

基于 MILS CORBA 的多级安全分区通信机制

崔西宁¹ 王聪琳² 裴庆祺² 李亚晖³ 沈玉龙¹

(西安电子科技大学计算机学院 西安 710071)¹ (西安电子科技大学通信工程学院 西安 710071)²

(中国航空工业计算技术研究所 西安 710068)³

摘 要 随着航空电子系统的飞速发展,机载操作系统对保证不同安全关键级别的软件互不影响越来越严格,面对这种情况,多重独立安全级别(MILS)嵌入式操作系统应运而生。MILS架构的中间件层采用实时 CORBA 技术。同时 MILS CORBA 架构采用分区通信机制进行通信。为了满足分区通信的安全性和 MILS 架构对分区密级的严格控制,设计了基于实时 CORBA 技术的 MILS 架构的多级安全分区通信机制。提出了将 MILS IOP 作为实时 CORBA 的一部分来实现 MILS CORBA 架构的多级安全分区通信的机制。整个机制保证了不同密级的数据安全独立的传输,同时也保证了系统的整体安全性。

关键词 MILS, 实时 CORBA, 分区通信, 多级安全, 加密认证

中图分类号 TP311 文献标识码 A

Multiple Security Partition Communication Mechanism Based on MILS CORBA

CUI Xi-ning¹ WANG Cong-lin² PEI Qing-qi² LI Ya-hui³ SHEN Yu-long¹

(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)¹

(School of Communication and Engineering, Xidian University, Xi'an 710071, China)²

(Aeronautics Computing Technique Research Institute, Xi'an 710068, China)³

Abstract With the rapid development of avionics system, the requirement of ensuring different security classification software not to communicate in the avionic operate system is more and more strict. In this case, multiple independent levels of security and safety (MILS) embedded system was proposed. The middleware in MILS is Real-time CORBA (RT CORBA). And MILS CORBA is used partition communication to communicate with each other. In order to meet the security of partition communication and the strict control of the security classification in MILS, the multiple security partition communication in MILS architecture based on RT CORBA was proposed. The mechanism we proposed is that MILS IOP as a part of real-time CORBA can ensure to achieve multiple security partition communication in MILS CORBA. The whole mechanism can ensure that the transmissions among the data of different security classifications are independent. And it also guarantees the security of the whole system.

Keywords MILS, Real-time CORBA, Partition communication, Multiple security, Encryption and authentication

1 引言

在如今的航空系统中,机载操作系统越来越强调保证不同安全关键级别的软件之间互不影响这一安全需求。MILS (multiple independent levels of security and safety, 多重独立等级安全)架构将操作系统进行层次划分,分为应用程序层、中间层和微内核层3层。其中应用程序层和中间层位于不同的安全级别的分区中,保证不同安全级别分区的安全。由于 MILS 架构的微内核层十分精简,因此中间件层不仅要屏蔽底层操作系统的差异,而且要完成被内核层精简掉的相关系统服务。因而中间层是实现 MILS 架构的一个重要环节,亟需对 MILS 架构中的中间件进行研究。

MILS 架构的思想最先由 Dr. Jim Alves-Foss 等人^[10]提出,现在美国军方已经有成型的 MILS 系统投入使用,但国内 MILS 架构的研究仍处于起步阶段。文献[1]提出了一种 MILS 架构的实现机制,即利用 TNIU(trusted network interfaces units,可信网络接口单元)和分区中 Enclave 的划分来完成 MILS 架构的实现。文献[3]提出了 MILS 架构中的“红黑区”思想和一种实现方式,以保证不同安全级别的数据在通信时不被泄密。文献[4]提到了 MILS 架构中分区通信(PCS, partition communication system)的思想,即不同分区之间必须经由 PCS 的处理才能通信,以使整个系统通信更加安全。在实时 CORBA 的研究方面,美国华盛顿大学以 Douglas C. Schmidt 为首的工作组自行研制了 ACE 系统,该系统具有

来稿日期:2012-07-27 返修日期:2012-11-10 本文受航空科学基金(2010ZC31002, 2010ZC31001, 20101981015)资助。

崔西宁(1964—),男,博士生,研究员,主要研究方向为并行分布式操作系统、实时控制与容错技术、信息安全技术等, E-mail: cuixining@tom.com; 王聪琳(1989—),女,硕士生,主要研究方向为信息安全; 裴庆祺(1975—),男,CCF 会员,主要研究方向为数字内容保护、无线安全等; 李亚晖(1976—),男,工程师,主要研究方向为嵌入式操作系统、计算机网络、信息安全。

独特的体系结构,同时他们基于 ACE 系统实现了实时 CORBA 系统 TAO^[5]。在国内,东南大学计算机学院参加了国家 863 高技术计划九五重大攻关项目“面向 CIMS 并行工程集成框架关键技术”的子课题“面向 CIMS 并行工程企业层框架关键技术”的研究和开发工作,采用了遵从 CORBA2.0 规范的软总线系统。

上述文献只概述了 MILS 架构实现的思想或者论述了实时 CORBA 系统,并没有对中间件层在通信中起到的作用进行详尽研究。并且结合 MILS 架构操作系统、支持多等级安全的分布式网络中间件技术的研究,在国内还处于起步阶段。本文在 MILS 架构研究的基础之上,结合实时 CORBA 中间件技术,提出了基于实时 CORBA 技术的 MILS 架构的多级安全分区通信机制,以实现 MILS CORBA 架构的多级安全分区通信机制,保证不同密级的数据安全独立的传输。

本文第 2 节对 MILS 架构进行详细的阐述;第 3 节对 MILS CORBA 分区通信原理进行介绍,结合实时 CORBA 技术提出完成分区通信的重要工具 MILS IOP;第 4 节介绍 MILS CORBA 多级安全分区通信和分密级安全传输通道的实现方法;第 5 节是对所提方案的安全分析;最后对全文进行总结。

2 简介

航空领域中,机载航电分布式系统在现代航空技术中扮演着关键和重要的角色。随着微电子、计算机和信息技术的迅猛发展,机载分布式系统也面临着严峻的挑战。面对这样的挑战,MILS 架构应运而生。MILS 是一个在同一系统中执行不同安全级别应用的可验证的安全体系结构,其安全性的核心设计思想要求将操作系统进行层次划分。按照层次划分的思想,MILS 架构分为微内核层、中间件层和应用程序层,共 3 层。图 1 显示了 MILS 架构的结构。

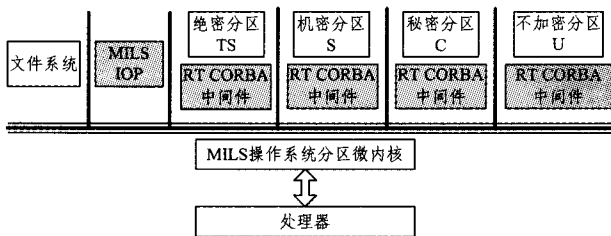


图 1 MILS 架构

MILS 架构中的微内核层十分精简,只负责数据隔离、信息流控制和损坏限制^[1]。中间件层主要负责屏蔽底层操作系统的差异以及完成微内核所精简掉的相关系统服务(如设备驱动和分区化通信软件)。中间件层采用的是实时 CORBA 技术,实时 CORBA 和实时操作系统结合完成中间件层的整体任务。最上层应用层仅仅负责实施应用层的安全策略。

MILS 架构中的分区按照不同的安全等级分为:绝密(TS)、机密(S)、秘密(C)和不加密(U) 4 个级别。每个级别有其独立的安全传输通道。在基于实时 CORBA 的 MILS 架构中,另有一个重要的分区是 MILS IOP,就是负责分区间的通信以及不同密级的安全独立传输。MILS IOP 作为 CORBA 的一部分,与其他分区的 RT CORBA 共同组成了 MILS CORBA 架构中的 CORBA 结构。下节将详细阐述 MILS CORBA 分区通信原理。

3 MILS CORBA 分区通信原理

实时 CORBA(Real-time CORBA,简称 RT CORBA)技术作为一种实时分布对象中间件技术,是 OMG(Object Management Group,对象管理组织)组织制定的 CORBA(Common Object Request Broker Architecture,通用对象请求代理体系结构)规范的一部分,可应用于机载高可靠分布式通信环境,用于构建开放、可重用、可互操作、易于移植的机载分布式系统,可有效提高机载分布式系统开发和集成的效率,降低开发和集成的难度。MILS CORBA 中实时 CORBA 的具体结构如图 2 所示。

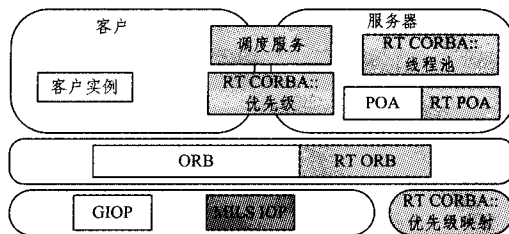


图 2 MILS CORBA 架构中实时 CORBA 结构

实时 CORBA 由客户端、服务器端、ORB 核心和传输规程 4 部分组成。客户端和服务端需要通过 ORB 和传输规程才能互相通信。在一次任务中,客户将需要完成的工作交给 ORB,由 ORB 决定由哪一个对象实例完成这个请求,然后激活这个对象,将完成请求所需要的参数传送给这个激活的对象。除了客户传送参数的接口外,客户不需要了解其它任何信息,从而实现位置透明性,为上层的应用层提供一个更为安全广阔的平台。

但与其他系统不同的是,航电系统要求严格的分区策略,所以通用的 RT CORBA 在航电系统中不能完全适应分区策略的要求。在 MILS CORBA 架构中,每个分区都有其相应的密级,所以不同的分区之间不能直接相互通信,必须通过分区通信系统才能通信。因而,RT CORBA 中相应的传输规程必须要满足 MILS 分区通信机制才能真正适应航电系统的需求。

在 MILS CORBA 架构中,MILS IOP 属于 GIOP(General Inter-ORB Protocol,通用 ORB 间协议)的扩展,它能实现分区数据的加解密以及独立传输,从而保证数据通信的多等级安全需求得到有效的满足,是 MILS CORBA 实现多级安全分区通信的重要部件。MILS CORBA 分区间的具体通信流程如图 3 所示。

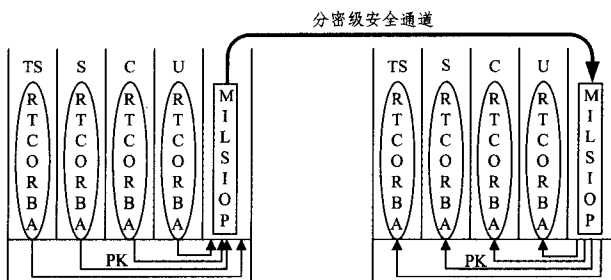


图 3 MILS CORBA 分区通信流程

每个分区的信息通过实时 CORBA 再经由内核层传送给 MILS IOP,MILS IOP 完成分密级的加解密并选择相应的分密级安全通道传输到目的端的 MILS IOP。目的端的 MILS IOP 收到消息后会进行相应密级的加解密,然后交由内核层

传输到目的分区,完成整个通信流程。具体的实现将在下一节详细介绍。

4 MILS CORBA 多级安全分区通信的实现

4.1 多级安全加解密机制

在 MILS 架构中,系统中的数据被分为多个安全级别,即绝密(TS)、机密(S)、秘密(C)和不加密(U) 4 类。它们之间的数据路由通道都是相对独立的,独立安全通道的示意图如图 4 所示。

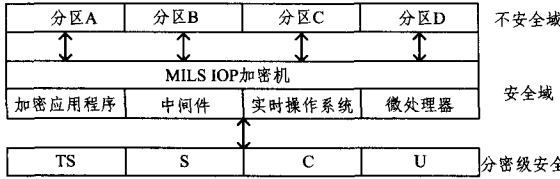


图4 独立安全信道

分区的数据可能存在不安全因素,处在不安全域当中。通过 MILS IOP 对数据消息进行加密,使得加密后的消息安全可靠,处于安全域当中,进而再在分密级的独立安全通道上进行传输,才能保证消息数据的安全可靠。独立安全通道可以借助虚通道等技术实施,从而保证每个不同密级的数据传输安全可靠地相互独立传输。

由于系统中不同分区的密级不同,因此不同的密级在 MILS IOP 中对应的加密方式也不相同。同时,每个密级的数据也拥有独立的传输通道,以保证数据流的安全。图 5 详细介绍了 MILS IOP 的机制。整个机制的主要部件分为 5 个:ORB 核心及其安全调用拦截器、GIOP、MILS IOP 地址解析器、分级加密模块和独立安全通道。其中 ORB 核心及其安全调用拦截器、GIOP 处在分区中;MILS IOP 地址解析器以及加密模块和独立安全通道则驻留在 MILS IOP 分区中,是 MILS IOP 的组件。

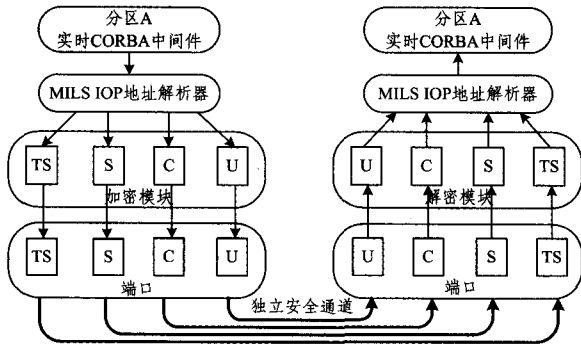


图5 MILS IOP 工作流程

ORB 核心是实时 CORBA 的核心部件,它相当于实时 CORBA 的“处理器”,负责 RT CORBA 的整体调度和实现。安全调用拦截器处于 ORB 核心和 GIOP 之间,仅对 ORB 可见,客户和服务端都不可见。安全调用拦截器对要发送的消息一无所知,只处理 GIOP 消息,保障消息层的完整性和机密性^[2]。GIOP 是实时 CORBA 之间通信的必要通信规程,消息要经过 GIOP 才能正常通信。MILS IOP 是分区通信的中心环节,首先它要解析 GIOP 传递过来的消息的目的分区,从而根据目的分区的级别进行加解密,最后由独立安全通道进行传输。在接收端,MILS IOP 负责对收到的消息进行解密和身份认证,认证成功后数据才有效。具体流程如图 5 所示。

分区 A、B 内的具体结构如图 6 所示。

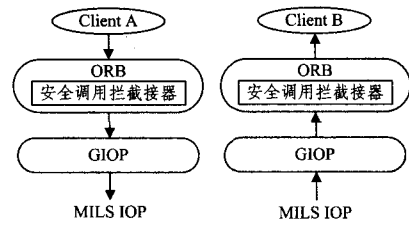


图6 分区 A、B 内的具体流程

结合图 5 和图 6,整个 MILS CORBA 多级安全分区通信流程如下:

- 1)分区 A 中的客户 A 发起通信的请求,将消息传递给 ORB 核心。
- 2)ORB 核心收到消息后,调用其中的安全调用拦截程序。安全调用拦截程序会重组原始的 GIOP 消息并传递给 GIOP。
- 3)GIOP 收到消息后,将源端和目的端的分区级别和消息传递给 MILS IOP。
- 4)MILS IOP 收到 GIOP 传送来的消息后,MILS IOP 地址解析器分析将要传送到的目的端的分区密级,然后选择相应密级的加密模块将消息传送到加密模块中。
- 5)加密模块分为 4 个级别的小加密模块,分别用于 4 个不同安全级别数据的加密。机密模块收到消息后,对消息进行加密。不同安全级别的加密方式和密钥均不同,加密完成后将加密后的数据发送给相应密级的传输端口。
- 6)不同安全级别的传输端口与相应密级的独立安全通道相连,负责数据的安全传输。
- 7)接收端的端口收到独立安全通道传送过来的加密数据后,将数据传送到与端口对应密级的加密模块中。
- 8)接收端的加密模块分密级地对加密数据进行解密和身份认证。身份认证通过后才将解密的数据发送给 MILS IOP。
- 9)MILS IOP 地址解析器收到解密的数据后,将消息整理成 GIOP 的消息模式,发送给 GIOP。
- 10)GIOP 将消息传送给安全调用拦截器,对消息进行分段,以满足 ORB 核心处理的需求。ORB 核心完成后续操作,整个通信过程结束。

4.2 加密模块流程

MILS IOP 一个重要的部件就是加密模块。MILS 架构中的分区是分密级的,不同密级之间的数据有严格的限制,所以要求不同密级间的加密方式以及密钥不同。为了满足不同密级的需求,MILS IOP 中也对消息进行了分密级加解密和认证,具体流程如图 7 所示。

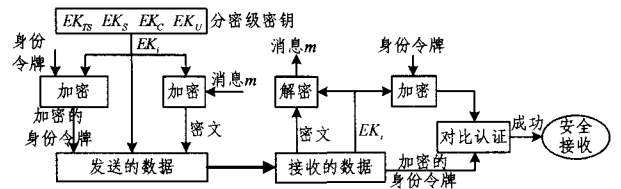


图7 分密级加解密流程

不同密级的分区拥有不同的身份令牌,同时也拥有不同的加解密密钥和加解密算法。图中 EK_{TS} 、 EK_S 、 EK_C 和 EK_U 分别代表绝密分区、机密分区、秘密分区和不加密分区的加解密密钥。系统根据发送分区拥有的身份令牌决定此次加解密选用的密钥和算法。

客户端发送的数据包括 3 个部分:加密的身份令牌、分密级密钥 EK_i 和加密的密文。每个密级拥有不同的密钥 EK_i 。可信第三方会向客户端和服务端颁发身份令牌并进行密钥管理, EK_i 参与身份令牌和消息 m 的加解密。在接收端会对收到的身份令牌进行认证,从而完成整个加解密和认证的过程。

1)发送端:用分密级密钥 EK_i 对身份令牌(ST)和消息(m)进行加密,生成加密的秘密令牌(EST)和密文(EM),然后和分密级密钥 EK_i 共同作为发送的数据(EST, EK_i ,EM)通过分密级安全通道发送给接收端。

2)接收端:接收端收到(EST, EK_i ,EM)后,用分密级 EK_i 对密文 EM 解密得到消息 m ,用分密级密钥 EK_i 对服务器端的身份令牌进行加密得到 EST_r,与收到的 EST 进行对比认证。若对比一致,则认证成功,解密得到的消息 m 为有效数据;若不一致,则认证失败,解密的消息 m 为无效数据,不予传输,并返回错误信息。

在加密过程中,密钥管理是一个重要问题。在航电系统中,数据须经蓝图的统一配置,系统工作的每一步都由蓝图机制进行描述,蓝图是系统管理和运行的灵魂。MILS CORBA 架构是适应航电系统的安全架构,它的配置也依托蓝图的配置。所以密钥管理依靠蓝图,由蓝图对密钥进行统一静态的配置,包括对身份令牌的分发、不同级别加密方式的确定和密钥的选择。

5 系统安全性分析

MILS CORBA 架构下的多级安全分区通信机制能够满足 MILS 要求的分区通信要求,同时也满足航空电子系统的高可靠、跨平台的通信要求。其安全性分析从以下 3 点进行论述:

1)ORB 核心和安全调用拦截器:实时 CORBA 能够很好地满足航电系统跨平台的要求。ORB 核心作为实时 CORBA 屏蔽底层差异的核心部件,负责对整个 CORBA 的数据信息进行统一的处理。安全调用拦截器位于 ORB 核心和 GIOP 之间,是 OMG 规定的“Security Service”标准提供的标准组件之一,旨在保证信息层的完整性和机密性,为整个系统提供更好的技术支持。

2)GIOP:作为实时 CORBA 的通用传输规程,GIOP 规定了一系列协议框架,可以支持底层网络的不同需求,也可以设计符合底层网络的协议。但是在 MILS 架构中,如果只有 GIOP 这一基本框架作为支撑,并不能完成多级安全分区通信,也不能保证 MILS 架构中不同密级分区对通信传输的要求。因此,需要对 GIOP 进行扩展,从而完成多级安全分区通信。MILS IOP 作为 GIOP 的扩展,能够很好地完成实时 CORBA 的通信任务,同时它基于实时 CORBA GIOP,能够和实时 CORBA 技术兼容,保证系统的正常运作。

3)MILS IOP:包括地址解析器、加密模块和传输端口。首先,MILS IOP 作为 MILS CORBA 架构的一部分,既继承了 MILS 架构的重要思想、满足了 MILS 架构的需求,又很好地结合了实时 CORBA 技术。MILS 安全性的核心设计思想要求将操作系统进行层次划分,其内核层十分精简,只提供数据隔离、信息流控制和损坏限制,而传统操作系统的需求全部交由中间件层完成,因此运行在每一个分区中的不同安全级别的应用就可以被独立地评估,可指数级地降低系统的安全隐患。同时,MILS IOP 又作为 GIOP 的扩展,也能很好地和实时 CORBA 技术融合。其次,地址解析器能够准确地解析

目的分区的地址和密级,为加密模块分密级加密做准备。再次,加密模块中为每个密级准备了独立的加密区,保证不同级别的数据不会发生相互干扰,使得数据加密的过程更加安全。不同的密级有不同的加密方式,保证了分密级数据的机密性。同时,加密模块在负责加解密的同时也负责对身份的认证,防止恶意的数据写入,保证分区内数据的干净。由于身份令牌由蓝图颁发,因此身份令牌的可靠性得到保证,从而对身份令牌的认证能够对对方的身份进行很好的认证。对于传输端口,每个密级拥有自己独立的安全传输通道,以保证数据安全快速的传输。独立安全传输通道可以抑制隐蔽通道。最后,虚通道技术的发展为独立安全传输的实现奠定了基础。

综上所述,通过 ORB 核心、GIOP 和 MILS IOP 三方的互补合作,能够很好地完成多级分区通信,使整个系统的安全性和可行性都得到了很好的保证。

结束语 未来高度综合的机载航电系统将是一个开放的分布式系统,各应用于系统间的通信需要满足异构、跨平台和强实时等任务特性。满足 MILS 架构的实时 CORBA 中间件技术构建的分布式对象调用机制能够提供与位置无关的、统一的系统应用中间件支撑平台,并且提供安全可靠的加密传输服务,使整个系统更加安全可靠。我们通过对 MILS 架构和实时 CORBA 技术的研究,设计了 MILS IOP,从而实现了 MILS CORBA 架构的多级安全分区通信机制,保证了不同密级的数据安全独立的传输。

参考文献

- [1] Alves J, Harrison W S, Oman P, et al. The MILS Architecture for High-Assurance Embedded Systems[J]. International Journal of Embedded System, 2005, 2(3/4): 239-247
- [2] 杨剑峰,等. 分布式系统原理与规范[M]. 北京:清华大学出版社, 2001
- [3] Boettcher C, Delong R, Rusby J, et al. The MILS Component Integration Approach to Secure Information Sharing[M]. IEEE, DASC, 2008; 1. C. 2-1-1. C. 2-14
- [4] Uchenick G M, Vanfleet W M. Multiple Independent Levels of Safety and Security: High Assurance architecture for MSLS/MILS[C]//MILCOM 2005. IEEE, 2005; 610-614
- [5] O’Ryan C, Schmidt D C. The Design and Performance of a Real-time CORBA ORB Endsystem[OL]. <http://europepmc.org/search/?page=1&query=The+Design+and+Performance+of+a+Real-time+CORBA+ORB+Endsystem>
- [6] Common Object Request Broker Architecture (CORBA) Specification, Version 3. 1[S]. OMG. 2008-01-04
- [7] Real-time CORBA Specification, Version 1. 2[S]. formal/05-01-04, OMG. January 2005
- [8] MILS CORBA Protection Profile, Internal Draft 0. 52[M]. September 2003
- [9] ASSAC Phase II Final Draft of Proposed Guidelines for System Issues[J]. Security Aspects, 2004, 6
- [10] Alves J-Foss, Harrison S, Oman P. UI MILS-CORBA Student Team University of Idaho[R]. MILS-CORBA Status Report
- [11] Alves-Foss D J, Oman P, Taylor C. Secure Middleware Architecture[M]. University of Idaho
- [12] High Granular Multi-Level-Security Model for Improved Usability, Dirk Thorleuchter[C]//2011 International Conference on System Science, Engineering Design and Manufacturing Informization. IEEE, 2011
- [13] Karuppan A S, et al. A New Robust Distributed Real Time Scheduling services for RT-CORBA Applications[C]//2008 International Conference on Computing, Communication and Networking. IEEE, 2008