基于 MILS 架构的嵌入式操作系统多级安全域动态管理技术

高沙沙[1,2] 王中华[1]
(中国航空工业集团公司西安航空计算技术研究所 西安 710068)[1]
(西安电子科技大学计算机学院 西安 710071)[2]

摘 要 基于 MILS 架构的嵌入式操作系统能够实现不同应用分区之间不同密级数据的安全隔离。然而,现有基于 MILS 架构的嵌入式操作系统无法满足任务运行出现故障后正确安全迁移的需求,从而无法实现任务功能重构和实时动态加载的目标。因此,在对现有基于 MILS 架构的嵌入式操作系统的优点和不足进行分析的基础上,提出了面向任务的多级安全域动态管理架构,并详细描述了架构中各个功能模块的工作原理,从而能够保证任务在特定的安全域内进行动态迁移和功能重构。

关键词 多级安全域,MILS,功能重构
中图法分类号 TP393.08 **文献标识码** A

Dynamical Management Technology of Multi-Level Security Domain for Embedded Operating System Based on MILS

GAO Sha-sha[1,2] WANG Zhong-hua[1]
(Xi'an Aeronautics Computing Technique Research Institute, AVIC, Xi'an 710068, China)[1]
(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)[2]

Abstract The embedded operating system based on MILS architecture can achieve security isolation of data from different application partitions. However, the existing embedded operating systems based on MILS architecture can not meet the need of secure migration, and cannot complete tasks' functional reconstruction and real-time dynamic loading after the failure of task. Therefore, on the basis of analyzing the advantages and disadvantages of the existing embedded operating systems based on MILS, a task-oriented multi-level security domain management architecture was proposed. Besides, the working principle of each functional module in the architecture was described in detail, which can ensure the dynamic migration and functional reconstruction within a specific security domain.

Keywords Multi-level security domains, MILS, Functional reconstruction

1 引言

在信息化背景下,操作平台的无人化特征以及多个操作平台协同工作,使得嵌入式操作系统的信息安全问题成为机载软件设计的焦点。MILS 架构将操作系统进行层次划分,分为应用程序层、中间件层、微内核层 3 层。应用程序层将内存分区,达到 MILS 系统的空间隔离,保证任务故障只发生在一个分区内,不影响该系统上的其他分区上运行的任务。中间件层不仅屏蔽了底层操作系统的差异,而且提供微内核层精简掉的系统服务。微内核层具有十分精简的系统服务。

为了支持多安全级别信息的混合处理,为信息安全提供支撑,Rushby[1-2] 最早提出 MILS 架构,采用微内核构建分区环境。Alves-Foss 等[3] 系统设计的 MILS 高安全保障系统组件,使得系统架构更经济、更安全以及一体化。Shield 等[4] 基于 MILS 架构的时空隔离和故障隔离特性造成的信息共享和信息聚类的困难,提出了两种信息关联方式:可视化信息关联和链接信息关联。张灯等[5-6] 通过研究 MILS 系统的中间件,实现了 MILS 系统的信息跨分区跨平台的互通。李健等[7] 基于 MILS 多级安全架构的安全架构对 MILS 多级安全架构的目标机通信框架进行了改造。杨姗[8] 基于 MILS 的安全性、实时性、实用性出发,研究了 MILS 系统的多种关键技术,包括多级融合实时调度机制、分区间的通信技术、I/O 设备复用技术以及强安全访问控制技术。石鹏[9] 实现了基于 seL4 微内核的 MILS 架构的原型系统。总之,在分析基于 MILS 架构的微内核[10] 的基础上,研究中间件[11-14] 实现微内核精简掉的系统服务,包括安全访问控制[15] 和文件系统[16-17] 等功能,都必须满足分区通信的安全性和 MILS 架构对分区密级的严格控制。

综上所述,基于 MILS 架构的操作系统通过时空隔离从根本上构建了一个安全的机载软件基础。上述研究主要集中在 MILS 架构的优化以及 MILS 中间件方面,尤其在研究 MILS 的跨域数据传输[18] 时,都需要以保证 MILS 的隔离特

本文受装发预研项目(31511020202)资助。
高沙沙(1994—),女,硕士生,主要研究方向为嵌入式安全;**王中华**(1983—),男,博士,工程师,主要研究方向为云计算、嵌入式安全,E-mail:mackay.wang@126.com(通信作者)。

性不受破坏为前提。然而，MILS 架构实际运用于嵌入式系统中，无法实时解决任务故障问题。为了解决任务故障问题，本文提出构建多级安全域用来管理运行于多个平台上的不同安全级别的任务，实时监控各个平台任务的状态变化。当实时感知到运行中任务出现异常时，能够根据多级安全域动态管理机制保证任务继续正常运行。

本文第 2 节将对多级安全域的系统平台——基于 MILS 架构的嵌入式操作系统的安全基础进行总结归纳；第 3 节详述了多级安全域动态管理的框架；第 4 节详述了多级安全域动态管理的实现方法；最后对全文进行总结并指出了下一步研究方向。

2　MILS 架构

随着嵌入式硬件出现各类安全漏洞，如 Meltdown 和 Spectre 等安全威胁频发，嵌入式系统的安全性能面临着极大的挑战。因此，对 MILS 架构的安全性能进行不断优化以应对频发的安全威胁成为嵌入式系统安全领域的研究重点。

MILS 架构是一个可以在同一系统上执行不同安全级别应用的可验证的安全体系结构。MILS 架构将操作系统进行层次划分，MILS 架构中的微内核层只包括系统服务中最精简的部分，只负责数据隔离、信息流控制和损坏限制，中间件层主要负责屏蔽下层操作系统的差异以及补充微内核层精简掉的系统服务，应用层的系统分区主要包括应用层的安全策略。

MILS 架构的核心概念是将多个子系统的应用程序以分区的形式运行在同一个处理器上，每个分区具有独立的分区操作系统和资源，这种结构保证了分区间的空间隔离；同时采用严格的时间片轮转调度机制来完成分区时间调度，以保证分区间的时间隔离。因此，基于 MILS 架构的中间件研究、分区通信以及应用开发，都需要将 MILS 架构的时空隔离和分区特性考虑在内。其软件架构如图 1 所示。

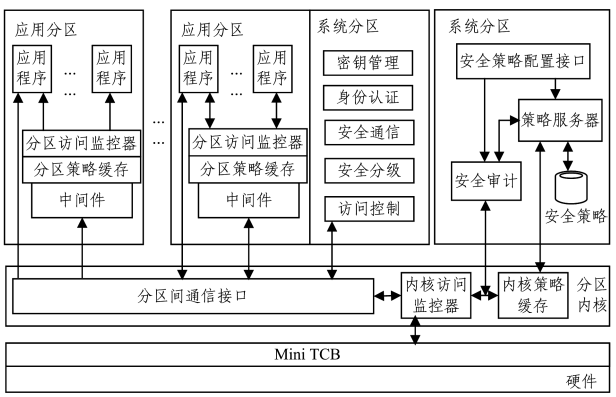

图 1　MILS 软件架构

基于 MILS 架构的操作系统的安全性主要体现在时空隔离和故障隔离，但是这些安全特性也造成了不同分区运行程序之间信息共享和信息聚合的复杂性。为保证不同安全等级分区之间的信息共享、信息传输而进行的中间件研究和信息共享方式研究又破坏了信息分级分区保护和故障隔离特性。因此，对 MILS 分区系统应用层运行的任务进行分区分域管理，将不同安全等级的任务在同一安全等级域内运行，既不破坏 MILS 架构上的隔离属性，还能进一步增加 MILS 分区操作系统的安全性。

3　多级安全域动态管理的总体架构

安全域是同一逻辑区域内有相同安全需求和保护策略的要素的集合，同一安全域内的任务执行相同的安全策略，相互信任，域间任务的安全防护执行安全域之间的信息流隔离策略。在基于 MILS 架构的嵌入式操作系统基础上构建多级安全域，务必保证安全域内相互信任、安全域间隔离的特性不受影响。

多级安全域硬件由安全域服务器和多个客户端以及时间触发网络（Time Trigger Ethernet，TTE）组成。将该系统内运行于不同客户端，但具有相同安全等级的任务划分为同一安全域。各种功能类型的任务运行在客户端，客户端负责实时搜集任务的状态信息，并将其发送到安全域服务器。任务异常时，客户端还要根据安全域服务器的控制信息，搜集任务状态参数，中断旧任务，启动新任务。安全域服务器负责多级安全域的创建、多级安全域的同步和多级安全域的更新，以及在任务异常时发送信息指导客户端做出反应。TTE 网络负责安全域服务器和客户端、客户端和客户端之间通信。多级安全域的模块组成如图 2 所示。

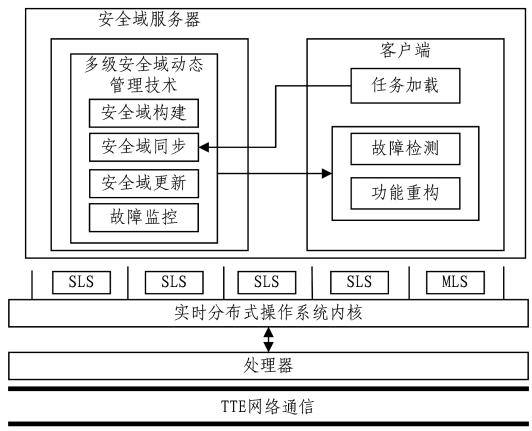

图 2　多级安全域模块组成

4　多级安全域动态管理的具体实现

4.1　多级安全域管理

MILS 架构的分区也有不同的安全级别，包括非密级分区（U）、秘密级分区（C）、机密级分区（S）、绝密级分区（TS）以及多安全级别分区 5 种。在每个分区内存储对应安全级别的安全域内的任务信息。MILS 架构的分区和多级安全域之间的对应位置如图 3 所示。

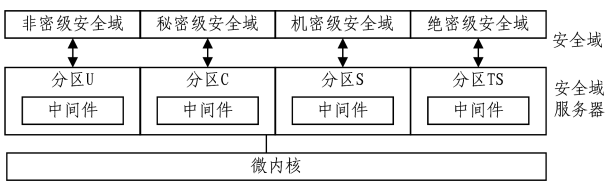

图 3　安全域信息存储

通过 MILS 架构的分区隔离保证了不同安全域数据的独立性，同一安全域内的任务安全等级相同。多级安全域的同步指的是客户端上的任务加载时，同步更新安全域。

任务加载时，根据任务的安全等级将其加载到对应安全等级的分区上，同时将其备份至安全等级匹配的同一节点的其他分区或者其他节点的安全等级匹配的分区上，然后将该

任务的安全域信息通过 TTE 网络发送到安全域服务器对应安全域内存储，从而实现安全域的同步。

表 1 任务安全域信息表

任务编号	安全等级	所在节点	所在分区	主备份	备份节点	备份分区
01	U	0	U	主	0	ML
02	S	0	S	主	1	S
03	C	0	C	主	1	C
04	TS	0	TS	主	0	ML

任务安全域信息的数据格式如表 1 所列。其中，任务编号按照任务加载顺序依次编号；任务安全等级分别为绝密(*TS*)、机密(*S*)、秘密(*C*)、非密(*U*)；任务运行的计算节点编号有 0，1；任务的主备份属性包括主任务以及备份任务；涉及到的分区安全等级包括绝密(*TS*)、机密(*S*)、秘密(*C*)、非密(*U*)4 个单安全级别以及可存储多安全级别任务的 *MLS* 分区。

安全域的同步流程如图 4 所示。1)客户端新加载任务时，通过 TTE 网络将任务安全域信息发送到安全域服务器；2)安全域服务器收到任务安全信息后，通过定位该任务的任务安全等级来确定要存储的安全域；3)将该任务安全信息存储至对应分区上的安全域内。

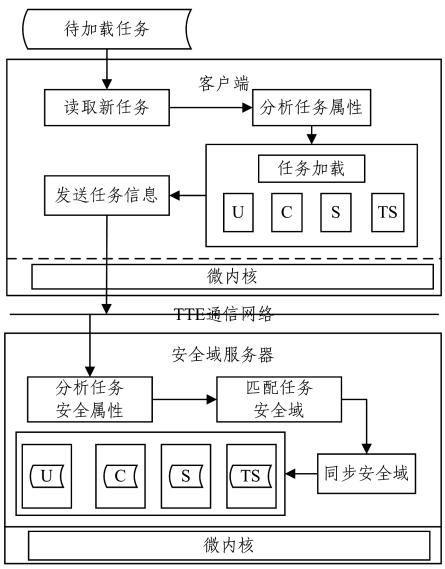

图 4 安全域的同步原理

任务运行时，客户端的故障监测模块实时监测任务状态，根据任务属性 *PROCESS_SATE* 判断该任务是否出现运行异常，若任务正常，则将任务故障标识设为 1，若任务异常，则将任务故障标识设为 0，并发送任务状态信息，告知安全域服务器该任务的运行状态。同时，若在固定时间段 *SleepTime* 内安全域服务器监控模块没有收到客户端任务状态信息，则判断任务异常。任务状态信息的数据格式如表 2 所列。

表 2 任务状态信息表

任务编号	安全等级	故障标志
01	U	0
02	S	0
03	C	1
04	TS	1

安全域更新涉及位于客户端的故障检测模块和功能重构模块、安全域服务器上的故障监控模块以及客户端和安全域服务器之间的 TTE 通信。故障检测模块实时监控任务运行状态，并且对每个任务的运行状态进行故障判断，将任务故障状态添加到任务信息中，将任务状态信息打包，通过 TTE 通信发送到安全域服务器。安全域服务器上的故障监控模块分析接收到的数据包，若任务无故障，则结束本次行为，若任务发生故障，则定位该任务的安全域，从安全域内读取该任务的备份任务，然后将该任务重构信息发送到客户端的功能重构模块，同时修改该任务的安全域信息。

安全域的更新流程如图 5 所示。1)接收到客户端的任务状态信息后，分析该信息的任务故障标志；2)若任务无异常，则结束该流程；3)若任务发生故障，则定位该任务安全域；4)读取该故障任务的安全信息，并将该信息发送到客户端；5)更新该任务存储在安全域内的信息，将原备份节点修改为任务节点，原备份分区修改为任务分区，主备份设置为备份。

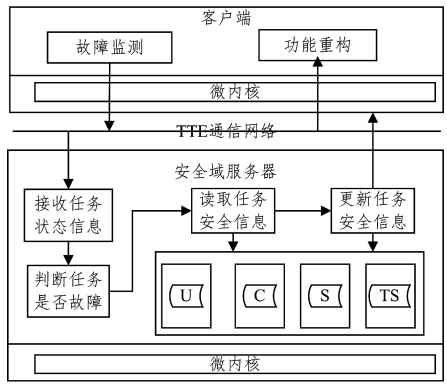

图 5 安全域更新原理

4.2 故障监控

该模块实现在固定时间间隔内循环获取客户端上任务的运行状态，并通过故障判定模块判定该任务的故障标志值[正常：0，故障：1]，将该任务状态信息发送到安全域服务器的故障监控模块。故障监控模块通过接收到的数据来判断该任务是否异常；若故障监控在固定时间内没有收到该任务信息，则判定该任务异常。该功能模块的流程如下：

(1)客户端的故障检测模式间隔固定时间搜集任务状态；

(2)客户端判断故障判定模块确定该任务的故障标志值；

(3)将该任务状态信息发送到安全域服务器的故障监控模块；

(4)安全域服务器的故障监控模块分析数据包，若任务发生故障，则修复该任务功能；

(5)若安全域服务器的故障监控模块在固定时间内没有收到客户端信息，则同样判定该任务故障。

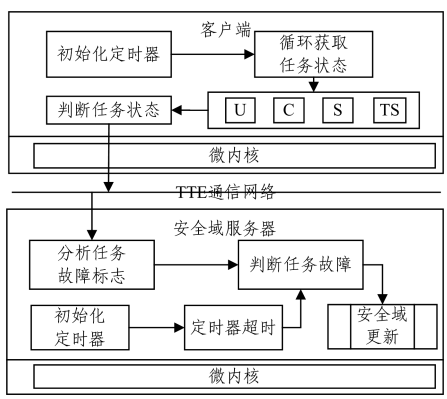

图 6 故障监控原理

4.3 功能重构

任务故障时，安全域服务器的故障监控模块接收到任务

状态信息，确定该任务发生故障，查询安全域内该任务的信息，将该故障任务的功能重构信息发送到客户端。同时，将删除安全域中该任务的安全信息的部分属性[所在节点，所在分区]，主备份属性设为备份，并重置属性[备份节点，备份分区]为空值。客户端上的功能重构模块接收到安全域服务器发送的故障任务的任务重构信息时，将该任务功能迁移。任务重构信息的数据格式如表 3 所列。

表 3　任务重构功能信息表

任务编号	安全等级	所在节点	所在分区	备份节点	备份分区
01	U	0	U	0	U
02	S	0	S	1	S
03	C	0	C	1	C
04	TS	0	TS	0	TS

该模块实现了故障任务的功能重构，保证了任务在发生故障后继续正常运行。

该模块位于客户端和安全域服务器上。该功能模块包括任务迁移以及原故障任务的挂起和新任务的继续运行。任务迁移指的是冷迁移，即将故障任务挂起，启动新任务。

该功能的实现需考虑两种情况：1)若备份任务节点与原任务所在节点相同，则安全域服务器的任务重构信息只需发送到原节点，原节点的功能模块启动新任务，并且挂起故障任务；2)若备份任务节点和原任务节点不同，则安全域服务器的任务重构信息要发送到两个节点，备份任务节点的功能重构模块启动新任务，原故障任务节点的功能重构模块挂起原任务。

功能重构的流程以节点迁移为例，如图 7 所示。

(1)安全域服务器判断出该任务故障后，从安全域数据库读取该任务信息；

(2)根据该任务信息确定该任务的迁移节点；

(3)组装该任务的控制信息，即发送到故障节点的故障控制信息和发送到迁移节点的迁移控制信息；

(4)发送控制信息到故障节点和迁移节点；

(5)故障节点根据故障控制信息查询故障任务的位置，并终止该任务；

(6)迁移节点根据迁移控制信息查询新任务的位置，并启动该任务。

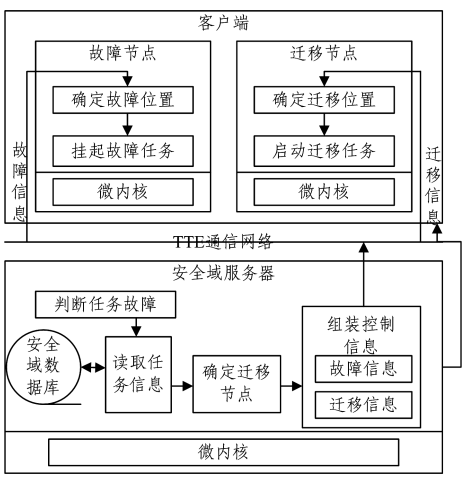

图 7　功能重构原理

结束语　为解决现有基于 MILS 架构的嵌入式系统因任务出现故障导致不能实现功能重构和任务安全迁移的问题，本文提出构建基于 MILS 架构的嵌入式系统多级安全域管理架构。通过详细描述面向实时任务的多级安全域管理、故障监控和功能重构等功能的工作原理，来达到在任务运行出现意外故障时能够实现任务安全迁移和功能重构的目的。该管理框架目前仅应用于 MILS 架构的操作系统，接下来将继续在航空电子操作系统 ACorOS653 上继续验证该工作原理。

参 考 文 献

[1] RUSHBY J M. Design and verification of secure systems[J]. AcmSigops Operating Systems Review，1981，15(5)：12-21.

[2] RUSHBY J M. Proof of separability a verification technique for a class of security kernels[C]// International Symposium on Programming. Springer，Berlin，Heidelberg，1982：352-367.

[3] ALVES-FOSS J，OMAN P W，TAYLOR C，et al. The MILS architecture for high-assurance embedded systems[J]. International Journal of Embedded Systems，2006，2(3/4)：239-247.

[4] SHIELD J，CHENOWETH S，PRENDERGAST P，et al. Information Associations for Multi-Domain Applications：Addressing Data Utility in Segregated Networks[C]// Proceedings of the Australasian Computer Science Week Multiconference. ACM，2019：4.

[5] 张灯，任晓瑞，胡宁，等. 基于 MILS 架构的安全中间件研究[J]. 电子技术，2013，42(7)：16-19.

[6] 张灯. 面向多重独立安全等级架构的安全通信机制研究[D]. 西安：西安电子科技大学，2011.

[7] 李健，陈革，叶晓芸，等. 基于 MILS 多级安全架构的远程调试机制[J]. 计算机工程，2016，42(1)：61-65.

[8] 杨姗. 基于 MILS 架构多级安全操作系统的若干关键技术研究[D]. 成都：电子科技大学，2018.

[9] 石鹏. 基于 MILS 架构的操作系统安全技术研究与实现[D]. 成都：电子科技大学，2016.

[10] HOM J. International Journal of Embedded Systems[J]. Ismir，2012：95-100.

[11] 崔西宁，王聪琳，裴庆祺，等. 基于 MILS CORBA 的多级安全分区通信机制[J]. 计算机科学，2013，40(5)：38-41.

[12] 成亚萌. MILS 系统中分区间的信息流控制[D]. 西安：西安电子科技大学，2012.

[13] 邢薇薇. 面向航空电子的分区内核关键技术研究[D]. 西安：西安电子科技大学，2011.

[14] TUCHS K D，HALMAI T，VAN SELM M. Multi-security domain management integration architecture for end-to-end service management in military networks[C]// 2011-MILCOM 2011 Military Communications Conference. IEEE，2011：1375-1380.

[15] 潘楠，李亚晖，沈玉龙. MILS CORBA 中的多级安全访问控制[J]. 互联网天地，2013(1)：50-54.

[16] 杨琼，周霆，胡宁，等. 一种面向 MILS 的多级安全文件系统的架构设计[J]. 科学技术与工程，2011，11(30)：7443-7447.

[17] HECKMAN M R，SCHELL R R，REED E E. A multi-level secure file sharing server and its application to a multi-level secure cloud[C]// MILCOM 2015-2015 IEEE Military Communications Conference. IEEE，2015：1224-1229.

[18] WRONA K，OUDKERK S. Integrated content-based information security for future military systems[C]// MILCOM 2015-2015 IEEE Military Communications Conference. IEEE，2015：1230-1235.