种适用于网络动态仲裁策略的调度算法:基于网络传输性能降级约束的双层优先级调度,该算法利用关键函数的预判性来避免动态失效;分析了该算法的可调度性条件。理论分析和仿真表明,当机载网络设备资源不足时,通过实施网络传输性能降级约束可以把网络性能降级的程度限制在可控范围内,从而增强机载网络的可靠性。

关键词:航空电子;可靠性;网络性能;降级;可调度性分析;动态失效

中图分类号:V247;TP393 **文献标识码**:A

飞行器的机动性强,运行环境恶劣,机载网络的可靠性关系到航空电子系统中任务的顺利实现,更关系到飞行器本身的生存与否,因此机载网络的可靠性至关重要。通常对网络设备进行充分的冗余备份是最可靠的策略,目前对机载网络可靠性的研究也集中在如何进行冗余备份[1-2]。但机舱内空间有限,且飞行器对载荷重量也有严格的限制,不宜大量备份网络设备,因此当部分网络设备出现故障或被摧毁时,机载网络将无足够网络设备可用,此时可用网络设备的负载率必将增加,从而造成机载网络传输性能下降。如果没有预先定量约束性能降级的程度,传输性能降级对整个航空电子系统产生的影响将是无法预料的。这种不可预知的网络传输性能降级可导致灾难性后果,为避免这种危险,有必要约束和量化分析机载残存网络传输性能降级的程度,从而把网络性能的降级对整个航空电子系统产生的影响预先限制在可控范围内。

网络传输性能指网络正确实时传输航电消息的能力,即航电消息通过网络在其截止期限内到达目的节点,且无错误的数量占所有需要传输的航电消息总量的百分比,正常情况下其为100%。如果网络无法确保所有航电消息在其截止时间内无错误地到达目的节点,则称机载网络传输性能降级。

在实际工程背景中,即使在硬实时网络系统中,偶尔的消息传输失败是可以容忍的。因为系统具有健壮性,偶尔发生消息实例传输失败不会对系统造成灾难性影响,或者虽然偶尔的消息实例传输失败会引起系统性能降低,但仍能满足特

收稿日期:2010-12-07;**退修日期**:2011-03-25;**录用日期**:2011-04-18;**网络出版时间**:2011-04-27 16:00:52
网络出版地址:www.cnki.net/kcms/detail/11.1929.V.20110427.1600.003.html **DOI**:CNKI:11-1929/V.20110427.1600.003
基金项目:国家自然科学基金(61073012)
* **通讯作者**.Tel.:010-82317202 E-mail:hgxiong@ee.buaa.edu.cn

引用格式:张勇涛,黄臻,熊华钢. 基于传输性能降级约束的机载网络可靠性研究[J]. 航空学报,2011,32(8):1461-1468. Zhang Yongtao, Huang Zhen, Xiong Huagang. Study on network reliability in avionics based on performance degradation constraints[J]. Acta Aeronautica et Astronautica Sinica, 2011, 32(8): 1461-1468.

定的应用需求。但是“偶尔失败”是一种很模糊的描述，文献[3]首先提出了(m,k)-firm 概念试图定量地描述“偶尔失败”。(m,k)-firm 表示：在连续 k 次任务调用中，至少要有 m 次调用成功完成。为了满足(m,k)-firm 约束，系统使用一种动态的尽力服务调度算法——当任务接近违反约束时，就在最后 k 次调用时提升任务的优先级；文献[4]建立了分析模型来评估系统不满足(m,k)-firm 约束的概率；文献[5]～文献[9]在(m,k)-firm 约束框架下设计调度算法，并分析系统的服务质量；文献[10]和文献[11]中提出了弱硬实时概念，作者通过定义“弱硬实时”约束来描述“偶尔失败”；文献[12]中提出了一种动态判定是否满足弱硬实时约束的方法；文献[13]提出了一种新的弱硬实时约束；文献[14]提出了几种保证弱硬实时约束的调度算法；文献[15]讨论了在弱硬实时约束下，如何对离散事件系统进行优化，但(m,k)-firm 与弱硬实时约束都没有对任务失败的数量和分布同时进行精确的描述。

本文在上述研究的基础上，结合机载网络的特定应用需求，从性能降级的角度研究网络设备资源不足条件下机载网络的可靠性，从而把网络性能的降级对整个航空电子系统产生的影响预先限制在可控范围内。

1 μ 序列

如果消息实例在其截止期限内到达目的节点，则称消息实例传输成功；虽然消息实例到达目的节点，但消息实例总延迟而超过截止期限制，则为传输失败。

消息实例是否传输成功可由“0”、“1”组成的二进制序列进行描述，本文称这种二进制序列为消息的 μ 序列，下面对其进行形式化定义。

定义 1(μ 序列) 消息的 μ 序列 α 是由 $\Delta=\{0,1\}$组成的二进制序列，“1”代表消息实例传输成功，“0”代表传输失败，l_α 为 α 的长度，$\alpha(i)\in\Delta(1\leqslant i\leqslant l_\alpha)$。$\alpha(a..b)(a\geqslant 1,b\leqslant l_\alpha)$为 α 从 a 到 b 的子序列，也称 $\alpha(a..b)$为一个窗口或子窗口。

例如，μ 序列“110011”的长度是 6，它有 3 个长度为 4 的子窗口：{1100，1001，0011}，其中“0011”是最新的子窗口。

2 网络传输性能降级约束

只用一个参数无法精确描述航空电子系统对消息传输失败的容忍度，例如，仅使用百分比描述系统对消息传输失败的容忍度是不充分的，如果要求消息传输失败不超过 10%，仅仅表示消息的平均传输失败率不超过 10%，在 100 次消息实例传输中，可能连续 10 次传输中有一次失败，也可能前面 90 次传输全部成功，而最后 10 次传输全部失败，这两种情况对系统造成的影响有很大不同。为精确描述消息传输失败的分布，引入窗口约束，即把系统对消息传输失败的容忍度约束在任意连续的 w 次传输窗口内。

消息实例的连续性传输失败和非连续性传输失败对航空电子系统造成的影响是不同的，航空电子系统对消息实例连续性传输失败非常敏感，如果相同数量的消息实例非连续地传输失败，系统很可能不受影响。与消息传输失败的分布相对应的是消息传输成功的分布，在航空电子系统中，若某一消息实例传输失败，为弥补此次失败对系统造成的影响，之后必须连续多次成功传输。综合连续性传输成功和连续性传输失败两种因素，定义以下两种类型的约束。

定义 2(网络传输性能降级约束$\langle n,w,p\rangle$和$\langle \bar{n},w,p\rangle$)

$\langle n,w,p\rangle$：在任意连续 w 条消息实例的传输窗口中，至少有连续 n 条消息实例传输成功，且消息实例的传输成功率不低于 p，其中，w 为约束的窗口长度，$2n\leqslant w$，$\dfrac{2n}{w}\leqslant p<1$。

$\langle \bar{n},w,p\rangle$：在任意连续 w 条消息实例的传输窗口中，至多有连续 n 条消息实例传输失败，且消息实例的传输成功率不低于 p，其中 $p\leqslant\dfrac{w-n}{w}$。

定义 3 α 是一个 μ 序列，且 $l_\alpha\geqslant w$，λ 是一个窗口长度为 w 的网络传输性能降级约束，如果 α 的任意一个长度为 w 的子窗口都满足 λ，则称序列 α 满足 λ，记为 $\alpha\vdash\lambda$。

例如，对于弱硬实时约束$\langle 5,20,0.8\rangle$，如果 μ 序列 α 的任意一个长度为 20 的子窗口都至少包含 5 个连续的“1”，且“1”的总数至少为 16，则 $\alpha\vdash\langle 5,20,0.8\rangle$。

定义 4(动态失效) α 是一个 μ 序列,且 $|\alpha|\geqslant w$,λ 是一个窗口长度为 w 的网络传输性能降级约束,如果 α 存在一个长度为 w 的子窗口 $\alpha(a+1..a+w)$ 不满足约束 λ,则称 α 是动态失效的,子窗口 $\alpha(a..a+w)$ 为动态失效窗口。

推论 1 约束为 $\langle n,w,p\rangle$ 或 $\langle \bar{n},w,p\rangle$ 的消息,在无动态失效发生时,此消息的成功传输率至少是 p。

证明 由约束的定义和动态失效的定义得证。

定义 5(历史 μ 序列和将来 μ 序列) 历史 μ 序列记录的是已经传输的消息实例的传输状态,将来 μ 序列则描述对将来要传输的消息实例的传输状态的期望或估计。

在任何时刻,都可以同时使用历史 μ 序列与将来 μ 序列来描述消息的传输状态。

定理 1 如果 λ 是一个窗口为 w 的传输性能降级约束,μ 序列 α 的长度为 l_α,$l_\alpha\geqslant w$;且 $\alpha\vdash\lambda$,$c\in\Delta$,联合序列 $\alpha'=$"αc",如果 α' 最新的一个子窗口 $\alpha'(l_\alpha-w+2..l_\alpha+1)$ 满足约束 λ,则 $\alpha'\vdash\lambda$。

证明 α' 除了最新的长度为 w 的子窗口以外,其他长度为 w 的子窗口与 α 长度为 w 的子窗口相同。

3 关键函数

为预先确定下一条消息实例传输失败是否会产生动态失效,定义关键函数来度量消息历史 μ 序列与动态失效之间的距离。

定义 6(关键函数) λ 是一个窗口为 w 的网络传输性能降级约束,α 是一个长度为 l_α 的历史 μ 序列,且 $l_\alpha\geqslant w$,α 基于约束 λ 的关键函数 $f_\lambda(\alpha)$:$\Delta^w\to\mathbf{Z}$ 有如下性质:

(1) $f_\lambda(\alpha)=0$ 表示此刻为关键时刻,若下一条消息实例传输失败则将产生动态失效,若下一条消息实例传输成功则将避免动态失效。

(2) $f_\lambda(\alpha)>0$ 表示即使下一条消息实例传输失败也不会产生动态失效,且在不发生动态失效的前提下,此后最多可允许 $f_\lambda(\alpha)$ 条消息实例传输失败。

(3) $f_\lambda(\alpha)<0$ 表示即将发生动态失效,即使此后所有消息实例都传输成功,动态失效仍不可避免,其绝对值 $|f_\lambda(\alpha)|$ 表示从此刻起,由历史 μ 序列 α 引起的不可避免的动态失效窗口数量。

定理 2 α 是一个长度为 l_α 的历史 μ 序列,且 $l_\alpha\geqslant w$,则

(1)

$$f_{\langle n,w,p\rangle}(\alpha)=\begin{cases}\min(I_n(\alpha)-n,N_{\bar{p}}) & I_n(\alpha)\geqslant n,P_w\geqslant p\\ \min(I_n(\alpha)-n+c(1,s(w,n,\alpha)),-N_p+1) & I_n(\alpha)<n,P_w<p\\ -N_p+1 & I_n(\alpha)\geqslant n,P_w<p\\ I_n(\alpha)-n+c(1,s(w,n,\alpha)) & I_n(\alpha)<n,P_w\geqslant p\end{cases}$$

是 α 基于约束 $\langle n,w,p\rangle$ 的关键函数。

(2)

$$f_{\langle \bar{n},w,p\rangle}(\alpha)=\begin{cases}\min(n-c(0,\alpha),N_{\bar{p}}\} & c(0,\alpha)\leqslant n,P_w\geqslant p\\ n-w+1 & c(0,\alpha)>n,P_w\geqslant p\\ -N_p+1 & c(0,\alpha)\leqslant n,P_w<p\\ \min(-N_p+1,n-w+1) & c(0,\alpha)>n,P_w<p\end{cases}$$

是 α 基于约束 $\langle \bar{n},w,p\rangle$ 的关键函数。

其中:

$P_w=\sum_{i=2}^{w}\alpha(i)/w$。

$N_{\bar{p}}=\max\left(x\left|\sum_{i=x+1}^{w}\alpha(i)\right/w\geqslant p,1\leqslant x\leqslant w-1\right)$,表示此刻以后最多可以有连续 $N_{\bar{p}}$ 条消息传输失败,若多于 $N_{\bar{p}}$ 条消息传输失败,则将有窗口不再满足最低传输成功率要求。

$N_p=\min\left(x\left|\left(\sum_{i=x+1}^{w}\alpha(i)+x\right)\right/w\geqslant p,1\leqslant x\leqslant w-1\right)$,表示后面至少要有连续 N_p 条消息传输成功,才能使后面窗口满足最低传输成功率要求。

$c(e,\alpha)=\max\{z\mid\alpha(w-z+1..w)=e^z\}$,表示序列 α 的最右边连续出现符号"e"的个数,其中 $e\in\Delta$。

$$I_n(\alpha)=\begin{cases}\max\{i\mid\alpha(i..i+n-1)=1^n\} & 1^n\in\alpha\\ 0 & \text{Otherwise}\end{cases},$$

表示序列 α 中最右边的子序列 1^n 在 α 中的起始位置。

$s(w,n,\alpha)=\alpha(w-n+I_n(\alpha)+1..w)$，表示序列 α 最右边长度为 $n-I_n(\alpha)$ 的子序列。

证明

(1) 如下两种原因都将引起动态失效：①不满足最低成功传输率要求；②不存在子序列 1^n。这两种原因也将决定关键时刻的到来：原因①引起的关键时刻称为关键时刻 I；原因②引起的关键时刻称为关键时刻 II。

情况 1：在 $P_w \geqslant p$ 时，由 P_w 的定义可知 $\alpha(2..w)$ 已经满足最低成功传输率要求，即使下一条消息实例传输失败，也不会违反最低成功传输率约束，因此 $N_{\bar{p}}$ 表示与关键时刻 I 的距离，即连续 $N_{\bar{p}}$ 条消息实例传输失败后，才会到达关键时刻 I。

情况 2：在 $P_w<p$ 时，若 $N_p=1$，则由 N_p 定义可知，此时已经到达关键时刻 I。若 $N_p>1$，则即使将来 μ 序列 β 全部为“1”，记 $\gamma=$“$\alpha\beta$”，窗口 $\gamma(2..w+2)$，$\gamma(3..w+3)$，…，$\gamma(N_p..w+N_p)$ 仍为动态失效窗口，共 $|-N_p+1|$ 个动态失效窗口。

情况 3：如果在 $I_n(\alpha)=n$ 时下一条消息实例传输失败，则将来 μ 序列 $\beta=$“0…”。记 $\gamma=$“$\alpha\beta$”，则 $\gamma(n+1..n+w)$ 必为动态失效窗口，即使以后所有消息实例全部传输成功也不可避免。如果在 $I_n(\alpha)=n$ 时下一条消息实例传输成功，则将来 μ 序列 $\beta=$“1…”，此后最多需要连续 $n-1$ 条消息实例传输成功即可以避免动态失效。例如，对于约束〈3，10，0.7〉和 $\alpha=$“1111101010”，如果 $\beta=$“0…”，则 $\gamma=$“1111101010|0…”，此时即使后面所有消息实例全部传输成功，$\gamma(n+1..n+w)=$“1101010|011”仍为动态失效窗口；如果 $\beta=$“1…”，则 $\gamma=$“1111101010|1…”，此时只需后面连续 $n-1=2$ 条消息实例传输成功，即 $\gamma(n+1..n+w)=$“1101010|111”，就可避免动态失效。因此 $I_n(\alpha)=n$ 时到达关键时刻 II。

$I_n(\alpha)>n$ 时，$I_n(\alpha)-n$ 表示距离关键时刻 II 的距离，即连续 $I_n(\alpha)-n$ 条消息实例传输失败后，才会到达关键时刻 II。

情况 4：如果在 $I_n(\alpha)<n$ 时 α 最右边长度为 $n-I_n(\alpha)$ 的子序列全为“1”，那么若下一条消息实例传输失败，则将来 μ 序列 $\beta=$“0…”。记 $\gamma=$“$\alpha\beta$”，则 $\gamma(I_n(\alpha)+1..I_n(\alpha)+w)$ 必为动态失效窗口，即使此后所有消息实例全部传输成功也不可避免。若此情况下，下一条消息实例传输成功，则将来 μ 序列 $\beta=$“1…”，此刻以后最多需要连续 $I_n(\alpha)-1$ 条消息实例全部传输成功，即可以避免动态失效。因此 $I_n(\alpha)-n+c(1,s(w,n,\alpha))=0$ 时也到达关键时刻 II。例如，对于约束〈3，10，0.7〉和 $\alpha=$“1111010101”，$I_n(\alpha)=2$，α 最右边长度为 $I_n(\alpha)-1=2-1=1$ 的子序列全为“1”，如果 $\beta=$“0…”，$\gamma=$“1111010101|0…”，则即使此刻以后所有消息实例全部传输成功，$\gamma(I_n(\alpha)+1..I_n(\alpha)+w)=$“11010101|01”仍为动态失效窗口；如果 $\beta=$“1…”，$\gamma=$“1111010101|1…”，则只需后面连续 $I_n(\alpha)-1=1$ 条消息实例传输成功，即 $\gamma(I_n(\alpha)+1..I_n(\alpha)+w)=$“11010101|11”，即可避免动态失效。如果 $I_n(\alpha)-n+c(1,s(w,n,\alpha))<0$，则即使将来 μ 序列全部为“1”，仍会有 $|I_n(\alpha)-n+c(1,s(w,n,\alpha))|$ 个动态失效窗口。

综合以上 4 种情况可知 $f_{\langle n,w,p\rangle}(\alpha)$ 是 α 基于约束〈n，w，p〉的关键函数。

(2) 如下两种原因都将引起动态失效：①不满足最低成功传输率要求；②存在子序列 0^{n+1}。这两种原因也将决定关键时刻的到来：原因①引起的关键时刻称为关键时刻 I；原因②引起的关键时刻称为关键时刻 II。

情况 1 和情况 2 与(1)中情况 1 和情况 2 相同。

情况 3：如果在 $c(0,\alpha)=n$ 时下一条消息实例传输失败，则将来 μ 序列 $\beta=$“0…”。记 $\gamma=$“$\alpha\beta$”，则 $\gamma(n+1..n+w)$ 中必将存在子序列 0^{n+1}，因此必为动态失效窗口。如果在 $c(0,\alpha)=n$ 时下一条消息实例传输成功，则将来 μ 序列 $\beta=$“1…”，$\gamma(n+1..n+w)$ 中将不存在子序列 0^{n+1}，从而避免了动态失效。因此 $c(0,\alpha)=n$ 时到达关键时刻 II。$c(0,\alpha)<n$ 时，$n-c(0,\alpha)$ 表示距离关键时刻 II 的距离，即连续 $n-c(0,\alpha)$ 条消息实例传输失败后，才会到达关键时刻 II。

情况 4：$I_n(\alpha)>n$ 时，记 $\gamma=$“$\alpha\beta$”，即使将来 μ 序列 β 全部为“1”，窗口 $\gamma(2..w+2)$，$\gamma(3..w+3)$，…，$\gamma(w-n..w+w-n)$ 中也必包含子序列 0^{n+1}，因此仍会有 $|n-w+1|$ 个动态失效窗口。

综合以上 4 种情况可知 $f_{\langle n,w,p\rangle}(\alpha)$ 是 α 基于

约束$\langle\bar{n},w,p\rangle$的关键函数。

4 最小确定性将来μ序列

本节引入确定性将来μ序列来描述对将来消息实例传输状态的期望。

定义7(确定性将来μ序列) λ是一个窗口为w的网络传输性能降级约束,α是一个长度为1的历史μ序列,β是将来μ序列,如果$\alpha=$"1"时,联合μ序列$\gamma=$"$\alpha\beta$"满足λ,即$\gamma\vdash\lambda$,则称β为基于约束λ的确定性将来μ序列。

确定性将来μ序列描述消息将来传输状态与起始传输状态之间的兼容性,兼容性表示无动态失效发生,例如,序列"1^w"是适用于任何约束的确定性将来μ序列。在所有的确定性将来μ序列中,我们将关注包含最少"1"的序列。

定义8(最小确定性将来μ序列) λ_i是基于约束P_i的确定性将来μ序列,如果将μ中任何一个"1"改为"0",μ将不再是基于约束μ的确定性将来τ_i序列,称λ_i为基于约束μ的最小确定性将来η_λ序列。

最小确定性将来μ序列描述在不发生动态失效时将来消息实例传输成功的最少数量。

定理3

(1)

$$\begin{cases}\eta_{\langle n,w,p\rangle}=\text{“}\omega\omega\cdots\text{”}\\ \omega=\underbrace{\overbrace{11\cdots1}^{n}\overbrace{00\cdots0}^{N_0}\overbrace{11\cdots1}^{N_1-2n}\overbrace{11\cdots1}^{n}}_{w}\end{cases}$$

是基于约束$\langle n,w,p\rangle$的最小确定性将来μ序列。

(2)

$$\begin{cases}\eta_{\langle\bar{n},w,p\rangle}=\text{“}\omega_1\ \omega_1\cdots\text{”}\\ \omega_1=\underbrace{\overbrace{11\cdots1}^{N_1-k_{\bar{n}}-1}1\overbrace{00\cdots0}^{n}1\overbrace{00\cdots0}^{n}\cdots1\overbrace{00\cdots0}^{n}1\overbrace{00\cdots0}^{N_0-nk_{\bar{n}}}}_{w}\\ \qquad\qquad\qquad\underbrace{\qquad\qquad\qquad\qquad}_{1}\ \underbrace{\qquad\qquad}_{2}\qquad\underbrace{\qquad\qquad}_{k_{\bar{n}}}\end{cases}$$

是基于约束$\langle\bar{n},w,p\rangle$的最小确定性将来$\mu$序列。其中:

$N_1=\min\left(N\left|\frac{N}{w}\geqslant p\right.\right)$,表示长度为$w$的序列中"1"的最少数量。

$N_0=w-N_1$,表示长度为w的序列中"0"的最大数量。

$k_{\bar{n}}=\left\lfloor\frac{N_0}{n}\right\rfloor$,$\lceil x\rceil$表示对$x$进行向下取整。

证明 (1)由于$\gamma=$"$1\eta_{\langle n,w,p\rangle}$",且$\eta_{\langle n,w,p\rangle}$是循环序列,所以$\gamma$所有长度为$w$的子窗口都包含在前$w+1$个长度为$w$的子窗口中,通过逐一检查$\gamma$的前$w+1$个长度为$w$的子窗口可得其全部满足约束$\langle n,w,p\rangle$,因此$\gamma\vdash\langle n,w,p\rangle$;同理可证明,如果将$\eta_{\langle n,w,p\rangle}$中任何一个"1"改为"0",则序列$\gamma$至少存在一个长度为$w$的子窗口不满足约束$\langle n,w,p\rangle$。(2)证明同上。

5 约束实施策略

本节给出两种实现约束的策略,当网络设备资源不足时,可根据机载网络的拓扑类型(如总线型或交换型)或应用需求确定选择使用何种策略。

5.1 消息源节点静态过滤策略

消息实例未发送到网络前,在消息源节点预先根据约束进行过滤,然后才将消息发送到网络中,此方法适用于所有拓扑类型的机载网络,且只需在消息发送节点加入约束过滤功能模块,在需要实施约束时启用此模块,易于实现。过滤模块根据约束的最小确定性将来序列对消息实例进行过滤,发送最少数量的消息实例到网络中进行传输。但此策略对网络的最坏情况估计过于悲观,不能充分利用网络资源尽量提升网络性能。

5.2 网络动态仲裁策略

消息发送节点将所有消息实例都发送到网络中,网络转发节点根据消息的历史传输状态动态选择要转发的消息实例,从而满足降级约束。此方法可适用于交换型或者集中调度型的机载网络,并能充分利用现有的网络资源尽量提升网络性能,但需要设计基于约束的调度算法,第6节提出一种基于网络传输性能降级约束的双层优先级调度算法,来支持网络动态仲裁策略的实施。

6 基于网络传输性能降级约束的双层优先级调度算法

负载加重时,如果消息延迟增加但仍满足截止时间要求,则按正常情况进行调度,若已不满足截止时间要求,则以传输错误进行处理,启用基于传输性能降级约束的双层优先级调度算法。

同时利用历史$\langle\bar{2},10,0.6\rangle$序列和最小确定性将来$\mu$序列是此调度算法的关键,利用历史$\mu$序

列的关键函数动态确定队列中消息实例的状态，利用最小确定性将来 μ 序列进行可调度性分析。

6.1 调度模型和算法思想

调度模型如图 1 所示，消息集 Π 中的所有消息竞争同一个输出端口，调度器根据调度算法选择下一条消息的输出。每个消息 $\tau_i(1\leqslant i\leqslant N)$ 通过如下特征进行描述：消息周期或最小到达间隔 G_i，相位 Θ_i，截止时间 D_i，传输时间 C_i，网络传输性能降级约束 λ_i，消息优先级 P_i 和历史 μ 序列 α_i；即 $\Pi=\{\tau_i=(G_i,\Theta_i,D_i,C_i,\lambda_i,P_i,\alpha_i)\}_{1\leqslant i\leqslant N}$。此时调度器的负载率为

$$R_{\text{load}}=\sum_{i=1}^{N}\frac{C_i}{G_i}\times 100\%$$

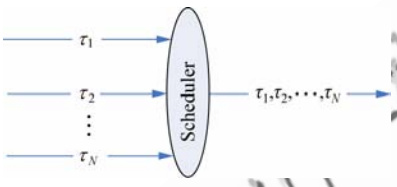

图 1 调度模型

Fig. 1 Scheduling model

对于消息 τ_i，λ_i 是窗口长度为 w 的约束，α_i' 是 α_i 最新的一个长度为 w 的子序列，当 τ_i 的消息实例在队列中等待传输时，根据如下条件赋予消息实例不同的状态：① $f_\lambda(\alpha_i')>0$，赋予正常状态；② $f_\lambda(\alpha_i')=0$，赋予关键状态；③ $f_\lambda(\alpha_i')<0$，赋予紧急状态。

基于网络性能降级约束的双层优先级调度算法，根据消息实例的状态优先调度处于紧急状态的消息实例，在没有紧急状态的消息实例等待传输时调度关键状态的消息实例，在没有紧急状态和关键状态的消息实例等待传输时，才调度处于正常状态下的消息实例。处于相同状态下的不同消息实例，根据消息的优先级进行调度，并丢弃排队延迟已超过其截止期限的消息实例。

6.2 可调度性分析

引理 1 在消息历史 μ 序列的第 1 个长度为 w 的子窗口满足约束时，若调度算法能确保以后处于关键状态的消息实例全部传输成功，则调度算法确保无动态失效发生，且不会出现紧急状态的消息实例。

证明 由关键函数的性质 1 可得出结论。

此定理表示仅在发生动态失效时，才会产生处于紧急状态的消息实例，即只有在消息集不可调度时才会出现紧急状态的消息，因此在分析算法的可调度性时，不需要考虑紧急状态的消息实例。

引理 2 负载为消息集 Π 的调度器使用基于网络传输性能降级约束的双层优先级调度算法，对于任意 $\tau_i\in\Pi$，其最小确定性将来 μ 序列为 η_λ^i，则有

(1) 如果 τ_i 处于关键状态，则在长度为 t 的时间窗口内，τ_i 对低优先级的消息造成的最大延迟为

$$T_i(t)=\sum_{j=1}^{k}\eta_\lambda^i(j)C_i,\quad k=\left\lceil\frac{t}{G_i}\right\rceil$$

式中："$\lceil\cdot\rceil$"表示向上取整。

(2) τ_i 在关键状态下的最大延迟为

$$d_i=C_i+\sum_{j\in h(i)}T_j(d_i)$$

式中：$h(i)$ 表示处于关键状态且优先级比 τ_i 高的消息集。

证明

(1) 在关键状态下，仅当 $\eta_\lambda(i)=1$ 时，τ_i 才会对低优先级的消息实例产生干扰，且最大干扰发生在低优先级消息实例与所有高优先级消息实例同时到达的时刻，因此从高优先级消息的角度看，高优先级消息实例在一个周期内，最多对低优先级的消息实例产生 C_i 单位时间的延迟。

(2) 关键状态消息实例仅受到同处于关键状态且具有较高优先级的消息实例的干扰。

d_i 可通过如下迭代进行计算：$d_i^0=0$，$d_i^{n+1}=C_i+\sum_{j\in h(i)}T_j(d_i^n)$；当 $d_i^{n+1}=d_i^n$ 或 $d_i^n>D_i$ 时停止迭代。

定理 4 负载为消息集 Π 的调度器使用基于网络传输性能降级约束的双层优先级调度算法，如果对于所有 $\tau_i\in\Pi$ 都有 $d_i\leqslant D_i$，则消息集 Π 是可调度的。

证明 由引理 1 和引理 2 得证。

7 仿真验证

在相同的消息负载下，以动态失效窗口的数量来衡量机载网络的可靠性。消息集参数设置见表 1。

表 1 消息集参数

Table 1 Parameters of message set

Π	T_i	D_i	C_i	P_i	λ_i	Load rate/%
τ_1	10	10	5	1	$\langle\overline{2},10,0.8\rangle$	
τ_2	10	10	5	2	$\langle\overline{2},10,0.6\rangle$	
τ_3	50	50	5	3	$\langle\overline{2},10,0.6\rangle$	
τ_4	100	100	5	4	$\langle\overline{2},10,0.6\rangle$	130
τ_5	100	100	5	5	$\langle 3,10,0.8\rangle$	
τ_6	100	100	5	6	$\langle 3,10,0.8\rangle$	
τ_7	100	100	5	7	$\langle 3,10,0.8\rangle$	

使用 C++语言建立采用离散事件驱动机制的仿真系统,对 17 组(由于篇幅原因,表 1 中只列出负载率为 130%的一组消息集作为示例)负载率不同,但都满足定理 4 可调度性条件的消息集,分别使用基于时延的最小期限优先算法(Earliest-Due-date-First,EDF)、优先级调度算法和基于网络传输性能降级约束的双层优先级调度算法进行仿真,仿真时间为最长消息周期的 1 000 倍,运行仿真 20 次,统计动态失效窗口的数量。图 2 以消息集负载率为横轴,给出了 3 种调度算法下动态失效窗口的数量。

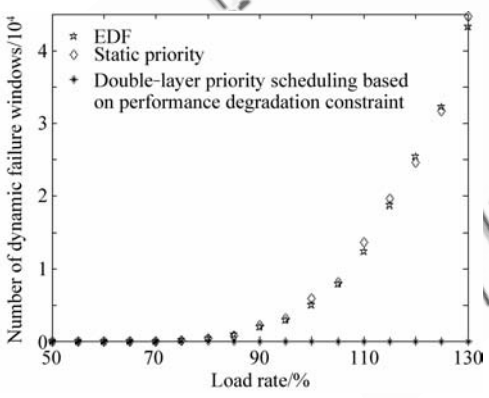

图 2 仿真结果

Fig. 2 Simulation result

由图 2 可以看出:若没有预先限定性能降级约束,无论是使用 EDF 还是优先级调度算法,在系统负载率高于 80%时,都将有动态失效窗口发生,且随着系统负载率的增加,动态失效窗口的数量急剧增加;但在网络传输性能降级约束下,使用基于网络传输性能降级约束的双层优先级调度算法,只要满足定理 4 的可调度性条件,即使消息负载率达到 130%,仍无动态失效窗口发生,既验证了第 6 节可调度性理论分析的正确性,也表明实施降级约束可以增强机载网络在资源不足时的可靠性。

8 结 论

定义了两种网络传输性能降级约束,为分析网络设备资源不足条件下机载网络的可靠性提供了理论依据,并给出了工程中易于实现的约束实施策略。理论分析和仿真表明,当机载网络设备因出现故障而导致资源不足时,使用动态失效窗口的数量来度量机载网络的可靠性,通过实施网络传输性能降级约束,即使负载率大于 1,仍能保证无失效窗口发生,因此把网络性能降级的程度限制在可控范围内,从而增强了机载网络的可靠性。

参 考 文 献

[1] 徐亚军,张晓林,熊华钢. 航空电子系统 FC 交换式网络的可靠性研究[J]. 航空学报,2007,28(2):402-406.
Xu Yajun, Zhang Xiaolin, Xiong Huagang. Study on reliability of FC fabric in avionic[J]. Acta Aeronautica et Astronautica Sinica, 2007, 28(2): 402-406. (in Chinese)

[2] 姜震,邵定蓉,熊华钢,等. 实时网络系统可靠性建模研究[J]. 航空学报,2004,25(3):275-278.
Jiang Zhen, Shao Dingrong, Xiong Huagang, et al. Research on reliability model of real-time network systems [J]. Acta Aeronautica et Astronautica Sinica, 2004, 25(3): 275-278. (in Chinese)

[3] Hamdaoui M, Ramanathan P. A dynamic priority assignment technique for streams with (m, k)-firm deadlines [J]. IEEE Transactions on Computers, 1995, 44(12): 1443-1451.

[4] Hamdaoui M, Ramanathan P. Evaluating dynamic failure probability for streams with (m, k)-firm deadlines[J]. IEEE Transactions on Computers, 1997, 46(12): 1325-1337.

[5] West R, Zhang Y T, Schwan K, et al. Dynamic window-constrained scheduling of real-time streams in media servers[J]. IEEE Transactions on Computers, 2004, 53(6): 744-759.

[6] Chen J M, Wang Z, Song Y Q, et al. Scalability and QoS guarantee for streams with (m, k)-firm deadline[J]. Computer Standard and Interface, 2006, 28(5): 560-571.

[7] Balbastre P, Ripoll I, Crespo P. Analysis of window-constrained execution time systems[J]. Real-Time Systems, 2007, 35(2): 109-134.

[8] Chu Y C H, Burns A. Flexible hard real-time scheduling for deliberative AI systems [J]. Real-Time Systems,

2008, 40(3): 241-263.

[9] Koubaa A, Song Y Q. Graceful degradation of loss-tolerant QoS using (m, k)-firm constraints in guaranteed rate networks[J]. Computer Communications, 2005, 28(12): 1393-1409.

[10] Bernat G. Specification and analysis of weakly hard real-time system [D]. Palma: University of the Balearic Islands, 1998.

[11] Bernat G, Burns A, Llamosi A. Weakly-hard real-time systems[J]. IEEE Transactions on Computers, 2001, 50(4): 308-321.

[12] Bernat G, Cayssials R. Guaranteed on-line weakly-hard real-time systems [C] // Proceedings of the 22nd IEEE Real-Time Systems Symposium. 2001: 25-35.

[13] 陈积明, 宋叶琼, 孙优贤. 弱硬实时系统约束规范研究[J]. 软件学报, 2006, 17(12): 2601-2608.
Chen Jiming, Song Yeqiong, Sun Youxian. Research on constraint specification of weakly hard real-time system [J]. Journal of Software, 2006, 17(12): 2601-2608. (in Chinese)

[14] 陈积明. 弱硬实时系统及其调度算法[D]. 杭州: 浙江大学, 2005.
Chen Jiming. Weakly hard real-time system and its scheduling algorithms [D]. Hangzhou: Zhejiang University, 2005. (in Chinese)

[15] Zhuang S X, Cassandras C G. Optimal control of discrete event systems with weakly hard real-time constraints[J]. Discrete Event Dynamic Systems, 2009, 19(1): 67-89.

作者简介:

张勇涛(1983—) 男,博士研究生。主要研究方向:信息网络和实时系统。
Tel: 010-82338712
E-mail: zhangyongtao394@ee.buaa.edu.cn

黄臻(1982—) 男,博士研究生。主要研究方向:航电网络。
E-mail: huangzhen@ee.buaa.edu.cn

熊华钢(1965—) 男,博士,教授,博士生导师。主要研究方向:航空电子和数字通信。
Tel: 010-82317202
E-mail: hgxiong@ee.buaa.edu.cn

Study on Network Reliability in Avionics Based on Performance Degradation Constraints

ZHANG Yongtao, HUANG Zhen, XIONG Huagang *

School of Electronics and Information Engineering, Beihang University, Beijing 100191, China

Abstract: In order to enhance network reliability in avionics when there is a shortage of network equipment due to malfunction, two performance degradation constraints are defined. Both degradation constraints employ three arguments to accurately describe the number and distribution of message failures or successes during transmission. New concepts, such as dynamic failure, critical function and minimal guaranteed future sequence, are defined to analyze the performance degradation constraints: the value of critical function can predict whether a dynamic failure will occur if the transmission of the next message fails; the minimal guaranteed future sequence can minimize the number of successful transmissions without the occurrence of dynamic failure. Two strategies are proposed to implement the performance degradation constraints in avionic networks: static filtration by message source and dynamic arbitration by network. A double-layer priority scheduling algorithm is proposed, which is based on performance degradation constraints and used in the strategy of dynamic arbitration by network. The algorithm is able to avert dynamic failure by means of the predictability of critical function. The schedulability of the algorithm is also analyzed. The analysis and simulation proves that the network reliability in avionics is improved by implementing the performance degradation constraints.

Key words: avionics; reliability; network performance; degradation; schedulability analysis; dynamic failure

Received: 2010-12-07; **Revised**: 2011-03-25; **Accepted**: 2011-04-18; **Published online**: 2011-04-27 16:00:52
URL: www.cnki.net/kcms/detail/11.1929.V.20110427.1600.003.html **DOI**: CNKI:11-1929/V.20110427.1600.003
Foundation item: National Natural Science Foundation of China (61073012)
* **Corresponding author**. Tel.: 010-82317202 E-mail: hgxiong@ee.buaa.edu.cn