**编号**

**版本**

**深度包和访问控制分析报告**

**项目名称：**

**项目负责人：**

**编写：**

**校对：**

**审核：**

**批准：**

**单位:**

**年 月 日**

目录

[一、现状综述 2](#_Toc472522830)

[二、深度包检测和访问控制技术 3](#_Toc472522831)

[2.1工业控制系统防护模块数据包处理流程 3](#_Toc472522832)

[2.2访问控制 3](#_Toc472522833)

[2.2.1数据信息提取 5](#_Toc472522834)

[2.2.2安全策略设计 5](#_Toc472522835)

[2.3 深度包检测 13](#_Toc472522836)

[2.4 以Modbus TCP协议为例的深度包检测技术的实现 14](#_Toc472522837)

[三、结束语 17](#_Toc472522838)

**关于深度包检测和访问控制技术的分析报告**

近年来，随着工业化与信息化进程的不断交叉融合，越来越多的信息技术应用到了工业领域。各种工业自动化控制系统正快速地从封闭、孤立的系统走向互联（包括与传统IT系统互联）从工业控制系统自身来看，随着信息技术的发展，工业控制系统开始广泛采用信息技术，开放的软硬件技术、协议标准的应用以及工业控制系统和信息系统的集成使工业控制系统接口越来越开放，减弱了系统与外界的隔离。从外部环境来看，工业控制系统漏洞发现、攻击技术和攻击人员能力正不断增强，工业控制系统面临日益升级的安全威胁。

2010年的Stuxnet和2011年的Night Dragon，Duqu，Nitro，以及2012年的Flame等标志性事件，将这一严峻形势进一步推向了历史舞台的中央。其中还涉及到西门子等国内外知名工控系统制造商的产品。从已经发生的攻击看，现有的信息安全防护措施难以完全保证将攻击阻止在控制系统外。必须研究控制系统面临的信息安全威胁，通过为控制系统开发专门设计的信息安全防护模块提升控制系统的信息安全，从而保证控制系统运行的安全、稳定和可靠。

# 一、现状综述

工业控制系统信息安全产品目前还不多见，主要集中在用于隔离工业控制系统和lT系统的隔离网关，这其中以中科网威、力控华康，加拿大多芬诺公司的工业防火墙、西门子中国研究院研发的Janus安全网关为代表。这类设备更多针对TCP/IP和OPC协议，部署在PLC前段或控制区域和管理区域之间，针对ModbusTCP、DNP3.0等工业控制协议的深度防御不足，对控制系统的防护不足。国内厂商如和利时在今年尝试推出了安全工业交换机，这种设备可以帮助控制系统抵御来自二层的攻击，对三层以上的攻击无法提供防御。

本文所提出的工业控制协议深度包检测技术(Deep packet inspection，DPI)是相对普通报文分析而言的一种新技术，不仅检测网络层和传输层数据包头部更能够对4 至7 层的报文信息进行分析，而且深入到应用层数据包的有效载荷所封装的内容中，搜寻合法或非法的内容以决定是否允许数据包通过。针对ModbusTCP、DNP3.0等工业控制协议进行深度的解析检测，是保障工业控制系统信息安全的重要并且有效的手段。

访问控制是网络安全防范和保护的主要策略，其目的是防止网络资源被非法用户访问和使用。访问控制是保证网络安全的核心策略之一。网络通讯的核心协议TCP/IP。利用了网络协议的层次性和相关协议的知识，对TCP/IP 协议族中各种数据包的源IP地址、MAC地址、源端口、目的IP地址、目的端口等进行分析，能快速、准确地判断攻击特征是否存在。

# 二、深度包检测和访问控制技术

## 2.1工业控制系统防护模块数据包处理流程



图2-1 数据包处理流程

如图2-1所示首先进行访问控制，检测分析IP包的四层以下的内容，包括源地址、目的地址、源端口、目的端口以及协议类型是否符合预制规则，如果出现异常则输出到报警日志并拒绝该数据包通过。顺利通过访问控制后，则进行深度包检测，深入到应用层数据包的有效载荷所封装的内容中，搜寻合法或非法的内容以决定是否允许数据包通过。如果数据非法则输出到报警日志并拒绝通过，反之则顺利通过防护模块。

## 2.2访问控制

访问控制（Access Control），指的是根据定义的策略，来规定客体对某种资源的访问获取权限，或者变更的权限等，并且防止非法客体对资源的过渡使用。在网络中，根据不同的角度，对于访问控制有着不同的理解。从访问控制的对象来看，其控制的对象由信息实体、信息流、事件流以及时间流组成。一般所说的访问控制主要指的是对信息实体和信息流的控制。而从访问控制在网路通信中的控制范围来看，其可以对整个网络，即物理层、数据链路层、网路层、传输层以及应用层实现访问控制。访问控制一般包含了三元组，即主体（subject）、客体（object）、控制策略（Attribution）。其中，主体通常指的是进行访问操作或者存取请求的一方，一般是用户或者用户的某一进程。客体指的是将被使用的程序或者存取的数据。操作指的是主体对客体采取的一定的措施。许可指的是规定的主体对客体的访问权限。访问控制原理如图2-2所示。



图2-2 访问控制原理

访问控制技术框架如图2-3所示，其中包括了两大部分，即数据信息提取和安全策略。数据信息提取是安全策略实现的前提，安全策略是整个访问控制技术实现对攻击防御的核心。



图2-3 访问控制技术框架

### 2.2.1数据信息提取

数据信息的提取是整个访问控制模型的基础。其得到的数据包信息直接被用于策略的制定和数据的控制。所以其得到数据包信息的准确性，直接影响着安全策略的实现。

数据信息提取的目的在于将网络通信中的数据包包内信息提取出来。因为攻击者制造的各类攻击，都是通过修改数据包中的各种信息或者监听、截取网络中的数据包，然后进行伪装、构造等恶意数据包来实现攻击。

数据信息提取的总体框架如图2-4所示。



图2-4数据信息提取框架

### 2.2.2安全策略设计

安全策略在整个访问控制技术中属于核心部分，其实现的是对提取到的数据信息进行某种操作。所以，对其设计的好坏程度，直接影响到访问控制能否有效的识别和防御攻击。

策略总共分为了三大部分，即是针对基于IP非法访问攻击的安全域策略，针对基于端口非法访问攻击和部分欺骗性攻击的白名单访问控制策略，以及针对syn flood攻击的安全策略。



图2-5安全策略设计总体框架

1. 安全域策略

安全域（security region），在传统IT网络中是指同一区域内具有相同的安全保护需求，相互信任，并且具有相同的安全访问控制和边界控制策略的子网或者网络，而且相同的网络安全域共享一样的安全策略。

在工业控制网络中，资产、设备的通信、访问以及操作并没有传统IT网络那样复杂。而且，控制网络中生产过程所涉及的控制设备与执行设备之间的关系，即是配置、组态、下发、刷新、监测等一系列的控制流程，在某种程度上都是比较固定的。如图2-6所示，工程师站A、操作员站B以及PLC三者之间共同完成一个生产项目，将其划分为安全域1。而工程师站B和控制器则一起完成另一项目，将其划分为安全域2。这样划分的意义在于，它们都工作在自己的安全域内，都有自己的一套域内安全策略，而且如果发生了跨域的非法操作行为等攻击行为，则更容易被发现以及处理。所以，制定合理的安全域策略能够更高效的、更精确的保证工业控制网络中的通信安全。



图2-6 安全域划分

根据工业控制网络中资产间的通信行为、操作行为等，以及结合攻击的攻击特点来制定。具体设计方法如图2-7所示：

1. 对整个控制网络进行风险评估，并确定资产的重要等级。
2. 明确各资产所属的系统结构层次，即企业管理层、监视控制层以及现场设备层，并获取其IP地址等能够表明其所处位置的信息。
3. 根据各资产在网络中实现的功能或者操作，将完成同一控制过程或者同一环节的资产，划分在同一安全域内。
4. 标记安全域，记为，其中，表示资产设备位置信息。



图2-7 安全域设计

1. 针对IP地址欺骗的安全策略设计

欺骗性的攻击一般包括了多种欺骗类型。对于IP地址和MAC地址的欺骗性攻击来进行策略设计。该类攻击一般分为域间IP欺骗和域内IP欺骗。如图2-8所示，演示的是一个IP欺骗的全过程。由于在安全域内，所以假设攻击者X已经获得了域内的访问权限，目标设备A和被冒充设备B是信任关系。在实施欺骗前，攻击者X先通过一定手段使得设备B不能工作。然后攻击者X向设备A进行多次试探，了解ISN（初始序列号）的规律。之后，攻击者X伪造源地址为设备B、ISN为m的SYN包向设备A请求连接。设备A在收到所谓的“设备B”的请求包后，向“设备B”返回SYN+ACK包其中包括A的ISN为n，确认号为m+1，并等待“设备B”返回的ACK包。攻击者X在收到A返回的SYN+ACK后，通过某种手段估算出了应答号为n+1，并构造源IP为B的ACK包，发送给设备A。设备A收到ACK后，此时就认为自己是和设备B建立了连接。但实际上是攻击者X伪装的“设备B”。此后，攻击者X就可以对A进行更深层次的攻击了。



图2-8 IP欺骗过程分析

综上分析，IP欺骗主要利用的是设备间的信任关系，伪造IP地址以及利用三次握手的通信规则，伺机伪装发动攻击。由于MAC地址是全球唯一的，所以一般针对IP欺骗攻击的防御手段是将IP地址与MAC地址进行绑定构造一张表，然后通过匹配来实现防御。此种方法在一定程度上能够识别出IP欺骗，特别是在工业控制网络中，各个资产间的通信、访问、操作行为是比较有规律性的。但是如果攻击者同时获得了目标的IP地址和MAC地址，那么上述绑定的防御方法就失效了。而通过图2-8欺骗过程，可以发现，攻击者X在第五步返回给设备A的ACK包时，其中要返回一个n+1的应答号，而这个应答号是攻击者X自己估算的。而我们则可以通过构造出复杂的ISN，增加攻击者估算难度，使其不能够成功实现连接。鉴于此，设计一种基于IP和MAC地址绑定结合ISN重构造的安全策略，其框架如图2-9所示：



图2-9 针对IP欺骗的安全策略

1. 当收到SYN包时，对其解析，并通过IP地址和MAC地址表进行IP与MAC的匹配。如果匹配失败，则丢弃此包，成功则进入下一步。
2. 通过cookie计算的方法对ISN进行重构，再载入SYN+ACK包中，并返回给发送方。
3. 下一时刻收到ACK包后，对其返回的确认号进行cookie计算，并进行验证。如果验证成功则进行连接，验证失败则不予以连接。
4. 白名单控制策略设计

在划分好安全域后，其使得各个划分好的区域之间有了一个有效的通信防护。然而，对于域内的安全防护，也需要制定相关的安全策略。如图2-10所示，在安全域内，工程师站A被允许对访问PLC1的502端口，而工程师站B被禁止。但是在某时刻，工程师站B的被感染或者工作人员恶意操作访问PLC1的502端口达到攻击目的。更有严重情况，如图2-11所发送的欺骗性攻击，攻击者通过某种手段获得安全域内合法的权限或某合法资产的信息。再伪装成合法的资产，欺骗域内其他资产，建立合法连接，发送恶意篡改的数据内容如对某PLC的线圈数据进行修改，导致工艺出差错或者严重生产事故发生。所以，针对上述攻击类型，在安全域内制定相应的安全策略显得尤为重要。



图2-10对于端口的非法访问



图2-11 基于操作内容的欺骗性攻击

对于安全域内的安全防护，通常的模型如下所示：





其中，指的是源地址，指的是源端口，指的是目的地址，指的是目的端口，指的是对数据操作，总共包括3种操作：

：指的是对数据进行允许通过操作。

：指的是对数据进行丢弃操作。

：指的是允许数据通过，但同时发送报警。

此模型只是对网络层和传输层的数据信息设定了安全策略，但是对于上述的通过篡改应用层中操作相关的数据内容而进行的欺骗性攻击却无能为力。鉴于此，本小节根据上述攻击在网络层、传输层以及应用层所表现出的攻击特点，提出基于白名单的安全策略，设计模型如下所示：





其中，表示源地址，表示源端口，表示目的地址，表示目的端口，表示功能码，表示操作对象起始地址，表示操作对象的数目，表示对数据的操作，而白名单策略的操作是允许，即。

基于白名单策略的设计过程如图2-12所示：

1. 在划分好的安全域中，根据安全域内各资产设备间的通信行为、访问行为、操作行为等基于数据包交换的特点，定义合法的通讯集合。
2. 将上述定义好的合法通讯集合，通过本小节设计的白名单模型予以表示出来。
3. 对其他不包括在上述合法通讯集合的数据，全部予以丢弃操作。



图2-12 白名单策略设计

1. 针对syn flood的安全策略设计

对基于IP地址和操作内容的欺骗性攻击作了安全策略的设计，但是攻击者还可以通过感染安全域的操作系统或者伪装合法的IP地址，向目标机发送大量的伪造TCP连接请求来发动syn flood攻击。如图2-13所示，是TCP三次握手正常情况下和异常情况下的syn flood攻击。在正常三次握手情况下，Host A向Host B发送SYN连接请求包，Host B接收到请求包后，向Host A返回SYN+ACK包。在Host A接收到返回的包后，再向Host B返回一个ACK包，至此表示三次握手成功。而在发动syn flood攻击时，攻击者通过某种手段获得Host A的信息后，伪装成Host A不断向Host B发送SYN包，而Host B则不断的发送SYN+ACK进行回应。与此同时，攻击者不再返回ACK包，使得握手一直处于半连接状态。而Host B的系统资源一直被积压在其连接队列中，最终Host B的资源被耗尽，甚至造成系统崩溃。此种情况若发生在工业控制网络中，将导致严重生产事故发生，后果不堪设想。所以，针对syn flood攻击的安全策略设计，也显得很有必要性。



图2-13 TCP三次握手正常与异常情况

针对syn flood攻击的防御，一般传统的方法是利用syn proxy技术，其原理是通过提高连接资源的利用率来实现防御。但是该类方法在出现攻击流量比较大时，却无法起到好的防御效果。鉴于此，根据上述攻击特点，并结合syn cookie技术，设计了一种防御syn flood的安全策略，其策略框架如图2-14所示。假设在大量SYN 包到达Host B时，针对不同IP地址来的SYN包，进行一个计数统计，并设置一个阈值。那么，当来自同一IP地址的SYN包的个数小于所设阈值时，允许再到达的SYN数据包通过，如果是大于了所设阈值，就丢弃再到达的SYN数据包。而对于到达的来自同一IP地址的ACK包，由于此类数据包是三次握手中，Host A和Host B已经建立了半连接才会收到ACK包，说明了Host A和Host B之间属于正常的连接。此时，因为已经明确了是正常的连接，所以对此ACK包对应IP地址的SYN包的计数进行减一。其他IP地址传来的SYN包和ACK包也按上述方法进行处理。当数据包到达算法模块后，在表中进行查找是否有相匹配的IP，如果没有，直接将数据包信息写入表中。如果有，则判断此数据包是什么类型的数据包，如果是SYN包，则判断表中flag（数据包个数阈值）大小，若大于n，直接丢弃此数据包，若小于或等于n，flag进行加1，并将此包转发。如果是ACK包，则对flag减1，并转发此数据包。



图2-14 针对syn flood安全策略设计框架

## 2.3 深度包检测

深度包检测技术即DPI技术是一种基于应用层的流量检测和控制技术，当IP数据包、TCP或UDP数据流通过基于DPI技术的带宽管理系统时，该系统通过深入读取IP包载荷的内容来对应用层信息进行重组，从而得到整个应用程序的内容，然后按照系统定义的管理策略对流量进行整形操作。

不同的应用通常依赖于不同的协议，而不同的协议都有其特殊的指纹，这些指纹可能是特定的端口、特定的字符串或者特定的Bit 序列。基于“特征字”的识别技术通过对业务流中特定数据报文中的“指纹”信息的检测以确定业务流承载的应用。

图2-15所示为基于特征匹配的深度包检测。



图2-15 深度包检测流程图

深度包检测包括深度命令解析和深度内容分析。命令解析是通过对数据包中的命令进行分析，检测出违反协议规范的行为，实现对已知攻击的检测，如果防火墙发现访问命令中发现入侵、攻击性命令，就将数据包做异常处理，将其丢弃。深度内容分析是对数据包中的内容进行匹配检测，由于网络协议具有高度的规则性，对各协议类型的包所包含数据的类型有严格的规定，如果数据类型或有效载荷与协议要求不一致，则表明存在数据异常或发现伪装攻击可能性，即进行异常处理。

深度包检测的任务就是把当前数据包中应用层载荷的特定内容与协议标准定义的期望值进行比较,检查其是否符合协议标准的规定,从而确定应用层协议的种类，以及应用的内容。如图2-15深度包检测首先对工业控制协议进行协议标示符检测，数据长度检测，功能码检测，地址检测，数据类型，数值大小的检测。

## 2.4 以Modbus TCP协议为例的深度包检测技术的实现

Modbus TCP协议最初主要被用在与其他网络相隔离的工业控制网络中，除了对可靠性、实时性和效率的要求外，并未考虑到协议本身的安全问题，而且目前Modbus管理组织也没有在协议中添加任何安全特征。同时，Modbus TCP协议底层基于TCP/IP技术，因此标准以太网的底层协议缺陷也被继承下来。

当前Modbus TCP协议的安全缺陷主要有以下几类：

1）缺少认证保护

缺少认证主要表现在仅需一个合法的功能码和一个合法的地址就可以通过TCP协议的502端口建立起一个Modbus通信会话。未认证的控制指令对控制过程造成严重威胁。

2）缺少授权保护

缺少访问控制机制，任何角色都可以对目标进行访问控制。缺乏对用户的分类以及对用户权限的划分，使得任何用户都能够进行任意的操作控制，实现任何的目的。

3）缺少加密保护

缺少加密表现在整个应用层的Modbus协议使用明文传输，通信过程中双方信息被第三方获取后，可以很轻易的解析出功能码、地址、数据等协议内容，为攻击者入侵提供了便利。

Modbus协议通信方式有两种：一种最常见的是为应答机制，Modbus主机发送请求（比如控制指令）给从机（比如执行器）进行一定操作，随后从机发送应答给主机；另外一种是广播的形式，主机发送广播给所有的从机，从机执行一定的操作而不需要给主机发送应答数据包。另外Modbus协议没有任何的安全防护机制。上述特点使得Modbus通信容易受到攻击。

现有的基于Modbus TCP协议工业控制系统的深度检测方法，主要是针对存在的攻击提出解决方案以及从Modbus TCP协议包和通讯特征入手进行异常检测。但是现有的方法大多存在着片面性和不完备性，尤其对于新型病毒和未知类型的攻击入侵行为缺乏有效的防护。

通过对Modbus TCP协议的分析可知，Modbus是基于主机与从机之间的工业控制协议，通信采用请求/响应的方式进行。工业控制网络中一般不允许随意更改相关设备的软件及其设置，也不允许更改网络结构。所以对于Modbus TCP协议的安全防护通常采用硬件防护模块的方法，将其串联在主机与从机之间，如图2-16所示。



图2-16 防护结构图

对Modbus TCP的防护一般采用入侵检测的方法，入侵检测按照行为可分为两种模式：误用检测和异常检测。误用检测是将所有可能的入侵行为归纳总结并建立一个模型，访问者发起的行为如果符合这个模型则会被判别为入侵；异常检测是建立一个正常的访问行为模型，如果访问不符合该模型的行为，则会被判定为入侵。

误用检测与异常检测各有自己的优缺点：误用检测直接与可能的入侵行为进行匹配对比，因此误用检测的误报率较低，但是不可能将所有的入侵行为归纳到模式库中，所以漏报率就会较高。异常检测刚好相反，它的漏报率很低，但是不符合正常行为模式的行为不一定就是入侵行为，所以异常检测的误报率较高。这就需要用户根据自身的需求以及它们各自的特点来选择检测模式，现阶段很多用户普遍采用两种模式相结合的策略。

Modbus TCP属于应用层的通信协议，普通的访问控制无法提供应用层的检测与识别能力，需要借助深度包检测技术对应用层的Modbus提供安全防护。将深度包检测技术应用到入侵检测中，实现对Modbus TCP协议的全面防护。防护流程图如图2-17所示，Modbus TCP数据分别经过了深度包解析，深度包过滤与异常检测。按照该流程设计Modbus TCP协议的安全防护方法：



图2-17 Modbus TCP防护流程图

1.深度包解析：通过深度包检测技术对Modbus TCP协议应用层的内容进行解析识别，获取Modbus控制指令的关键信息，为后续的过滤与检测提供信息基础。

2.深度包过滤：通过Modbus关键信息选项设置过滤规则，建立特征规则库，使所有的Modbus数据与规则库中的过滤规则进行比对，对合法的数据予以放行，非法的数据进行阻止。深度包过滤针对单个数据包逐一进行检测，该方法属于误用检测的范畴。

3.异常检测：对于高隐蔽性的攻击与恶意行为，针对单个数据包的深度包过滤方法通常难以发现。异常检测能够总结正常通信时的流量特征，若攻击行为发生时，必然扰乱正常的流量特征，异常检测以此来发现新型病毒以及未知的攻击等。

# 三、结束语

本文通过分析现有的工业控制系统信息安全产品的性能分析，针对控制系统的不足，提出了深度包检测和访问控制技术的策略。对硬件模块进行了设计与实现，并对典型的工业控制协议进行模拟实验，在基于Modbus Tcp协议通信实验中，对于协议内容中功能码、线圈地址、数据包长度、端口号、协议标识符等做全面的深度包解析，实现访问控制和通信管理,从而有效的实现防护功能。