doi:10.3969/j.issn.1671-637X.2016.11.015

TTE网络系统级网关的通信完整性保证机制

贾梦媛, 赵露西, 代亚楠, 李 峭
(北京航空航天大学,北京 100191)

摘 要: 时间触发以太网(TTE)的交换设备采用中央监视进行通信完整性检查,而对于具有网关的层次化TTE网络,需要在网关处设置系统级的通信完整性保证机制。面向通用的远程现场网络拓扑结构,设计了外部冗余物理链路和内部协议检查相结合的通信完整性检查网关,并构建半物理仿真平台,对设计实现进行了实验验证。仿真结果表明,该设计在充分利用设备级完整性检查功能的基础上,兼容了两端网络的交换式传输机制,有效地支持了系统级的故障隔离。

关键词: 时间触发以太网; 通信; 完整性; 半物理仿真
中图分类号: TP391.9 **文献标志码**: A **文章编号**: 1671-637X(2016)11-0068-05

An Integrity Guarantee Mechanism for System Level Gateway Communications in TTE Networks

JIA Meng-yuan, ZHAO Lu-xi, DAI Ya-nan, LI Qiao
(Beihang University, Beijing 100191, China)

Abstract: Switching equipment of the Time-Triggered Ethernet adopts central monitoring system to check the integrity of communication. But for a hierarchical TTE network with gateway, a communication integrity security mechanism on system level should be realized at the gateway. Based on general topological structure, this paper presents a gateway with communication integrity check function, combining the external redundancy physical link with the internal protocol check. A semi-physical simulation platform is constructed to verify the design mentioned. The results indicate that based on the full use of the equipment-level integrity check function, this design is compatible with both ends of the network transmission and can support system-level fault isolation effectively.

Key words: Time-Triggered Ethernet (TTE); communication; integrity; semi-physical simulation

1 TTE网络完整性概述

在通信系统中,完整性(Integrity)是系统在运行过程中发现故障并达到故障安全状态的能力,是可信性(Dependability)的重要属性之一[1]。

时间触发以太网(Time-Triggered Ethernet,TTE)是支持时间触发通信和速率约束通信的实时网络互连技术[2],它的协议标准考虑了通信和定时的完整性,已经被用于航空航天电子系统的综合化互连[3]。

TTE网络的完整性体现在时钟同步的完整性和通信的完整性两个方面。

对于时钟同步的完整性,TTE网络可将端系统(ES)的同步主控器(SM)设为高完整性设备,在冷启动和结团检测中将"随意"失效模式转化为"不一致"失效模式,从而有效降低解决同步错误的复杂度,对于压缩控制器(CM)的高完整性操作也有相应的研究[4]。

对于通信的完整性,不仅通过协议芯片级的指令/监视对(COM/MON pair)机制[5]保证了交换机接口处的通信完整性,而且对于网络设备和网络系统也可设置不同层次的完整性保证。上述机制与TTE网络的多冗余配置相结合,能够显著提高网络通信的可靠性。

作为网桥的TTE交换机具有设备级的通信完整性检查功能,用它们进行网络互连可以达到相当的规模。然而,对于具有多个舱段的航天器,例如欧航局的Ariane 6大型火箭(如图1所示),具有多层网络结

收稿日期:2015-09-28 **修回日期**:2015-11-20
基金项目:自然科学基金(61301086);中央高校基本科研业务费(YWF-15-GJSYS-055)
作者简介:贾梦媛(1991—),女,湖北巴东人,硕士生,研究方向为时间触发以太网。

构——第 3 级是指令任务高层控制系统的网络互连，第 2 级是嵌入式处理单元的交换式互连，第 1 级中的电子控制单元则远程接入到交换机。它们除了采用本地接入和 TTE 交换机级联之外，在第 3 级和第 2 级之间还设置网关，进行系统级的流量监视，以保证各级的通信完整性。

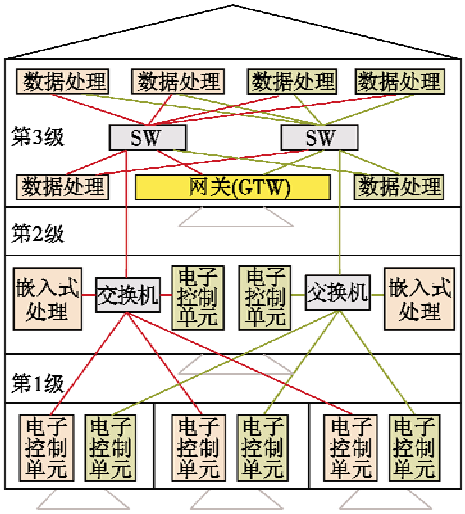

图 1　Ariane 6 航天电子系统互连框图

Fig. 1　Ariane 6 avionics interconnection system

更进一步，TTE 网关可以与通信过程更紧密地耦合，即：同时具备监视和流量管制功能，不同安全关键性等级的网络区域之间可以通过具有完整性检查功能的网关实现连接，保护高安全性网络免受低安全性网络的故障影响。文献[6]发明了一种 TTE 网关，它建立了内外结合的自检机制，实现远程现场网络（Remote Field Network）与控制台所在的任务系统 TTE 网络之间的通信完整性自检接口，然而，接入到该网关的现场网络仅限于特定的环形拓扑结构。

在前人研究工作的启发下，本文给出了具有双通道的内外结合自检的 TTE 网关设计方案，使之适应于更通用的交换式拓扑结构。根据 TTE 系统级完整性保证机制，给出具有通信完整性检查功能的 TTE 系统级网关的设计方案，提出相应的测试实验方法，并结合典型实验案例验证其功能。

2　TTE 网络完整性保证的基础

故障封闭能力是保证 TTE 网络完整性的基础，在芯片级和设备级分别以硬件和协议来实现相应的完整性机制，并支撑了系统级的完整性检查。

2.1　芯片级的完整性机制

为实现芯片级的故障封闭，TTE 网络在协议芯片级提出了高完整性设计——指令/监视对（COM/MON pair）机制。COM/MON 组件本质上是一个内部自检对，指令器 COM 执行实际活动，监视器 MON 观察 COM 的信号并在发生故障时关闭信号输出。

虽然 TTE 网络协议芯片的实现保证了底层的故障隔离，但是，设备实际运行过程中仍有一些故障是不可预见的，当这些故障形成错误并导致可见的设备失效，将会影响 TTE 网络设备和/或系统的通信完整性。

2.2　设备级的完整性机制

为了实现设备级的故障封闭，作为网桥设备的 TTE 交换机引入中央监视功能，通过设置特定的接收时间窗，保护 TTE 网络免受故障 ES 的影响[5]。图 2 描述了 TT 数据流的中心监视过程。

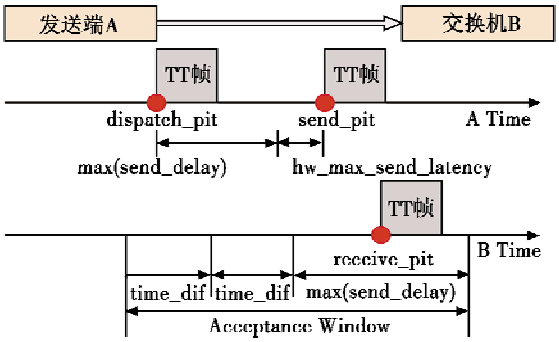

图 2　TT 流量的中心监视窗口

Fig. 2　Central monitor of TT

在发送过程中，由于链路繁忙造成的排队等待，TT 帧的实际发送时间点（send_pit）相对于调度表派发时间点（dispatch_pit）会有延迟。在接收过程中，由于数据流的传输延迟，TT 帧的到达时间（receive_pit）相对于 send_pit 又会有延迟。

TTE 交换机在考虑以上延迟参数的基础上，为每个 TT 帧设置了接收窗口，检查接收 TT 帧的时刻是否满足时间触发调度精度的要求。接收窗口的起始点需要考虑接收时间点 receive_pit 的最早可能值，满足以下条件：acceptance_window_start = dispatch_pit + link_latency − time_dif。其中，link_latency 为数据流链路的传输延迟，time_dif 为网络中两个正确同步的本地时钟的最大可能时间差。

同理，接收窗口的结束点也必须考虑 TT 帧的 receive_pit 最晚可能值，满足以下条件：acceptance_window_end = acceptance_window_start + 2time_dif + max（send_delay）。

当 TTE 交换机进行 TT 流量的接收窗口检查时，只有当 TT 帧的 receive_pit 处于 acceptance_window_start 和 acceptance_window_end 之间，交换机才能将它转发，否则被丢弃，实现故障隔离。

3 系统级网关的完整性检查

当实时通信网络包含多级嵌入式系统时，存在所谓的“网络分区”，例如：系统网络被分为控制数据网络与远程现场网络，区域之间需配备具有完整性检查功能的网关来实现系统级的故障隔离。

文献[6]给出了一种具有专用拓扑结构的网络——交织环形可用完整性网络(Braided Ring Availability Integrity Network，BRAIN)，将其作为把远程现场网络通过具有自检对的 TTE 网关接口与控制台相连的方案，其结构如图 3a 所示。该方案的独特之处在于网关的通信和监视模块分别具有独立的物理链路，具有“内外结合”的完整性检查结构，即：1) 外部存在两条物理链路同时发送消息；2) 内部存在缓冲区对消息进行完整性检查。

但是，BRAIN 结构只适用于环型连接的远程现场网络，为了适应通用的网络拓扑结构，充分利用 TTE 交换机自身的完整性检查机制，给出双通道网关的模型和设计方案，同样保证了内部和外部相结合的自检功能，其结构如图 3b 所示。

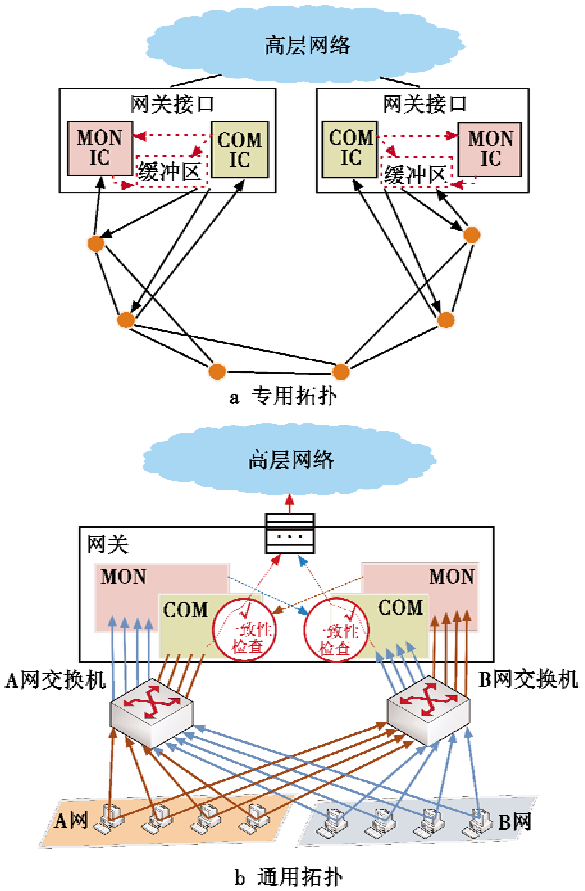

图 3 自检网关的实现方案

Fig. 3 Experimental scheme of self-check gateway

在该通用拓扑结构方案中，采用交换机构建双冗余网络，支持比 BRAIN 结构更复杂的具有全连通性的远程现场网络。该方案能够实现通用拓扑下内外结合的完整性保障机制，即网关外部的冗余链路提供了数据包物理传输的完整性保障，网关内部的一致性判决提供了数据包传输时间和内容的完整性保障。例如，图 3b 中，远程现场网络具有 A 网和 B 网双冗余配置，A 网和 B 网中节点的数据流分别通过 A 网和 B 网的 TTE 交换机到达网关，并将监控数据流馈入对侧的交换结构，形成交叉检查。

为了利用 TTE 交换机提供的设备级完整性保证机制，接入网关的 A 网和 B 网交换机的端口进行了特殊的配置，增加了冗余的外部物理通信链路，将交换机内部的芯片级监视流量也镜像到外部物理链路网络端口，向网关输入成对的 COM/MON 数据包。

以图 3 中 A 网的远程节点为例，发送的数据包经过 A 网交换机到达 A 网 COM 的同时，也会经过 B 网交换机到达 B 网 MON，A 网 COM 在接收到 A 网数据包后，会根据虚拟链路(VL)标识符和定时参数查找并访问 B 网最近到达的属于同一个 VL 的数据包，并将两者定时进行精度和内容的一致性检查，满足条件的 A 网数据包将会被转发到高层网络，不满足的将被丢弃。同理，B 网远程节点发送的数据包也经过相应的交叉检查。

4 半物理仿真环境下的通信完整性实验

4.1 实验平台的组成

为了验证上述网关的完整性检查功能，采用半物理仿真的形式搭建了图 4 所示的 TTE 网络完整性机制测试实验平台。该平台由远程现场网络模块、冗余链路模块、网关模块、监视模块 4 个部分构成。

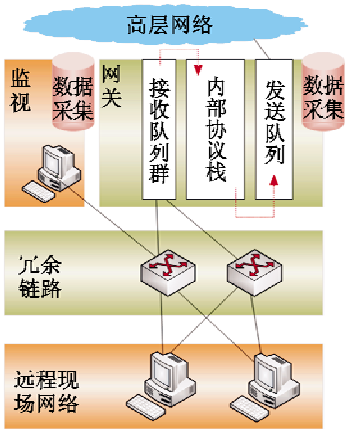

图 4 测试系统结构

Fig. 4 Test system structure

远程现场网络模块的终端节点作为 TT 数据流的发送端，具有生成和发送 TT 数据包的功能；冗余链路模块不仅有交换机提供设备级的完整性保证机制，还有双冗余的物理链路提供成对的 A/B 数据包供网关进行对比分析；网关模块在应用层实现，由接收队列群、内部协议栈和发送队列构成，负责完成 TT 数据包的接收、完整性检查和转发操作，并统计通过网关的 A 网数据包；监视模块负责实时记录经过网关前的 A 网数据包，为经过网关后的 A 网数据包提供对比。

4.2　网关的通信完整性测试

考虑到 TTE 交换机的一个 COM/MON 组件只有一个输入/输出端口，此处采用端系统应用程序来实现网关的内部协议栈判决功能。

网关的构成包括接收队列群、发送队列和内部协议栈 3 部分。该实验中，网关默认 A 网交换机传入的数据包为控制型数据包，B 网交换机传入的数据包为监视型数据包。接收队列群按需分为控制型队列和监视型队列，并通过多线程实现两种数据包的实时接收，当内部协议栈为空时，控制型队列将接收到的数据包送入内部协议栈，内部协议栈在接收到数据包后将读取监视型队列最前端的数据包，与控制型数据包进行两项检查：1）内容一致性检查；2）符合时间窗口的时间一致性检查。然后将符合条件的控制型数据包送入发送队列等待转发，具体实现流程如图 5 所示。

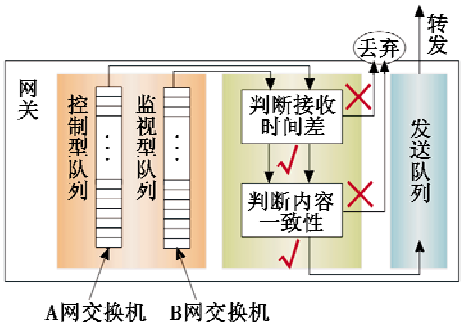

图 5　协议栈流程图

Fig. 5　Protocol stack

5　实验案例与实验结果

5.1　实验案例

为了说明系统级网关的工作原理，并展示测试实验平台的功能，设计了相应的实验案例。限于硬件设备的造价，实验中仅设置单个远程通信节点，但可以通过 VL 的参数配置模拟来自不同节点的流量。

该案例在图 4 所示的子系统中实现，实验分为 7 个阶段。其中，B，D 阶段引入了时序不一致的故障，F 阶段引入了内容不一致的故障，其他阶段均为正确配置下的对比实验。具体参数配置如表 1 所示。

表 1　网关测试参数配置

Table 1　Configure of gateway test

仿真阶段	A/B 网络	有效负载:64 位整数	消息周期/ms	A 网交换机中央监视	消息数量/条
A	A B	填充 1 填充 1	1000	开	50
B	A B	填充 1 填充 1	500 1000	关	100 50
C	A B	填充 1 填充 1	1000	开	50
D	A B	填充 1 填充 1	500 1000	开	100 50
E	A B	填充 1 填充 1	1000	开	50
F	A B	填充 1 填充 2	1000	开	50
G	A B	填充 1 填充 1	1000	开	50

5.2　实验结果

图 6 给出了发送端消息总数、监视模块捕获的消息总数、网关转发的消息总数随仿真时间的变化。

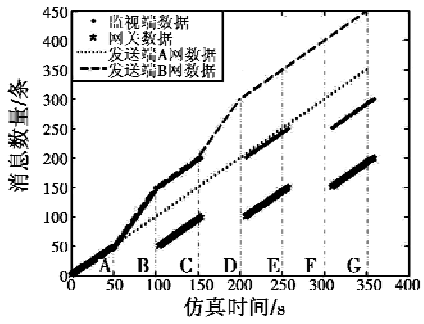

图 6　实验结果

Fig. 6　Result of the experiment

图 6 结果显示，在 B，D，F 阶段，相应地设置了错误的数据包都被阻断，没有到达接收端。其中，虽然 B 阶段故意关闭设备级中央监视功能，使得在监视模块几乎未发生丢包，但由于在网关处会进行时序检查并执行丢包，也能够实现故障隔离，说明 TTE 完整性检查网关对于时序不一致故障具有检查和隔离能力。

当然，在中央监视和网关完整性检查功能都开启的情况下，对故障数据包的隔离达到最完善，如 D 阶段所示。F 阶段中引入了内容不一致的流量，在监视模块几乎未发生丢包，但这些包在经过网关后被丢弃，说明 TTE 完整性检查网关对于内容不一致故障具有检查和隔离能力，该能力补充了单纯进行中心隔离的不足。

上述结果表明，该 TTE 完整性检查网关通过内部协议栈，实现了对内容不一致、时序不一致消息的故障隔离，达到了网关对通信完整性的保障功能。

6 总结

TTE网络的通信完整性保证机制对于提高网络的安全性和可靠性具有重要意义。本文提出的TTE完整性检查网关,可以使用于通用的交换式级联拓扑,其特点在于通过内外结合的双重通信完整性保障机制,能够满足级联拓扑下高完整性通信的需求。半物理仿真实验表明,利用TTE完整性检查网关,既可以隔离时序故障,又可以隔离内容故障,其中对于内容错误的故障数据流的隔离能够补充设备级中央监视机制的不足,有望在高安全性要求且分层次的航空航天TTE网络互连中得到应用。

参 考 文 献

[1] RADJENOVIC A, PAIGE R. Architecture description languages for high-integrity real-time systems[J]. Software, IEEE, 2006, 23(2):71-79.

[2] SAE Aerospace. SAE AS6802 Time-triggered Ethernet[S]. [S.l.]:SAE International, 2011.

[3] 熊华钢,王中华. 先进综合航空电子技术[M]. 北京:国防工业出版社,2009. (XIONG H G, WANG Z H. Advanced avionics integration techniques[M]. Beijing: National Defense Industry Press, 2009.)

[4] 兰杰,熊华钢,李峭. 时间触发以太网时钟同步的容错方法分析[J]. 计算机工程与设计,2015,36(1):11-16. (LAN J, XIONG H G, LI Q. Clock synchronization fault-tolerance in time-triggered ethernet[J]. Computer Engineering and Design, 2015, 36(1):11-16.)

[5] ROMAN O. Time-triggered communication [M]. New York:CRC Press, 2009.

[6] BRENDAN H, MICHAEL P, DWAYNE B, et al. Hybrid topolovy ethernet architecture: US, 008130773B2[P]. 2012-03-06.

(上接第67页)

[7] DUCHAINEAU M, WOLINSKY M, SIGETI D E, et al. ROAMing terrain: real-time optimally adapting meshes [C]//Proceedings of the 8th Conference on Visualization, IEEE Computer Society Press, 1997:81-88.

[8] BLOW J. Terrain rendering at high levels of detail [C]// Proceedings of the 2000 Game Developers Conference, 2000:37-45.

[9] PUPPO E. Variable resolution terrain surfaces [C]//Proceedings of the CCCG, Citeseer, 1996:202-210.

[10] HOPPE H. Smooth view-dependent level-of-detail control and its application to terrain rendering [C]//Proceedings of the Visualization, IEEE, 1998:35-42.

[11] PAJAROLA R, ANTONIJUAN M, LARIO R. Quadtin: quadtree based triangulated irregular networks [C]// Proceedings of the Conference on Visualization, IEEE Computer Society, 2002:395-402.

[12] 张燕燕,黄其涛,韩俊伟,等. 飞行模拟器视景系统的设计与实现[J]. 系统仿真学报,2009,21(12):3362-3367. (ZHANG Y Y, HUANG Q T, HAN J W, et al. Design and implementation of visual simulation system in flight simulator [J]. Journal of System Simulation, 2009, 21(12):3362-3367.)

[13] 李钦,戴树岭,赵永嘉,等. 分块LOD大规模地形实时渲染算法[J]. 计算机辅助设计与图形学学报,2013,25(5):708-713. (LI Q, DAI S L, ZHAO Y J, et al. A block LOD real-time rendering algorithm for large scale terrain [J]. Journal of Computer-Aided Design & Computer Graphics, 2013, 25(5):708-713.)

[14] 王响,雷小永,戴树岭. 基于视点预测的大规模地形的实时渲染[J]. 系统仿真学报,2013,25(6):1202-1206. (WANG X, LEI X Y, DAI S L. Real time rendering of large scale terrain based on viewport prediction [J]. Journal of System Simulation, 2013, 25(6):1202-1206.)

[15] VERVERS P M, HE G, SUDDRETH J, et al. Design and flight test of primary flight display combined vision system[J]. SAE International Journal of Aerospace, 2011, 4(2):738-746.