控制系统 Safe-Sec 安全通信方法研究

Study on the Safe-Sec Safety Communication Approach for Control System

宋　岩[1,2]　王天然[1]　徐皓冬[1]　杨志家[1]　王　铭[1]

(中国科学院沈阳自动化研究所[1],辽宁 沈阳　110016;中国科学院大学[2],北京　100081)

摘　要:针对控制系统功能安全和信息安全两类安全属性整合问题,提出了 Safe-Sec 网络模型。该模型利用纵深防御策略兼顾功能安全和信息安全,能有效对抗针对控制网络的蓄意攻击。针对经典功能安全方法无法对抗攻击的问题,提出了 Safe-Sec 安全通信方法。该方法在保障功能安全的前提下,大大提高了对抗蓄意攻击(如人为伪装攻击、重放攻击、数据篡改攻击等)的能力。最后对该方法的有效性和时间开销进行了分析。Safe-Sec 通信方法满足了控制系统安全通信对功能安全和信息安全的需求。

关键词:功能安全　信息安全　安全通信　控制系统　工业以太网

中图分类号:TP212　　**文献标志码**:A

Abstract: Aiming at the integration issue for two types of security attributes of functional safety and information security, the Safe-Sec network model is proposed. By utilizing the strategy of defense in depth, the functional safety and information security are both taken into account by the system; the deliberate attacks against to the control network can be effectively confronted. For the attacks that unable confronted by conventional functional safety methods, the Safe-Sec safety communication method is proposed. Under the premise of ensuring functional safety, the capability of fighting deliberate attacks, such as disguised attacks, replay attacks, and data tampering attacks, etc., is greatly improved. The analysis on effectiveness and time overhead of this method is given. The Safe-Sec communication method satisfies the demands for functional safety and information security of safety communication of control systems.

Keywords: Functional safety　Information security　Safety communication　Control system　Industrial Ethernet

0　引言

控制系统有功能安全[1](functional safety)和信息安全[2](information security)两类安全属性。前者针对潜在的危险和伤害,利用冗余和诊断等技术,避免设备失效带来灾难性后果;后者针对系统信息的完整性、保密性等。功能安全的概念由 IEC 61508[1]给出,即“不存在不可接受的风险”。典型的安全应用如列控连锁系统、安全仪表系统[3-4]、核电控制系统、紧急停车系统等[5]。控制系统信息安全问题在网络技术和无线技术大规模渗透的背景下也越来越突出[7]。目前,这两类安全问题都备受重视,但如何将二者有机结合起来是一个巨大的挑战[8-9]。对于一个典型的安全关键应用而言,既需要保障功能安全,又需要保障信息安全[10-11]。

本文针对控制系统的功能安全需求和信息安全需求,构建 Safe-Sec 安全网络模型,设计了一种 Safe-Sec 安全通信方法。

国家 863 计划基金资助项目(编号:2013AA040301);

国家自然科学基金资助项目(编号:61004068)。

修改稿收到日期:2012-10-18。

第一作者宋岩(1980-),男,现为中科院沈阳自动化研究所在读博士研究生,助理研究员;主要研究方向为工业通信和安全。

1　Safe-Sec 网络模型

本节讨论控制系统网络结构的形式及面临的风险和威胁,然后给出结构方面的解决方法,并提出 Safe-Sec 网络模型。

1.1　控制网络面临的风险和威胁

按现场级通信技术特点的不同,控制网络可分为总线类、工业以太网类、无线类等。

从信息安全角度看,专有的总线类网络由于协议和物理层的专有,面临的信息安全威胁最小。工业以太网因兼容商业网络,被攻击的可能性较大。工业无线开放信道面临的“威胁”最大。控制系统的功能安全风险和信息安全威胁如表 1 所示。

专有的总线协议并不是保障信息安全的有效手段。主流的现场总线协议如 FF H1、Profibus-DP、Profibus-PA 等,其协议文本是完全公开的。对于工业以太网,由于其物理介质和部分数据链路层与商业网络和桌面系统兼容良好,利用免费的报文分析工具即可直接对其进行分析、仿真和研究,其攻击难度进一步下降。对于工业无线,由于开放信道的技术特点,如果没有信息安全手段,则对其进行攻击没有任何门槛。

表 1　功能安全风险和信息安全威胁

Tab. 1　Functional safety risks & information security threats

网络类型	黑通道破坏	协议栈破坏	窃取	攻击	风险程度	威胁程度
现场总线	插入、乱序、破坏、寻址错	协议栈	通信监听	数据修改	风险高	威胁小
工业以太网	插入、乱序、延迟、破坏、寻址错、碰撞	参数错、内存跳变	通信监听、后门	泛洪、重放、伪装、篡改	风险高	威胁较大
工业无线		延时、丢包、重复	通信监听、伪装、信道阻塞	漫游者攻击、通信劫持	风险低	威胁很大

解决这些风险和威胁需要从网络结构和通信方法两方面进行。

1.2　Safe-Sec 网络结构模型

为满足前述控制网络的功能安全与信息安全需求,构建了 Safe-Sec 网络结构模型,其示意图如图 1 所示。

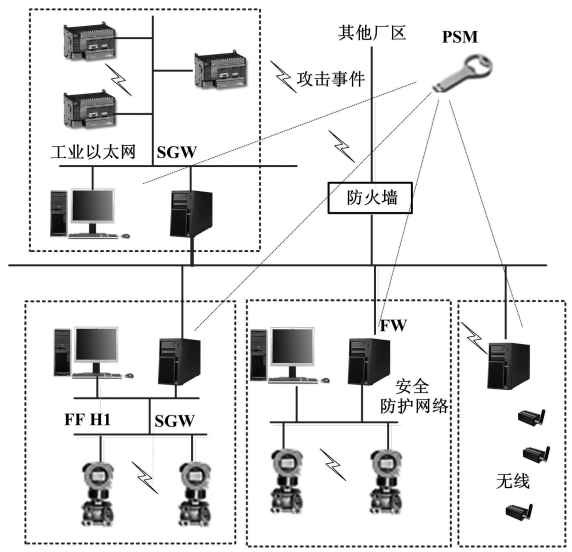

图 1　Safe-Sec 网络结构模型

Fig. 1　Safe-Sec network structure model

图 1 中,网络分为现场级网络、工厂级网络和公共网络 3 个层次。

1) 现场级网络实现控制功能和防护功能。现场级网络共有 4 种类型:①工业以太网,用以完成运动控制;②FF H1,用以完成过程控制;③工业无线网络,用于采集设备状态、震动、环境参数等,进行故障诊断和预测;④“安全防护网络”,它是工厂的安全防护系统,实现紧急停车、火气控制等。

2) 工厂级网络包括工程师站、信息安全主机等。现场级网络通过安全网关(security gateway,SGW)与工厂网络隔绝,这样就可以保证即使有恶意攻击,也需要花费相当大的代价才能侵入。工厂级网络通过防火墙在整个工厂范围内形成隔离区域(demilitary zone,DMZ)。

3) 公共网络提供不同厂区之间联系的通道,公共网络是不可信网络。

在不同的网络层级,功能安全与信息安全的优先级不同。

① 功能安全/信息安全的优先级

在 Safe-Sec 网络结构中,“安全防护网络”功能安全优先级高于信息安全,信息安全是为功能安全服务的。在现场级网络“工业以太网”、“FF H1”和“工业无线”子网中,由于主要任务是完成控制,涉及配方/工艺保密,所以一般信息安全的优先级更高。

② 控制网络信息安全策略

控制网络信息安全采用纵深防御策略防护,现场级网络通过 SGW 与工厂级网络连通;工厂级网络通过防火墙与公网连通。在工厂内部形成控制网络 DMZ 区域。安全防护网络通过网关与基础过程控制系统(basic process control system,BPCS)网络互联。

1.3　Safe-Sec 网络模型分析

本节分析 Safe-Sec 网络结构对抗威胁的有效性。威胁分为 3 类:网络外部威胁、现场级网络内部威胁、安全防护网络威胁。

针对网络外部威胁,使来自公网/企业网的全部流量需要经过图 1 中的防火墙才能进入隔离区域。通过制定白名单机制,可杜绝大部分外部攻击。

针对现场级网络内部威胁,使来自工厂级网络的命令需要通过两方面检查:先要经过安全网关(SGW)设备过滤;然后如果需要操作现场设备,需通过密码校验(加密机制和认证机制)。通过这两步的防御,可以消除大部分来自以太网的威胁。

来自安全防护网络的威胁小,但可能造成严重后果,根据图 1 可知,安全防护网络是与工厂级网络防火墙相隔离的。为减少安全防护网络威胁,可通过以下几种途径:①通过小型防火墙隔离信息安全计算机和工厂级网络的连接,防止来自以太网的攻击;②通过 Safe-Sec 通信方法,对抗余下的攻击,包括插入、数据破坏(人为和自然的)、伪装等。

2　Safe-Sec 安全通信方法

本节讨论控制系统两类安全通信的整合,对于功

能安全通信,多数总线通信行规如 FF H1、Profibus 等都给出了其解决方案,但功能安全通信没有足够强大的对抗入侵、攻击的能力。针对功能安全和信息安全两方面的不同约束,本文提出了一种 Safe-Sec 安全通信方法。该方法既保障功能安全,也保障信息安全,并且具有较高的效率。

2.1　传统功能安全通信技术的不足

综合 FF H1、ProfiSafe 通信行规,传统的通信功能安全常用技术手段如表2 所示。表2 中的"√"表示具有的特点。

表 2　功能安全常用技术手段

Tab. 2　The commonly used technical means for functional safety

类型	序列号	时间戳	期望时间	连接授权	反馈信息	完整性检查	交叉检查
数据破坏					√	√	
无意重复	√	√					√
乱序	√	√					√
丢失	√				√		√
延迟		√	√				
插入	√			√	√		√
伪装				√	√		
寻址错				√			

在实际应用中,常用到的手段包括序列号、时间戳、完整性检查(CRC)和冗余交叉检查。这几种手段对抗黑通道产生的非人为破坏是足够的,但是对于蓄意攻击则存在以下不足。

① CRC 容易在线计算,从而难以对抗人为的数据改变,如攻击者可以将阀门动作指令改为最大或最小,从而破坏系统,而 CRC 很容易在线计算,接收者无法区分;

② 由于没有数字签名,无法验证接收的信息一定是声称的消息发送者发送的;

③ 交叉冗余不能对抗人为数据改变的攻击;

④ 单纯的序列号能够防止由于网络环境导致的重放,但不能防止人为的重放攻击;

⑤ 对于信息需要保密的环境,没有加密方案。

针对以上几点不足,我们提出 Safe-Sec 安全通信方法,既保障功能安全,又保障信息安全。

2.2　Safe-Sec 安全通信方法

针对传统功能安全通信在信息安全方面的不足,我们考虑使用数据加密、数据消息摘要以及数字签名来对抗前述问题。

从信息安全的角度分析,网络通信面临的威胁包括恶意篡改数据、窃取数据和伪装等攻击,解决方法类似于功能安全通信,包括时间戳、序列号、通信密钥和消息摘要码,如有需要还可以对明文进行加密。

Safe-Sec 方法保留时间戳、序列号、关系密钥,使用数据消息摘要码(message adgist code, MAC)代替循环冗余校验码。MAC[4] 如果改变明文,MAC 码很难在线进行计算。由于 MAC 具有单向性,通过改变明文攻击计算机是不可行的。为实现数据不可否认性和数据完整性,我们采用 MD5 作为 Hash 函数产生 Hash 码,然后产生数字签名。采用数字签名是因为数字签名具有更强大的对抗伪装、更改攻击的能力。

算法步骤具体如下。

① 在尽可能低的通信层次获取系统时间作为时间戳 TimeStamp;

② 根据序列号产生规则,产生序列号 SN;

③ 根据选定的单向函数(如椭圆曲线),计算消息摘要码 Hash(SA,DA,Data,SN,TimeStamp);

④ 使用选定的加密算法和密钥(如采用对称密码体制,使用相同密钥,否则使用私钥)计算 ECMAC;

⑤ 产生待发送报文:Msg = [SA, DA, Data, SN, TimeStamp, ECMAC];

⑥ 发送消息;

⑦ 接收方解包消息,使用密钥(如采用公钥密码体制则使用发送方公钥 Era)计算 ECMAC;

⑧ 验证传递的 ECMAC 和计算得到的 ECMAC1、SN 及 TimeStamp 的正确性。

Safe-Sec 的报文结构和传统功能安全通信报文结构的对比如图 2 所示。

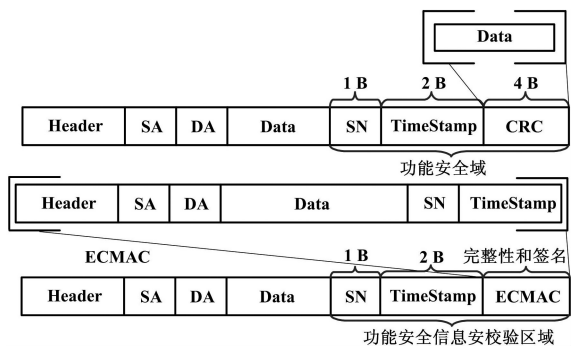

图 2　通信报文结构对比

Fig. 2　Contradistinction of the communication message structures

Safe-Sec 方法与传统功能安全通信相比,两者最大差别体现在 Safe-See 方法使用 ECMAC 替代 CRC,利用对全部信息的 ECMAC,可以保障数据的完整性和数据不可否认性。

我们采用 ECMAC 获得 MAC 码,原理如下式所示:

$$\begin{cases} ECMAC = E_k[Hash(SA, DA, Data, SN, TimeStamp)] \\ Msg_{send} = [SA, DA, Data, SN, TimeStamp, ECMAC] \end{cases}$$

式中:E_k 为加密算法;k 为密钥;$Hash$ 为单向函数。

如果加密算法使用对称密钥,则通信不便进行广播。考虑到实际应用,可以使用公钥加密体制,在此推荐椭圆曲线方法。

发送方使用如下公式:

$$\begin{cases} ECMAC = E_{Ra}[Hash(SA, DA, Data, SN, TimeStamp)] \\ Msg_{rcv} = [SA, DA, Data, SN, TimeStamp, ECMAC] \end{cases}$$

接收方使用对应 A 的公钥 Ua 进行 ECMAC 的解密和判断:

$$Hash[SA, DA, Data, SN, TimeStamp] = E_{Ua}(ECMAC)$$

上式如果成立,则说明该消息发布自节点 A。该方法的好处是速度较快,但不能实现数据的保密,大多数安全相关系统不需要数据保密功能。Safe-Sec 也可以使用 HMAC 和其他类型的消息摘要码实现。

2.3　Safe-Sec 安全通信方法有效性分析

Safe-Sec 安全通信方法能够对抗人为更改、伪装、人为延时攻击、人为重放攻击等,而传统安全通信并不能对抗以上攻击。为验证 Safe-Sec 在上述方面的有效性,将传统安全通信方法和 Safe-Sec 在典型用况下进行如下分析。

环境假设:设 A、B 为两个通信节点,A 向 B 发送安全数据 D 和 CRC(D),有恶意攻击者 C 进行攻击。应用环境示意图如图 3 所示。

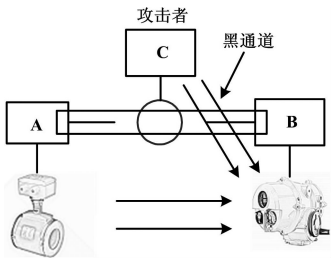

图 3　应用环境示意图

Fig. 3　Diagram of application environment

用况 1　恶意篡改、伪装安全数据。A 向 B 发送安全数据 D 和 CRC(D),有恶意攻击者 C 进行数据篡改攻击。

① 传统安全通信方法:攻击者 C 学习了数据 data,根据 data 和 CRC(data),可以反推出 CRC 多项式。此时 C 可以容易地发送数据 data′和 CRC(data′),接收者 B 验证 data′和 CRC(data′)相符合,不能检出错误。

② Safe-Sec 安全通信方法:A 向 B 发送经椭圆曲线 E_k 加密的 Hash 码,C 不知椭圆曲线的秘密(secret,如密钥),故无法在线计算数字签名。对于恶意篡改、伪装,Safe-Sec 方法的安全性依赖于椭圆曲线算法的强度。

用况 2　重放攻击。设 A 发布数据 cmd“阀门开度打开 20%”之后保持静默,C 伪装成 A 再次发布 cmd“阀门开度打开 20%”。

① 传统安全通信方法:攻击者把 cmd 中的 SN 递增 1,并且在线计算 CRC(cmd′),发布 cmd′,则接收端 B 验证 CRC 正确;SN 是期待的序列号,执行阀门开度再打开 20% 的动作,可能导致危险。

② Safe-Sec 安全通信方法:攻击者将 cmd 中的 SN 递增 1,由于未掌握椭圆曲线秘密,无法在线计算数据的新数字签名,无法构建具有足够欺骗性的数据。其防攻击能力依赖于椭圆曲线算法强度。

综上所述,对于恶意攻击如恶意篡改、伪装安全数据、蓄意重放攻击,Safe-Sec 均可完美解决,其安全性依赖于椭圆曲线强度,而传统安全通信方法在遭遇人为恶意攻击时,无法抵抗。

2.4　Safe-Sec 安全通信方法效率分析

通过对比采用 CRC32 的传统 61784-3 通信方式的编码时间和采用消息摘要码的 Safe-Sec 安全通信方法的编码时间,可以看出 Safe-Sec 方法时间效率是可以接受的。

试验结果如图 4 所示。

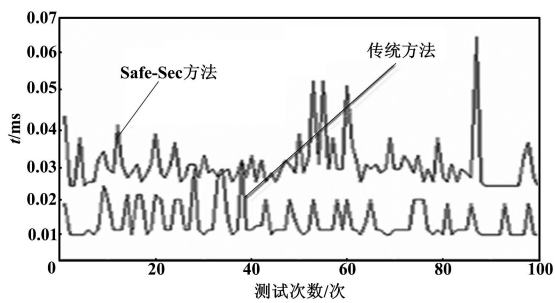

图 4　Safe-Sec 和传统方法编码时间

Fig. 4　Encoding times in Safe-Sec & classic approaches

3　结束语

本文系统地讨论控制系统面临的两类安全问题。针对该问题,从网络体系结构和通信方法两方面入手,提出了相应的解决方法。所提出的安全网络结构能够在不影响功能安全的大前提下,提高系统的信息安全水平。所提出的 Safe-Sec 通信方法较传统的安全通信

(下转第 38 页)