第35卷 第18期 计 算 机 工 程 2009年9月
Vol.35 No.18 Computer Engineering September 2009
·安全技术· 文章编号：1000—3428(2009)18—0119—03 文献标识码：A 中图分类号：TP309

基于SVPN的HLA/RTI安全机制

孟宪国，朱元昌，邸彦强，李纪敏
(军械工程学院光学与电子工程系，石家庄 050003)

摘 要：针对传统高阶体系结构/运行支撑框架(HLA/RTI)分布仿真系统的链路安全问题，设计并实现基于仿真虚拟专用网(SVPN)的RTI安全扩展模块。阐述传统HLA/RTI体系的信息流程，得到联邦间主要信息链路，并对仿真系统的信息安全进行分析，给出RTI安全扩展的具体安全目标。对具体的实施方案进行论述，给出系统的软件功能模块之间的逻辑关系，分析SVPN环境下HLA仿真应用的运行过程。
关键词：虚拟专用网；高阶体系结构/运行支撑框架；RTI扩展；链路安全

HLA/RTI Security Mechanism Based on SVPN

MENG Xian-guo, ZHU Yuan-chang, DI Yan-qiang, LI Ji-min
(Department of Optical & Electronic Engineering, Ordnance Engineering College, Shijiazhuang 050003)

【Abstract】 A security extension of RTI in Simulation Virtual Private Network(SVPN) environment is put forward against the data link security problems of the traditional distributed simulation system based on High Level Architecture/Run Time Infrastructure(HLA/RTI) technology. The information process in the federation interaction is analyzed, and a concrete security requirement is presented according to the analysis. The implementation of RTI security extension is presented in detail. The logical relation of the software components is provided and the running mechanism of HLA –SVPN simulation application is analyzed.

【Key words】 Virtual Private Network(VPN); High Level Architecture/Run Time Infrastructure(HLA/RTI); RTI extension; link security

1 概述

高阶体系结构(HLA)提供了一套通用技术的规范，从而建立一个高层次仿真体系结构，使用该体系结构可以提高各种模型与仿真之间的互操作性。在各种仿真实体之间互交互过程中，仿真链路传递着各种信息，其中不乏关系国防、商业秘密的敏感信息，但是HLA规范却没有对仿真系统的安全性做出任何的要求。这样就对在广域网范围内进行大规模的仿真应用造成了严重的威胁，如何确保仿真系统的安全已经成为亟需解决的问题。

由于HLA规范没有对安全性提出任何要求，因此国内外的研究者对HLA安全性的研究工作一直没有停止。文献[1]讨论分布式仿真中的安全需求，尤其对HLA的安全性作了重点分析，并给出当时的实现方法和对未来的展望。文献[2]总结了这些工作并进行了深入的讨论。Filsinger Lubbes和Ozdemir提出了基于安全保卫(secutity guard)和可信代理(trusted angent)结构，并结合单层次安全性和多层次安全性(multi-lever security)阐述了实现过程。ONERA/CERT的Bieber等人把安全性作为RTI的一个子层，这种实现方法是以ONERA开发的HLA/RTI为基础的[3]。SecProxy[4]安全体系设想为像HLA一样的分布式仿真框架实现安全系统，它依旧是建立在分布式系统多层安全、访问控制(access control)和服务认证(service authentication)的安全需求上。

关于HLA安全性的研究多以安全体系为研究对象，很少讨论信息在链路上的安全。Elkins等人虽然提出了用IEIF标准IPSec来保证HLA安全[5]，但没有进行深入的讨论，也没有结合RTI具体实现。本文的目标是建立一个与RTI无关的HLA安全扩展服务模块，它能与不同实现的RTI程序相结合，部署在任意仿真应用中，具有很大的灵活性和通用性。

本文在Windows操作系统的NDIS底层驱动中实现IPSec协议，构建仿真虚拟专用网(Simulation Virtual Private Network, SVPN)，通过对RTI运行库的扩展，实现SVPN与RTI的无缝结合，从而解决仿真互交互、互操作中的安全性问题[6-7]。

2 HLA/RTI体系安全缺陷分析

2.1 HLA/RTI的信息流程

如图1所示，HLA采用一种“匹配”机制(或称“过滤”机制)，即根据预先定义的路径空间或隐式绑定的路径空间，数据生产者可以在其中创建区域或使用绑定路径空间的默认区域，并向RTI声明所生产数据的特性，同样数据消费者也可在路径空间中创建区域或使用默认区域，然后向RTI声明所需要数据的特性。RTI根据双方的数据特性，在数据生产者和消费者之间按照一定的规则进行匹配(看关联区域是否相交)，将生产者生产的数据发送给合适的消费者。

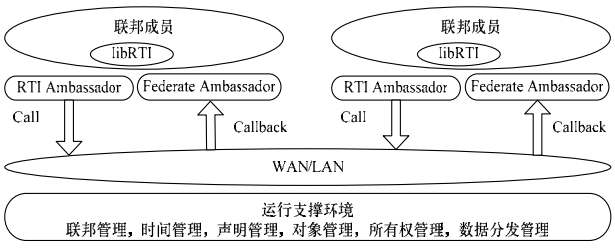

图1 HLA/RTI体系

联邦成员严格按照HLA规范进行开发，这样就可以与驻

作者简介：孟宪国(1979－)，男，博士，主研方向：分布交互仿真；朱元昌，教授、博士生导师；邸彦强，讲师；李纪敏，博士
收稿日期：2009-05-10 **E-mail：**mengxianguo@gmail.com

留在联邦成员的 RTI 大使进行无缝的通信联系，进而通过 HLA 的“匹配”机制，RTI 也就完成了联邦成员之间的桥接功能，从而不同结构的联邦成员之间就可以进行数据信息交换，达到他们之间的互交互、互操作。虽然 HLA 是一个多用途体系框架，但从网络信息安全的角度对 HLA/RTI 信息流程的分析，可以清晰地分辨出 HLA 体系中的 2 条信息交互链路：

(1)第 1 条信息链路是联邦成员与 RTI 大使之间的信息交互。RTI 大使是驻留在联邦成员计算机中的负责 RTI 通信进程，联邦成员的所有信息交互都要通过 RTI 大使来完成。

(2)第 2 条信息链路是驻留在联邦成员的 RTI 大使与 RTI 服务器之间的信息交互。由于根据 HLA/RTI 的消息处理机制，联邦成员之间的交互信息都要通过 RTI 服务器，因此他们之间的信息链路可以归结到这条链路中。

2.2 HLA/RTI 安全缺陷

在当今互联网广泛普及的时代，人们在享受它带来的便利的同时，信息安全也面临着重大的挑战。由于 HLA 的规范没有对安全性做任何的要求，因此 HLA/RTI 体系存在很大的安全隐患。如前所述，根据 HLA\RTI 信息流程分析，得出 2 条主干信息链路，在这 2 条信息链路上主要的安全问题有以下 3 个方面：

(1)没有身份验证。用户可以随意加入，联邦不清楚加入联邦的成员的身份，从而无从控制信息安全。非法联邦成员可能获取敏感信息。

(2)保密性。即敏感机密信息在传输和存储中被未授权者窃取。比如成员 1 发给成员 2 的信息被未授权的成员 3 或其他人获取。

(3)消息真实性。即攻击者篡改传输的数据，接收者不知道消息是否来自所需的发送者。比如成员 1 需要获取成员 2 发送的信息，攻击者伪造成员 2 发送信息。这种情形在网络安全中被称为主动攻击，则威胁信息的完整性、真实性和可用性。

2.3 HLA/RTI 安全目标

通过以上对 HLA/RTI 信息安全上的漏洞分析，可以看到 HLA/RTI 在广域网上信息安全问题主要集中在网络攻击、蓄意入侵、计算机病毒等方面。本文要实现的 HLA/RTI 安全扩展服务就是针对此问题设计的，它主要完成以下 4 个主要功能：

(1)具有身份认证功能，未授权用户不能加入联邦。

(2)加密联邦敏感数据，能确保传输的机密信息不泄露。

(3)完整性检查，确保传输信息的真实性得到保证。

(4)与 RTI 软件无缝结合、易于应用。

3 SVPN 框架结构

针对 HLA/RTI 体系链路安全方面的弱点，本文提出了基于虚拟专用网的解决方案，称为仿真虚拟专用网(SVPN)，由 SVPN 来保证分布仿真的链路安全。

如图 2 所示，基于 SVPN 的分布仿真框架由分布仿真门户、安全认证中心、仿真数据库、RTI 通信服务器和若干仿真节点组成。其中，分布仿真门户是整个系统面向用户的前端，含有整个系统概况和使用方法的介绍，同时还负责用户注册、仿真数据查询、仿真人员组织等多项功能。安全认证中心、仿真数据库、RTI 通信服务器是功能服务器，它们提供与分布仿真密切相关的安全认证、信息数据、通信保证等各项服务。仿真节点与 RTI 通信服务之间组成 SVPN，利用 IPSec 隧道协议来保护链路安全。

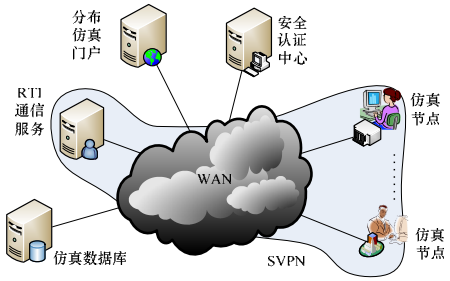

图 2 SVPN 整体结构

整个框架为广域网上的分布仿真应用提供了 HLA/RTI+SVPN 的解决方案。作为成熟的分布仿真中间件，HLA/RTI 提供了 6 大基本功能：联邦管理，时间管理，声明管理，对象管理，所有权管理，数据分发管理。这些功能为仿真信息的互交互和仿真应用的管理提供了有效的应用接口。SVPN 采用 IPSec 作为隧道协议，有力地保证了分布仿真的链路数据安全。仿真用户在开始分布仿真应用之前，需要在仿真门户上注册相关的信息，当申请被接受后，就可以根据仿真需要在仿真门户上组织人员和选取相关仿真资源。当参与仿真的节点准备就绪后，进入 SVPN 构建阶段，所有节点在安全中心领取本次仿真的密钥作为 IPSec 协议的密钥。为了保证分布仿真的实时性，尽量减少系统内开销，密钥的有效期为此次仿真过程。当 SVPN 建立起来以后，分布仿真就可以在 SVPN 环境中进行，SVPN 屏蔽了广域网的复杂设施有效地支撑了分布仿真应用。

4 RTI 链路安全机制实现

SVPN 的 IPSec 隧道协议满足了仿真应用的链路安全需求，但如何使 SVPN 框架与 HLA/RTI 中间件无缝集成，使 SVPN 建立自动化，成为在实现阶段考虑的主要问题。

4.1 RTI 链路安全扩展

如图 3 所示，SVPN 软件位于系统的网络层，在 Windows 操作系统中以 NDIS 网络驱动的形式实现。SVPN 本身具有与用户态进行通信的功能模块，通过封装将 SVPN 与 RTI 大使无缝连接起来，就构成基于 SVPN 的 HLA/RTI 扩展安全服务。

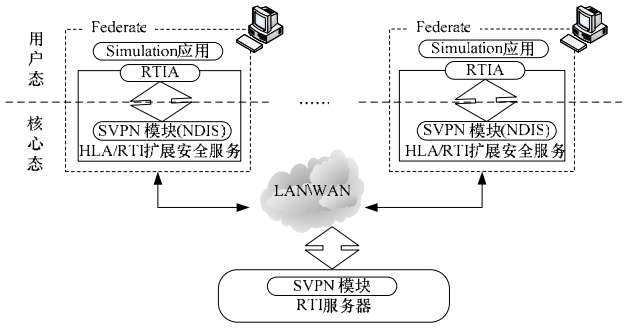

图 3 基于 SVPN 的 HLA 安全扩展服务

要达到使仿真应用数据受到有效保护的目的，需要在仿真应用的所有信息链路上对全部的数据包进行认证、完整性检查和加密，即联邦成员或 RTI 服务器与外界的所有数据交换都须通过 SVPN 模块的过滤。由于中间层驱动程序 SVPN 位于硬件驱动程序(链路层)和协议驱动程序(网络层)之间，因此发送到网络的所有数据包和从网络接收的所有数据包都须通过中间层驱动程序，从而有效地进行数据包的截获与解析。

4.2 软件结构与流程

整个扩展模块主要包括 3 个部分：SVPN 的用户态/核心态交互接口 DriverCom(类 TDriver)，RTI 应用程序接口(类

RTIA)和扩展后为仿真应用服务的 SRTI 应用程序接口(类 SRTI)，为使用方便，DriverCom 模块以静态库 IKElib 的形式进行封装。从类图中可以看出类 SRTI 通过聚合类 RTIA 和 IKElib，实现了对原有 RTI 功能的扩展，把 SVPN 的功能无缝集成起来。

SRTI 模块的数据流程如图 4 所示。仿真应用程序与扩展模块 API 进行符合 HLA 规范的数据交互，通过对 RTI API 初始函数的重新封装，调用 SVPN 用户态/核心态接口 DriverCom，在初始化 RTI 的同时，利用从网站获得的密钥，根据 IPSec 协议建立仿真 VPN。一旦 SVPN 建立成功，RTI 在广域网上的通信数据都将受到 IPSec 的保护。

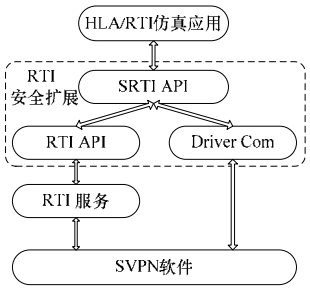

图 4　RTI 安全扩展模块数据流程

4.3　仿真联邦的建立与退出

基于 HLA/RTI 的仿真应用过程实际就是仿真联邦建立、仿真应用执行、仿真联邦销毁的过程。图 5 描述了在 SVPN 环境下，RTI 仿真联邦建立、退出的动态过程。

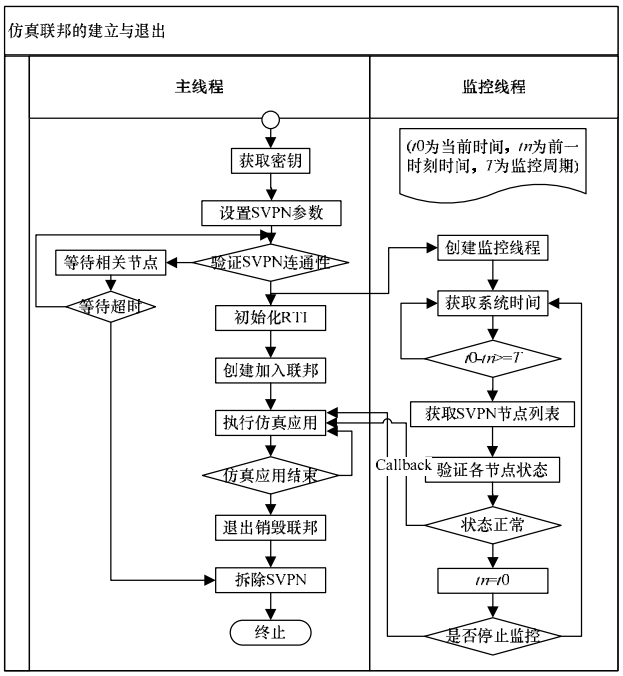

图 5　仿真联邦的建立与退出

SVPN 环境下的仿真过程包括 SVPN 和 HLA 联邦 2 个部分生命周期的管理。考虑到广域网的不可控，设计监控线程以确保整个 SVPN 状态正常。整个过程分为以下 5 个阶段：

(1)SVPN 建立阶段。仿真节点从仿真门户得到参与仿真的相关节点信息，从安全中心获知此次仿真的密钥。根据这些信息仿真应用在调用 RTI 安全扩展模块进行 RTI 初始化时，模块自动先进行 SVPN 的初始化工作。SVPN 参数设置完备后，会进行 SVPN 连通性验证工作，以保证所有仿真节点均已加入仿真虚拟专用网中。如果 SVPN 建立超时，则本次仿真任务失败，提示用户进行下一次尝试。

(2)联邦初始化阶段。SVPN 环境建立以后，仿真节点进入联邦初始化阶段。此阶段中与普通的 HLA/RTI 仿真应用基本相似，仿真节点创建和加入联邦，注册交互对象和属性值。

(3)仿真进行阶段。基于 SVPN 的仿真联邦建立后，仿真应用开始使用 RTI 进行分布仿真交互。SVPN 软件把 RTI 发送的仿真数据按照隧道协议进行封装，同时把网卡上传的仿真数据解封上传。这样，SVPN 为分布仿真应用提供了端到端的链路保护。上层的 RTI 软件并不知道 SVPN 软件的存在，从整个角度讲 SVPN 可以与任何 RTI 版本无缝结合，应用灵活度大大增强。

(4)SVPN 状态监控。由于广域网环境中网络拓扑复杂、不可控因素多，因此在设计中采用“心跳”策略来监控 SVPN 的连通性。同时，轮询的事件间隔 T 是可变的，以在复杂的网络环境中减少额外的系统开销。当发现 SVPN 状态出错时，监控线程会调用相应的错误处理回调函数通知仿真应用，由仿真应用来决定是否终止仿真。

(5)仿真结束阶段。仿真应用结束后，RTI 安全扩展模块首先退出、销毁 HLA 仿真联邦，然后终止监控线程并撤销 SVPN，释放相关系统资源。

5　结束语

针对传统 HLA/RTI 仿真系统的链路安全问题，本文设计了仿真虚拟专用网与 RTI 软件相结合的解决方案。通过开发 RTI 安全扩展模块，把 SVPN 软件和 RTI 的功能无缝结合到模块中。在 HLA 联邦的生命周期中，SVPN 环境自动建立和撤销，增加了系统的易用性。同时 SVPN 提供了对仿真链路安全的保证，满足了分布仿真的需求。SVPN 环境已成功地应用到某分布仿真训练系统中[8]，具有较高的实用价值。随着应用的深入，RTI 安全扩展模块将在封装形式、监控间隔选取等方面不断完善。

参考文献

[1] Filsinger J, Lubbes H Q. System Security Approach for the High Level Architecture[C]//Proceedings of the 14th Workshop on Standards for Interoperability of Distributed Simulation. Orlando, Florida, USA: [s. n.], 1996.

[2] Ozdemir H T. Security Issues in High Level Architecture[Z]. (1997-10-20). http://www.npac.syr.edu/projects/cps714fall97 hwl/cj 97hto.

[3] Bieber P F, Cazin J, Siron P, et al. Security Extensions to the ONERA HLA RTI[C]//Proceedings of Fall Simulation Interoperability Workshop Conference. Orlando, Florida, USA: [s. n.], 1998.

[4] Andrews D. Proposal for the Performance Impact of SecProxy Security Protection on a HLA Federation[D]. Ballarat, Australia: Bachelor of Computing, University of Ballarat, 2002.

[5] Peters B A, Smith J S, Medeiros D J, et al. Security Issues in High Level Architecture Based Distributed Simulation[C]//Proc. of the 2001 Winter Simulation Conference. Washington D. C., USA: IEEE Computer Society, 2001.

[6] 韩　超, 鞠儒生, 黄柯棣. 基于 Web 服务的 HLA 仿真系统扩展[J]. 计算机工程, 2006, 32(24): 20-22.

[7] 李　频, 唐家益, 陈丹伟, 等. 虚拟专用网分类和比较研究[J]. 计算机工程, 2006, 32(22): 133-135.

[8] 邸彦强, 朱元昌, 孟宪国, 等. 基于网格技术的多用户多任务模拟训练系统[J]. 系统仿真学报, 2008, 20(3): 643-647.

编辑　索书志