基于 KDC 的无线工业控制网络安全研究

陈 璐[1],刘 行[2],张 涛[1],马媛媛[1],王玉斐[1],黄秀丽[1]
(1. 中国电力科学研究院 信息与通信研究所,江苏 南京 210003;
2. 南京南瑞集团 信息通信技术分公司,江苏 南京 210003)

摘 要:无线通信在工业现场中的使用日益广泛,给无线工业控制网络带来了新的安全问题和挑战。面对无线工业控制网络的新形势,文中探讨了无线工业控制网络的安全风险。针对目前无线工控接入认证缺失的脆弱性,在分析无线工业控制网络的层次级安全架构的基础上,提出了一种适用于该架构的通信双方安全认证方案,构建基于密钥分配中心(Key Distribution Center,KDC)的无线工业控制网络密钥管理方法,保证无线工业控制网络通信双方的身份安全。

关键词:无线;工业控制;密钥分配中心;网络安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2014)01-0208-04
doi:10.3969/j.issn.1673-629X.2014.01.053

Security Research of Wireless Industrial Control Network Based on KDC

CHEN Lu[1],LIU Xing[2],ZHANG Tao[1],MA Yuan-yuan[1],WANG Yu-fei[1],HUANG Xiu-li[1]
(1. Institute of Information and Communication,China Electric Power Research Institute,Nanjing 210003,China;
2. Information and Communication Technology Company,NARI Group Corporation,Nanjing 210003,China)

Abstract:With the increasingly widespread use of wireless communication in the industrial field,new security issues and challenges have been brought to wireless industry control network. In this paper,faced to the new situation of wireless industrial control network,discuss the security risks of wireless industrial control network. In view of the lack of wireless access control in the certification of vulnerability,based on analysis of the hierarchy security architecture of wireless industry network,a security communication authentication program is proposed,the key management methods of wireless industry control network based on KDC are constructed,ensuring security identity of communications in wireless industrial control network.

Key words:wireless;industry control;KDC;network security

0 引 言

无线工业控制网络(Wireless Industrial Control Network,WICN)通常是由专用的硬件和通信组成,是单独的、孤立的系统[1],用于完成控制功能的计算资源(包括 CPU 计算时间和内存)都是极其有限的,如今已成为工业控制领域的研究热点,是满足工业应用高可靠、低能耗、硬实时等特殊应用需求的一类无线传感器技术[2]。由于无线工业控制网络的不断发展和广泛应用,在很大程度上降低了工业控制系统高额的投入和维护成本,极大地推动了工业无线技术在工业现场的应用,在未来几年,它也将成为工业控制产品的新的增长点[3-4]。

工业无线技术是从近几年最新的无线传感器网络技术中逐步发展而来的,工业无线网络技术的发展大致可以划分为以下两个阶段[5]:

(1)20 世纪 70 到 80 年代是第一个阶段,无线网络技术应用于工业,主要以解决长距离数据传输为目的,主要技术特点是以点对点通信为主。

(2)第二阶段则是在 21 世纪初,以短距离工业无线网络技术为主导,以解决低成本的信息获取为主要目的,主要特点是大规模和网络化。这一阶段的工业无线网络技术的进步得益于新兴的短程无线传感器网络技术的飞速发展。

无线工业控制网络拥有低成本、高可靠、易维护和

收稿日期:2013-03-24 **修回日期**:2013-06-28 **网络出版时间**:2013-11-12
基金项目:2012 年国家发改委项目(发改办高技[2012]1424 号)
作者简介:陈 璐(1984-),女,硕士,工程师,研究方向为无线通信信息安全、网络安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20131112.1636.023.html

高度灵活性的特点,与传统的有线工业控制网络相比,面临更大的安全威胁,更容易受到安全攻击。因此,一些适用于传统有线网络的安全方案在无线工业网络中不再适用,需要提出新的解决方案。

1　无线工业控制网络安全风险分析

相较于传统的有线通信方式,无线通信网络技术有着巨大的技术优势和发展潜力,对工业控制用户有着极大的吸引力,与此同时不容忽视的是,工业现场的强干扰以及工业应用本身对系统极高可靠性的严格要求,也给无线工业控制网络带来了新的问题和挑战[6-7]。

1)窃听和监听。

窃听(Sniffing)是指攻击者借助于技术设备、技术手段等获取传输信息。在无线网络常见的攻击方法之中,窃听无疑是容易实现的一种,由于无线链路的开放性,攻击者在不需要接到无线网络的情况下就可以进行监听。

为了防止监听和窃听无线网络,首先关闭任何网络身份识别的广播功能。然后,尽可能地禁止非授权用户访问无线网络。这可以防止一些网络工具发现无线网,进行破坏活动。但是,攻击者依然可以利用其他网络窃听设备来监控网络活动,甚至经过加密的不对外广播自己的身份的目标网络也会把通信量呈现给窃听器。

2)欺骗和非授权访问。

欺骗(Spoofing)是指攻击者采取非法手段将用户引向错误的网络资源,达到窃取资料或其他破坏目的。

非授权访问是指通过假冒、身份攻击等违反安全策略的操作,避开系统的安全机制或利用安全系统中的缺陷,对网络设备及资源进行非正常使用,因而,针对非授权方案应增加安全鉴别机制,防止非授权用户访问网络资源。对于具有核心节点的无线网络,可以较简单地实现认证功能;对于没有固定节点的无线网络,节点活动且移动未知,而且这种网络具有多跳性质,实现认证鉴别机制较为复杂。

3)未授权的信息破坏和篡改。

攻击者在传输媒介中途截获数据,对数据进行破坏或篡改。用户可以通过对数据进行完整性校验检测完整性。然而依然存在一个威胁,如果攻击者对数据完整性校验码本身进行修改,接收用户依然会认为数据完整性被破坏而丢弃数据。

4)拒绝服务(Denial of Service,DoS)攻击和洪泛攻击。

在无线网络中,拒绝服务攻击会使受攻击的网络节点瘫痪、使受攻击的网络终端服务失效,合法用户无法得到相应的资源、使受攻击的用户无法使用网络连接。在无线网中,有几个方法可以造成类似 PING 洪泛的服务中断。最简单的方法就是通过让不同的设备使用相同的频率,从而造成无线频谱内的冲突。另一个可能的攻击手段是发送大量非法或合法的身份验证请求,如果接入点(Access Point,AP)受困于成千上万个伪装验证请求,任何用户在提交身份请求的时候,就很难获得一个合法的会话过程。

为了防止 DoS 攻击,可行的解决方案并不多。在无线网络环境下,攻击者的攻击地点不局限于一个范围。可以在无线网关和无线路由下添加必要的安全功能,禁止外部用户访问路由、现场设备的 IP 地址、端口号等建立包过滤规则表,对非法连接进行阻断,从而提供了相关的安全机制。

5)耗能攻击。

由于现在的无线设备大多使用节能机制,在不进行通信时进入休眠状态是为了实现节约电池能量的目的。能耗攻击为了使设备无法进入节能模式,就不停地发送连接请求,达到破坏节能机制的目的。最终无线设备能量消耗完毕,攻击目的达成。目前,针对耗能攻击还没有行之有效的应对措施。

在上述安全问题中,文中针对无线网络接入认证机制缺失的问题,分析了无线工业控制网络的安全架构,提出了一种基于 KDC 的密钥管理方案[8],实现了通信双方的有效认证,使得攻击者(没有被安全系统认证通过的用户)即使捕获到分组,由于无法解密而失效。

2　无线工业控制网络的安全架构

根据工业控制网络需要,并结合 ISA 推荐的无线工业控制系统结构体系[9],可以将无线工业控制网络分为 3 个层次:管理层 L_3,过程层 L_2,装置层 L_1,如图 1 所示。

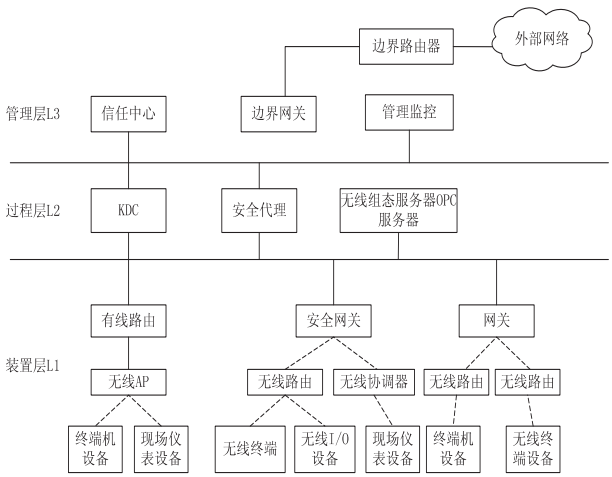

图 1　无线工业控制网络的安全架构

其中,装置层 L_1 用于无线工业生产现场的各种现场装置之间的连接,并且与过程层 L_2 的互联,主要面向现场数据业务流量较低、节点和网络生命周期要求较长的低端现场节点组网互联,通过分簇、多跳、簇树、网状、星型等组网方式将各现场节点的数据传送至接入节点(Access Point,AP),主要体现为短距离通信、大规模、低速、低成本、低功耗等特征。过程层 L_2 的功能是用于装置、人机接口以及控制室仪表之间的连接。管理层 L_3 负责管理监控,为了更好地拓展无线工业控制网络的应用领域,利用网络现有基础承载相关应用。

为了构成一个完整的无线工业控制网络安全架构,需要根据具体的层次采取相应的安全策略,还需要考虑工业控制网络中设备资源的有限性、实时性与安全管理问题,需要根据管理层、过程层、装置层的不同需求来制定不同的安全策略和措施。

过程层 L_2 的密钥分配中心(KDC) 主要负责密钥管理和设备鉴别工作,设备通过请求无线路由加入工控网络,在请求消息中要向 KDC 发送鉴别信息,KDC 通过鉴别消息判断是否允许该设备加入无线网络,从而形成 KDC 访问控制列表。

装置层 L_1 与过程层 L_2 的安全网关和无线路由负责边界保护,实现转发、过滤、流量控制等功能。通过安全网关可以防止外网的入侵,并根据现场设备的实际情况设置安全策略。

3 基于 KDC 的无线工业控制网络密钥管理

3.1 KDC 密钥管理方案的基本原理

对于一个 KDC 来说,至少应具备以下主要功能:

(1)能够分配并存储与之相连的各终端用户的公钥,并保证产生的公钥经过严格的随机性检验。

(2)能够使用随机数或伪随机发生器来产生会话密钥。

(3)能够向确立保密连接的两个用户发送随机会话密钥,并保证会话密钥是加密的。

(4)能够识别需要建立用户的身份标识符。

(5)能够有较完善的自我检验功能。

(6)能够在不影响网络通信效率的前提下,为两个用户建立保密连接。

图 2 表示的是与 KDC 相连的两个用户 T_1、T_2 通过 KDC 获取会话密钥的情况。其中,T_1 和 KDC 共享的公钥是 P_1,T_2 和 KDC 共享的公钥是 P_2。

当 T_1 希望和 T_2 进行保密通信时:

(1)T_1 向 KDC 发出会话密钥请求。密钥请求消息包含两项内容,第一项是 T_1 和 T_2 的身份标识符 ID_1 和 ID_2。

(2) 表示请求的消息由两个数据项组成,第 1 项是 T_1 和 T_2 的身份(ID_1 和 ID_2)。

(3)KDC 使用随机数或伪随机发生器来产生会话密钥 K。对 K 分别使用 P_1 和 $P_1 * P_2$ 进行加密。作为 T_1 的会话密钥请求应答消息。

(4)T_1 收到后,用公钥 P_1 解密获得会话密钥 K,并将 $P_2[K]$ 发送给 T_2。

(5)T_2 收到,用公钥 P_2 解密获得会话密钥 K。再发送确认消息给 T_1,作为收到会话密钥 K 的响应。于是,T_1,T_2 双方就可以交换加密数据。

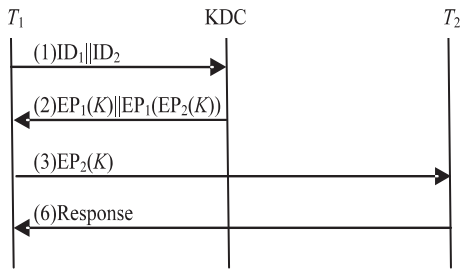

图 2 基于 KDC 的密钥管理方法

当用户双方通信完毕,则 T_1 和 T_2 将会话密钥 K 予以撤销。其目的就在于真正做到“一次一密”,保证每次通信过程都使用不同的会话密钥。

3.2 基于 KDC 的密钥管理方法

在无线工业控制网络环境中,当有现场终端要求进行通信时,为了保证消息的机密性要求通信双方进行身份认证,同时相互鉴别会话密钥。在此方案中,面临两个问题需要解决:

(1) 如何防止会话密钥被泄漏或篡改,为了保证密钥的机密性,要求现场终端的身份 ID 和私有密钥必须加密传输,公钥公开;

(2) 如何保证消息的时效性,即不受重放攻击的干扰[10-11]。

为了解决上述问题,构建一种基于 KDC 的无线工业控制网络密钥管理方案。假设 T_1 希望与 T_2 进行通信,T_1 和 T_2 在基于 KDC 的认证过程中,通信双方依据公钥密码理论,与 KDC 建立私钥 S_1、S_2,公钥 P_1、P_2。为了使通信双方 T_1 和 T_2 在建立私有密钥时可增加时间戳,KDC 为 T_1 和 T_2 分别建立一个共享的一次性会话密钥,保证了消息的机密性和有效性。

基于 KDC 的密钥分发和认证过程如图 3 所示。

(1)KDC 接收到 T_1 发出的会话密钥请求。

密钥请求消息包含两项内容,第 1 项是 T_1 和 T_2 的身份标识符;第 2 项是一个一次性随机数 R_1,是这次会话的唯一标识符,为了防止假冒攻击,每次密钥请求的 R_1 都不相同,且攻击者无法预测,通常采用随机数生成器产生。

(2)T_1 收到 KDC 回复的密钥请求应答消息。

密钥应答消息包含 5 项内容,且为了保证该消息只有 T_1 才能解密,KDC 用 T_1 的公钥进行了加密。第 1 项内容是一次性会话密钥 K;第 2 项内容是 T_2 的公钥 P_2;第 3 项内容是 T_2 的身份标识符 ID_2,T_1 通过解密后得到 ID_2 与之前发出的密钥请求消息相比较,查看是否是希望与之通信的现场终端;第 4 项内容是一次性随机数 R_1,以确定应答消息没有受到重放攻击;第 5 项内容是用 T_2 的公钥进行加密的一次性会话密钥 K 和 ID_1。这项内容 T_1 收到后直接向 T_2 转发,用于证明自己的身份。

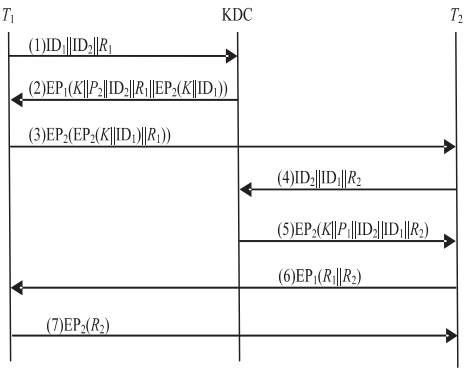

图 3　基于 KDC 的无线工业控制网络密钥管理

(3)T_1 收到 KDC 的密钥应答消息后,向 T_2 转发用 T_2 的公钥进行加密的一次性会话密钥 K 和 ID_1,以及一次性随机数 R_1。

T_2 收到后用自己的私钥进行解密,得到会话密钥 K,R_1 用于 T_1 和 T_2 双方握手的实现。

(4)KDC 接收到 T_2 发出的会话密钥请求。

密钥请求消息包含两项内容,第 1 项是 T_1 和 T_2 的身份标识符;第 2 项是一次性随机数 R_2,同样是这次会话的唯一标识符,作用与 R_1 相同。

(5)T_2 收到 KDC 回复的密钥请求应答消息。

密钥应答消息包含 5 项内容,且为了保证该消息只有 T_2 才能解密,KDC 用 T_2 的公钥进行了加密。第 1 项是一次性会话密钥 K,T_2 收到解密后与步骤(3) 中收到的 K 相比较,以确定其真实性;第 2 项是 P_1,是实现与 T_1 双方握手的密钥;第 3 项和第 4 项分别是 T_1 和 T_2 的身份标识符 ID_1 和 ID_2;第 5 项是一次性随机数 R_2,以确定之前向 KDC 发出的密钥请求消息没有收到重放攻击。通过步骤(1) 至步骤(5),会话密钥 K 就被安全地分配给了 T_1、T_2。

(6)T_2 用 P_1 实现双方握手,加密一次性随机数 R_1 和 R_2,并将加密结果发送给 T_1。

(7)T_1 以 $EP_1(R_2)$ 作为对 T_2 的应答,与步骤(6) 结合实现双方认证功能。

至此,T_1 和 T_2 就可以通过会话密钥 K 安全地进行通信了。

4　结束语

与传统的工业控制网络相比,无线工业控制系统网络拥有低成本、高可靠、易维护和高度灵活性的特点,应用日益广泛,同时也给工业控制系统带来了新的安全问题,有效解决安全技术问题是无线工业控制的关键部分。

文中分析了无线工业控制网络的层次级安全架构,提出了一种适用于该层次架构的安全方案,构建了基于 KDC 的密钥管理方法,弥补了目前关于无线控制网络有关接入认证缺失的脆弱性,实现了通信双方的安全认证。

参考文献:

[1] Stouffer K, Falce J, Scarfone K. Guide to industrial control systems (ICS) security[R/OL]. 2011-06. http://www.securityvibes.com/docs/DOC-1347.

[2] Adamczyk H, Rauchhaupt L. WLAN systems in industrial environments[J]. Mobile communication over wireless LAN, 2001(9):145-147.

[3] 曾　鹏. 工业无线技术的标准化与应用[J]. 中国仪器仪表,2008(3):40-44.

[4] 曾　鹏,徐皑冬. 工业无线通信技术[J]. 仪器仪表标准化与计量,2007(1):21-23.

[5] 于海斌,曾　鹏,梁韦华. 智能无线传感器网络系统[M]. 北京:科学出版社,2006.

[6] 阳宪惠. 工业数据通信与控制网络[M]. 北京:清华大学出版社,2003.

[7] 张　帅. 工业控制系统安全现状与风险分析[J]. 计算机安全,2012(1):15-19.

[8] Koulnmas C, Lekkas A, Papadopoulos G, et al. Delay performance of radio physical layer technologies as candidates for wireless extensions to industrial networks[C]//Proceedings of 8th IEEE international conference on emerging technologies and factory automation. [s. l.]:[s. n.], 2001:133-142.

[9] Kohl J, Neuman C. The Kerberos authentication service (V5)[S]. RFC 1510, 1993.

[10] Park J C, Jun A H. A light weight IPSec adaptation for small devices in IP-based mobile networks[C]//Proc of 8th international conference on advanced communication technology. [s. l.]:[s. n.], 2006:1-5.

[11] Zhang Y G. A multilayer IP security protocol for TCP performance enhancement in wireless networks[J]. IEEE journal on selected areas in communicaitons, 2004, 22:767-776.

基于KDC的无线工业控制网络安全研究

作者： 陈璐， 刘行， 张涛， 马媛媛， 王玉斐， 黄秀丽， CHEN Lu， LIU Xing， ZHANG Tao， MA Yuan-yuan， WANG Yu-fei， HUANG Xiu-li

作者单位： 陈璐,张涛,马媛媛,王玉斐,黄秀丽,CHEN Lu,ZHANG Tao,MA Yuan-yuan,WANG Yu-fei,HUANG Xiu-li(中国电力科学研究院 信息与通信研究所,江苏 南京,210003)， 刘行,LIU Xing(南京南瑞集团 信息通信技术分公司,江苏 南京,210003)

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(1)