自主可控的战术信息栅格安全传输技术研究

蒋昊东，朱恩成，高明远

（北京控制与电子技术研究所信息系统工程重点实验室 北京 100038）

摘要：本文研究了战术信息栅格系统的安全传输技术，分析了战术信息栅格信息传输的安全需求，结合 SSL 协议，给出了一个安全传输系统的实现。最后，针对战术信息栅格实时传输协议的安全特性进行了分析探讨。

关键词：战术信息栅格；SSL 协议；序列化；

0 引言

近年来兴起的军事信息栅格，是军事信息系统综合集成领域的新兴技术，它的核心是一个庞大的、分布于军事信息网络各个节点上的、协同工作的软硬件系统，其基本目的是利用信息技术的最新成果，对各种军事资源进行综合集成，实现高度共享和全面协作，提高一体化联合作战能力。

战术信息栅格基于栅格技术、嵌入式信息技术构造了一个战术层次上创新性的综合集成体系框架，将各类异构的、动态的传感器节点、武器平台节点、指控节点和其它软硬件资源有机融合。为战术信息的实时应用与按需服务提供了实用可行的解决思路和实施方案，能够对战术信息进行搜集、存储、传输、处理、分发，并对各类战术资源进行一体化的组织、管理，支持作战节点随遇接入、即插即用，支持信息的实时共享和作战行动的全面协作。

1 战术信息栅格安全需求

由于军事信息系统的特殊性，将栅格应用于军事，面临的最大挑战是安全问题，包括系统的安全和信息的安全，不同级别的用户，只能享有不同层次、不同粒度的信息使用权，确保己方信息及时、准确、不间断地获取、传输、处理和使用，同时阻止敌方对信息的获取和使用。

战术信息栅格网络由于是开放性的无线网络，解决其安全问题，需要做足够的安全配置和管理，需要采取与保护传统网络相同的安全措施，采用足够的安全策略，然后还要采用其他的一些特别措施。在传输层和应用层做出一种主动的信息安全保障措施，才能有效地弥补传统安全防护技术的缺陷，最大限度地提高系统的信息安全传输和保障能力。

战术信息栅格不安全因素主要集中在无线窃听，身份假冒和篡改数据上，这些不安全的因素可能导致许多不同类型的攻击。所以战术信息栅格系统的安全需求主要包括下面三个方面:

(1)身份认证

因为无线网络中用户不用直接连接网络，所以攻击者更容易非法登入网络，为了有效的防止非法用户登入，需要一定的身份认证机制来验证用户的合法性。

(2)数据加密

为了确保无线局域网中的传输数据只有合法接收者才能读取，信息必须具有机密性，为了实现这一点，通常使用综合性能良好的加密算法对数据加密，只有拥有密钥的接收方才能解密，而没有密钥的攻击者即使获得密文，也无法获知相应的明文。

(3)信息完整性认证

由于无线网中信息容易丢失或被攻击者修改并转发，因此需要进行信息完整性认证，包括对信息的完整性以及正确性进行验证。

2 战术信息安全传输系统设计

针对上节所说的战术信息栅格安全需求的三个方面：认证、加密和数据完整性，本节论述战术栅格安全传输系统的设计。

2.1 SSL 协议

SSL 协议 (Secure Socket Layer :安全套接字层)是 TCP/IP 协议集中目前较新的安全协议。可以实现通信过程的安全保密，它虽然是针对 Internet 环境提出的，但由于属于套接协议，具有与上层应用协议与下层网络协议无关性的特点，所以实际上在其他网络的通信中也可以使用。

安全套接字层协议(SSL)是在 Internet 基础上提供的一种保证保密性的安全协议。它能使客户/服务器应用之间的通信不被攻击者窃听，并且始终对服务器进行认证，还可选择对客户进行认证。SSL 协议要求建立在可靠的传输层协议(例如:TCP)之上。SSL 协议的优势在于它是与应用层协议独立无关的。高层的应用层协议(例如:HTTP，FTP，TELNET)能透明的建立于 SSL 协议之上。

SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作。在此之后应用层协议所传送的数据都会被加密，从而保证通信的保密性。

SSL 协议由 SSL 记录协议和 SSL 握手协议两部分组成。

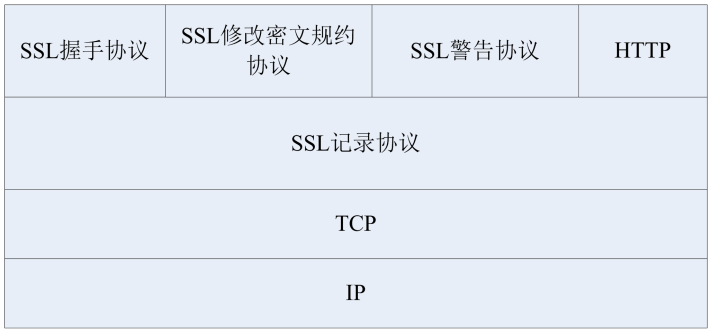

图 1 SSL 协议栈

2.2 数字签名技术

2.2.1 数据的完整性

数据的完整性是认证消息、检验数据是否被篡改的技术，散列函数是实现数据完整性的主要手段。散列函数 H 是一个公开的函数，它将任意长度的报文 M 变换成固定长度的散列码 h，散列函数表示为 h=H(M)，它生成报文所独有的“指纹”。散列函数是一种算法，算法的输出内容称为散列码或者报文摘要，报文摘要惟一地对应原始报文，如果原始报文改变并且再次通过散列函数，它将生成不同的报文摘要，因此散列函数能用来检测报文的完整性，保证报文从建立开始到收到始终没有被改变和破坏。运行相同算法的接收者应该收到相同的报文摘要，否则报文是不可信的。因此一般通过对报文摘要进行处理来实现数字签名和完整性检查功能。

2.2.2 数字签名技术

数字签名是在数据信息上附加一些数据或对数据信息作密码变换，这种附加数据或密码变换使接收方能确认信息的真正来源和完整性，并且发送方事后不能否认发送的信息，而接收方或非法者不能伪造或窜改发送方的信息。数字签名类似于手工签名，是手工签名的数字实现。数字签名的过程见图 2 所示。

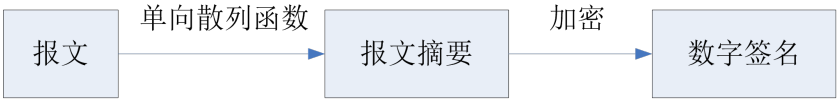

图 2 数字签名过程图

数字签名通过如下的流程进行:

(1)采用散列算法对原始报文进行运算，得到一个固定长度的称为报文摘要(MessageDigest)的数字串。

(2)发送方生成报文的报文摘要，用自己的私有密钥对摘要进行加密来形成发送方的数字签名。

(3)这个数字签名将作为报文的附件和报文一起发给接收方。

(4)接收方首先从接收的原始报文中用同样的算法计算出新的报文摘要，再用发送方的公开密钥对报文

附件的数字签名进行解密，比较两个报文摘要，如果值相同，接收方就能确认该数字签名是发送方的，否则就认为收到的报文是伪造的或者中途被篡改了。

2.3 战术信息栅格实时信息的安全传输系统设计

2.3.1 系统概述

较为完整的信息安全传输系统必须提供身份认证、加密及完整性验证功能。SSL 的基础上，结合了加密技术和数字签名技术，最终得到一个较为完整的战术信息安全传输系统。系统由四个模块构成:服务器与客户端认证模块、客户端用户登录模块、战术环境信息安全传输模块和密钥管理模块，这四个模块和 OpeSSL 相结合实现战术信息的安全传输。系统的结构图如图 3 所示。

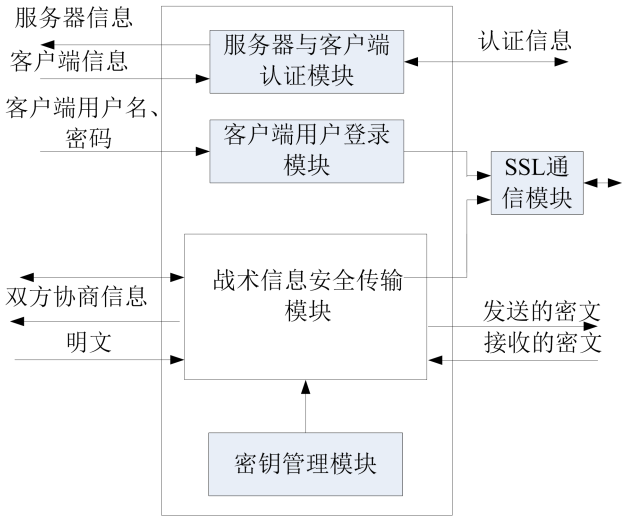

图 3 安全传输系统结构图

其中战术信息安全传输模块是由加密算法、数据签名两个子模块组成，在传输中，客户端用户根据战术信息加密级别的不同，选择不同的加密方式，从而保证战术信息安全、准确的在栅格网络中传输。

密钥管理模块包括 DES 密钥生成子模块、RSA 密钥生成子模块和密钥管理子模块组成，构建强健的密钥管理对系统的安全起着决定性的作用。

2.3.2 数字签名模块的设计

2.2.2 介绍的数字签名实现了对信息来源的签别，但对传送的信息本身却未保密。理论上只要截获到传输的信息，就能够得到信息明文。为了同时实现数字签名和保密通信，结合对称密钥加密技术和公开密钥加密技术的优点，对数字签名的实现流程作了改进。克服了对称密钥加密中对称密钥分发困难和公开密钥加密中加密时间长的问题，使用两个层次的加密来获得公开密钥技术的灵活性和对称密钥技术的高效性，保证信息的安全性。

由于改进后数字签名技术是把要发送的数字签名用接收方的公钥进行加密，只有接收方的私钥才能解开被加密的数字签名，而其他人不能解开，这样就确保了只有接收方才能准确地接收到数字签名，从而接收到发送方的报文。

具体步骤如图 4、图 5 所示。

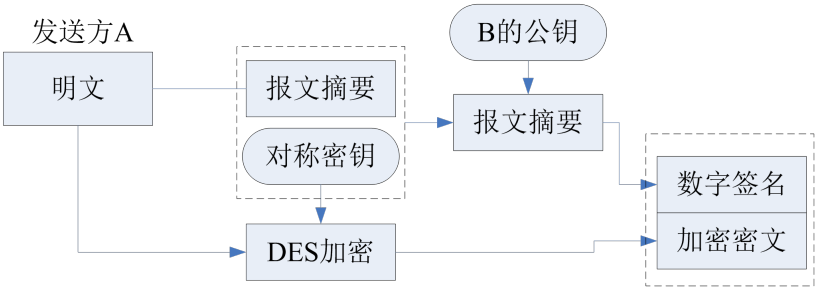

图 4 生成数字签名流程

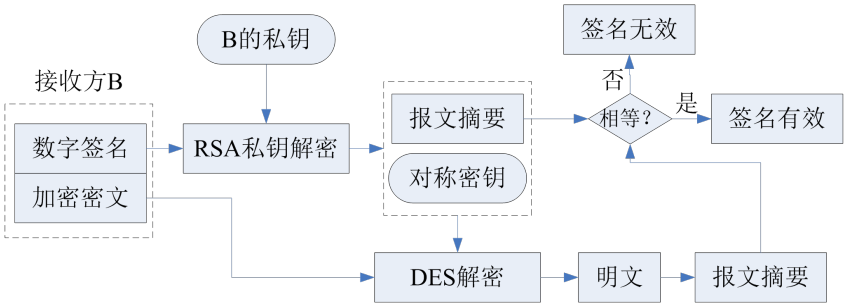

图 5 验证数字签名的流程

改进后的数字签名技术在外层使用公开密钥加密技术，因此可以获得公开密钥技术的灵活性。由于内层的对称密钥长度通常较短，从而使得公开密钥加密的相对低效率被限制在最低限度;而且由于可以在每次传送中使用不同的对称密钥，系统有了额外的安全保证。

2.3.3 SSL 通信模块的设计

SSL 协议位于 TCP 层之上，应用层以下，为数据通信提供安全支持，数据由应用层经过它流出的时候被加密，再送往 TCP 层;而数据从 TCP 层流经它这一层时被解密，然后再送往应用层。采用 SSL 协议后，服务器和客户端能够相互认证对方的身份，并在两者之间建立安全连接。这里详细讨论 SSL 通信模块的设计问题。

2.3.3.1 通信模块的工作流程

SSL 通信模块为通信双方之间数据的安全传输提供服务，如图 6 所示，整个模块结构可以分为两部分:服务器和客户端。从外部来看，服务器和客户端使用的安全通信系统都包括两部分内容:初始化握手部分和数据传输部分，具体对应于 SSL 安全协议的“握手协议”和“记录协议”。

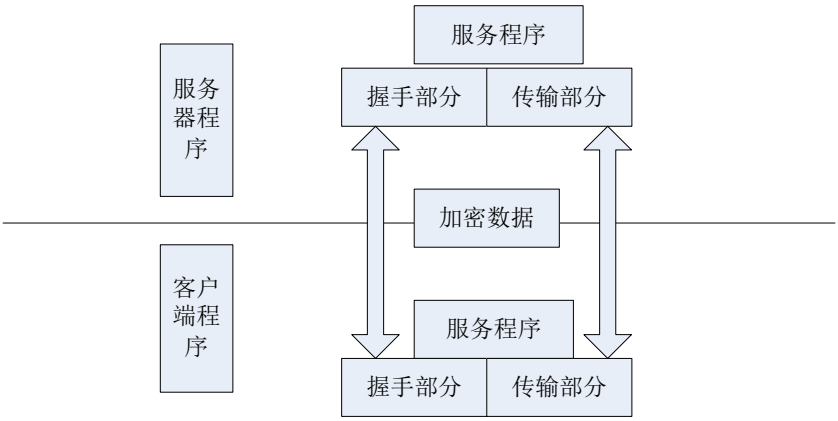

图 6 SSL 通信模块结构图

2.3.3.2 客户端实现

客户端的开发都是调用 OpenSSL 函数实现的，按照功能划分，主要分为:初始化过程、连接过程、身份验证和数据传输几部分。

1.初始化过程

总体上讲，初始化必须完成以下工作:

(1)初始化 SSL 库

(2)选择会话连接所使用的协议

(3)申请 SSL 会话的上下文环境 CTX

(4)加载自己信任的 CA 列表

(5)加载私有密钥和数字证书

(6)为随机数发生器抽取种子数据

(7)设置加密套件

2.连接过程

一旦客户端初始化了 SSL 上下文环境，就准备连接到服务器，然后进行 SSL 握手了。由于 SSL 协议是在 TCP 层之上工作，所以首先要建立一个 TCP 套接字，再建立 SSL 连接。

(l)建立 TCP 连接

(2)SSL 套接字的绑定

(3)建立 SSL 连接

3.身份认证

身份认证是 SSL 通信模块重要的组成部分，在通信的过程中通信双方可以验证对方的身份，以确定正在和想要连接的实体进行通信。过程如下:

(1)获得对方的证书

(2)验证证书的真实性

(3)验证证书的身份

4.数据传输

在进行连接后，服务器和客户端之间已经建立了一个安全的数据传输通道，此时在服务器和客户端之间传输数据和普通的 TCP 套接字类似，就可以进行数据读写了，只需写入要传输的信息，所有的信息都是由 OpenSSL 的库函数进行加密处理后通过网络进行传输，在接收端，则进行读取信息。

2. 3. 3. 3 服务器端实现

服务器等待客户端的 TCP 连接，并在接受连接后初始化一条 SSL 连接。一旦建立连接，它就从客户端读取数据，或写入数据发送到客户端。服务器的实现过程与客户端类似，按照功能也可以分为以下四部分: 初始化过程、连接过程、身份认证过程、数据传输。

3 战术栅格实时消息序列化协议

基于战术信息栅格的网络化作战需要大量的实时信息交换，但战术环境下可用带宽有限，且现有网络协议及服务协议存在效率低、实时性差、低性能等缺点，必须研究适合我军现有战术通信系统的实时交互协议。

在栅格信息系统中，各种格式的实时消息传输大量存在。现在普遍使用的方式是定义各式各样的消息帧格式，通信双方按照事先定义好的消息帧格式来封装、解析具体栅格消息。

但随着信息栅格系统变的越来越复杂，通过网络传递的消息类型、数据结构不断增多，实时性要求也越来越严格。设计通信协议时不仅要考虑系统内部的传输协议，还涉及各系统之间的数据交互，多系统、多平台之间在体系结构、操作系统、编程语言往往存在诸多不同，信息交互必然涉及数据的序列化和反序列化问题。传统的交互数据结构定义方式变得日趋复杂、维护困难、编程实现容易出错、文档众多，并且不具备可扩展性，任何字段的增删、调整、改动均有可能造成不可预料的后果。

上述问题可以结合现有序列化协议，通过设计更可靠、扩展性良好的数据传输协议解决。序列化是将对象状态转换为可保持或传输的格式的过程。与序列化相对的是反序列化，它将流转换为对象。

整个序列化/反序列化的流程如图 7 所示：

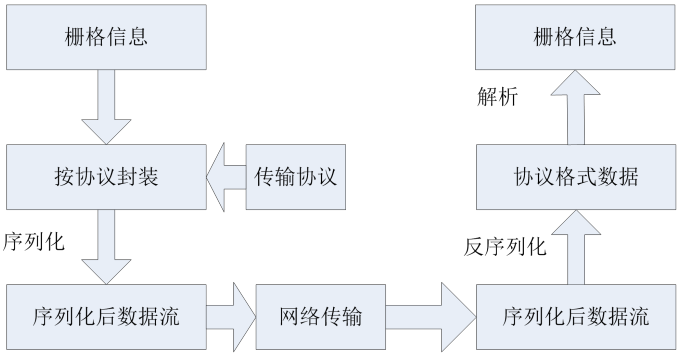

图 7 序列化/反序列化流程

采用序列化协议在信息安全传输带来两方面好处。

一是该序列化过程对网络传输阶段来说是“黑箱处理”，是隐蔽不可见的。由此使网络传输中的栅格信息得到一定程度的加密保护，即使网络攻击者窃取了网络中数据，也只能得到二进制的编码数据，只要序列化协议没被窃取，数据仍然是安全的。

二是序列化的过程也可以加上压缩、加密等措施，以实现再次加密和减少传输数据量的目的。

4 结语

战术信息栅格从根本上解决信息实时共享和信息按需分配问题，是我军实现信息化建设跨越式发展的重要途径，是未来战术环境下实现战术信息共享的基础设施。自主可控的实时信息传输是战术信息栅格的必然需求，战术栅格信息序列化机制和安全传输系统在某种程度上解决了安全的实时传输。但如何在现有网络安全技术的基础上更进一步地设计、实现战术信息栅格的安全体系框架，则是待研究和解决的问题。

参考文献：

[1]陈永凯，顾绍元.基于 AJAX 技术实现浏览器与服务器的异步通信[J].福建电脑，2006，10（9）: 87- 88.

[2]郜盼盼，贾庆轩，高欣. 一种基于 SSL 的“双密钥机制”认证密钥协商协议[J] .计算机技术与发展, 2012, 16(9) : 219- 221.

[3]付沙，何诚. 基于 SSL 协议的安全网络通信的理论和实现[J].计算机与现代化，2006，11

[3] Gu Yunhong, Grossman R L. UDT : UDP-based Data Transfer for High-speed Wide Area Networks[J]. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2007, 51(7) : 1777- 1799.