无线 HART 安全技术的研究与设计*

Research and Design of Security Technology for WirelessHART

何之栋[1] 陆卫军[2] 钟 晨[2] 王海凤[1]
(1 浙江大学智能系统与控制研究所工业控制技术国家重点实验室,浙江 杭州 310027;
2 浙江中控技术股份有限公司,浙江 杭州 310053)

摘 要

针对无线 HART 网络协议,对协议的安全技术进行研究与分析,列举无线 HART 面临的安全威胁及协议中的相关措施,同时指出在安全方面的漏洞。对于安全技术重要的组成部分,设计并实现了一种基于资源有限的嵌入式平台下的安全管理器,采用合适的密钥生成算法,预先生成的机制以及数据交换的操作方式满足了协议规定的实时性要求,占用系统资源较小。

关键词:无线 HART,无线网络安全,安全管理器,密钥管理

Abstract

The security threats and related measures compliant with WirelessHART standard are enumerated in order to analysis and classify the security technologies in network protocol,meanwhile point out the security vulnerabilities and propose the further research directions and recommendations on other effective security measures.Security manager as a crucial component for industrial wireless network security is designed and implemented based on the embedded platform of limited resources, which is composed of appropriate key generation algorithm, pre-generated mechanism and the operation modes of data exchange to meet the real-time requirements for WirelessHART.

Keywords:WirelessHART,wireless network security,security manger,key management

工业无线传感器网络是 21 世纪新兴的、面向设备间短程、低速率信息交互的无线通信技术,适合在恶劣的工业现场环境使用,具有很强的抗干扰能力、超低能耗、实时通信等技术特征,是对现有无线网络技术在工业应用方向上的功能扩展和技术创新。无线 HART 是一种专门为过程自动化现场设备监控等应用而设计的无线网格型网络通信协议。它是 HART 现场通信协议第七版的核心部分[1],兼容有线 HART 设备,已经成为全球应用最广的无线工业协议。由于工业无线传感器网络常用过程现场、基础设施等关键环境,一旦被信息被篡改或破坏将造成难以估量的损失,所以信息的安全性十分重要,而安全技术作为工业无线网络中的技术组成部分,具有重要的研究意义,其中安全管理器的设计必须满足可用性、实时性等要求,同时还要考虑嵌入式平台资源受限等各种因素。

1 无线 HART 安全技术分析

1.1 无线 HART 网络结构及设备简介

无线 HART 传感器网络采用集中式的管理方式,其主要设备包括:网络管理器、网关、安全管理器、现场仪表设备及手持设备。网络组织方式如图 1 所示。其中现场仪表设备具有数据采集及路由功能,设备之间的通信会话都必须通过网络管理器管理配置。手持设备用于新的现场仪表设备加入时的信息配置。网关为网络数据汇聚设备,同时负责指令及配置信息的下发。网络管理器负责整个网络的路由选择和通信资源分配,维护网络状态,施行网络安全措施等,网络管理器直接与网关通信。安全管理器用于生成及管理网络中各类密钥,只能与网络管理器进行交互。现今比较主流的实现方式是将网关、网络管理器、安全管理器嵌入式一体化集成实现。

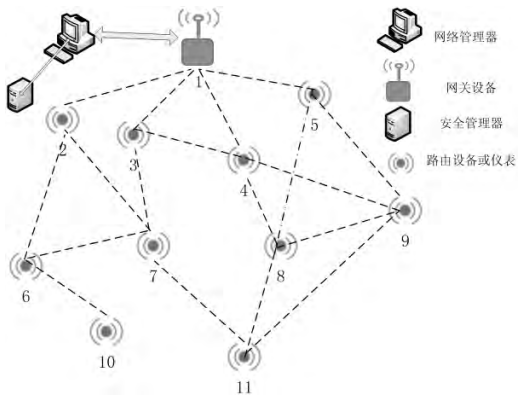

图 1 无线 HART 网络结构与设备

1.2 无线 HART 面临的安全威胁及措施

无线 HART 使用无线接入点,使其与传统有线 HART 相比,更容易收到外界的攻击威胁。针对无线 HART 面临的主要威胁,协议中定义了相应的安全措施加以解决,具体的威胁和措施如表 1 所示。

其他攻击还包括窃听、选择转发攻击[7]等。以上几种主要的攻击方式的特点可以分为几类:

信号干扰和信道拥塞攻击属于信道拥塞攻击,其主要特点使针对无线通信的物理号施行干扰或挤占,无线 HART 协议对于此类攻击有比较好的应对措施,黑名单机制和调频扩频机制提高了无线 HART 的可用信道数,尽可能地避免了网络信道的拥塞。无线 HART 可靠性大于 3-sigma (99.7300204%),与 ZigBee 相比,是目前最可靠的应用于工业过程自动化的通信协

* 国家 863 计划项目(2012AA041105)资助

表 1 无线 HART 的威胁分析和应对措施列表

安全威胁类型	威胁说明	无线 HART 应对措施
信号干扰	干扰是指无线电信号的无意扰动，同一频率和相同调制机制的信号可能在接收端覆盖掉真实信号。	多信道机制，跳频扩频技术（FHSS），使用 TDMA 机制分配时槽并利用路径的多样化[3]，减少干扰
信道拥塞攻击	引入同频率同调制机制的噪声或信号，用于干扰无线电信号	黑名单机制：如果某个特定频率的信道阻塞或者连续产生干扰源，则被加入黑名单。
Sybil 攻击[3]	一个攻击者可能持有多重身份认证。传统无线网络中缺少可信任的中心认证，可能遭受 sybil 攻击。	网关为每个实体绑定唯一的身份认证。网络管理器负责为每个连接的设备分配唯一的 nickname。
DOS 攻击[4]	针对可用性的攻击。发送大量请求导致资源消耗服务拒绝	无措施
流量攻击[5]	无线信号的广播特性使其更容易遭受流量分析攻击	NPDU 头和整个 DLPDU 都未经加密易受攻击。如果 DLPDU 负载使用网络密钥加密影响实时性
虫孔攻击[5]	在虫孔攻击中，攻击者通过无线或有线连接，在两个合法设备之间创建一个通道。	使用图路由[1]易受虫孔攻击，而使用源路由又缺乏工业环境需要的可靠性
同步干扰攻击[6]	攻击中通过在网络中引入错误的时间信息，破坏两个节点间的通信，同时使得设备消耗资源用于时间同步。	无线 HART 标准对时间有严格要求，Timer 模块必须满足时间要求，并且保证时槽（10ms）同步。

议。但同时，无线 HART 所应用的 2.4GHz 个频谱与 wifi，蓝牙，wibree，zigbee 和 ISA100.11A 有重叠，在异构网络中容易导致吞吐量下降。

流量攻击和 DOS 攻击属于数据拥塞攻击：其基本特点是针对无线 HART 流量特性，发送大量伪造数据，导致服务失效或延迟。无线信号的广播特性使其更容易遭受流量攻击。无线 HART 网络中，网络层数据单元头和整个链路层数据单元都未经加密，攻击者很容易对其进行分析。如果 DLPDU 负载使用网络密钥加密，可以消除流量分析的风险。但这样所有的中间设备都需要在数据链路层解密网络层数据单元，以找到目的地址和路由信息等，无法满足 10ms 的通信实时性要求。同样 DOS 攻击中，攻击者可以通过伪造大量的 join 请求，不断修改数据链路层数据单元并重新计算 MIC 等方式消耗网络资源，最终导致拒绝服务。基于实时性等性能的考虑，无线 HART 对于此类攻击并没有很好的措施，容易受到该类攻击。

Sybil 攻击、虫孔攻击、同步干扰攻击等属于篡改型攻击。例如 Sybil 攻击中，一个攻击者可能持有多重身份认证，通过控制系统的大部分节点来削弱冗余备份的作用。而无线 HART 中的网关为每个设备绑定唯一的身份认证，网络管理器维护每个设备唯一对应的地址列表，设备通过相关密钥与网关和网络管理器建立会话。所以 Sybil 攻击几乎不可能针对 WirelessHART 网络。再比如在虫孔攻击中，攻击者通过无线或有线连接，在两个合法设备之间创建一个通道，使用图路由（具有冗余路径）易受虫孔攻击，而使用源路由是由网络管理器指定的单条路径，可以抵御虫孔攻击，但其本身路由方式并不可靠，任一链接的失效将导致数据包丢失。此类攻击的前提是截获并破解网络中相关安全密钥，如果密钥安全等级较高，密钥的分配及维护机制合理，可以很大程度上避免此类攻击。

从上面的分析可以看出，无线 HART 网络协议虽然具有一定的安全性，但是对于许多攻击类型仍然没有有效地措施，工业实时数据的安全性至关重要，其安全技术需要更深入的研究。

1.3 无线 HART 协议中网络安全技术

无线 HART 为工业自动化提供安全可靠的通信协议。现场设备收集过程数据，通过安全方式向其他设备发送数据。也就是说，在无线 HART 网络中，所有数据以无线 HART 命令的方式传送，命令的保密性、一致性和认证可以获得保障。无线 HART 标准提供的安全机制分为两个层次：端到端、单跳间[8]。

1）端到端安全：端到端安全保护从源地址到目的地址的通信不受内部的恶意攻击。端到端安全在网络层实现，所有从网络层传向数据链路层的数据都需要经过加密（除了网络层协议数据帧报头），只有目的设备能够解密。无线 HART 协议栈中的网络层提供三种安全服务：保密性、完整性和认证。网络层使用的 AES 加密算法具有两种模式：使用 CBC-MAC 模式的 AES-CCM，用于计算消息完整性编码(message integrity code，简称为 MIC) 提供认证和数据完整性；使用计数器模式的 AES-CCM，用于加密网络层协议数据单元 NPDU 负载。

在无线 HART 网络中，所有通信都需要通过网关的会话密钥进行（除手持式设备外）。手持式设备可以使用手持式密钥(handheld key)与现场设备建立一对一的通信会话。为了建立这样的通信关系，手持式设备首先使用 Join key 加入网络；在成功加入网络后，手持式设备向网络管理器请求 Handheld 密钥。使用该密钥与同样持有该 handheld 密钥的现场设备创建点对点通信回话[1]。

2）单跳之间安全：数据链路层使用网络密钥为两个邻居设备提供单跳安全完整性认证。在无线 HART 网络中的所有认证设备都持有网络密钥，因此单跳安全可以防御外部攻击者，例如不属于无线 HART 网络的设备等。对于数据链路层数据单元，使用 AES-CCM 模式计算加密 MIC。

无线 HART 中的安全机制主要由以上两个层次的保护措施实现，其中每个层次都涉及安全密钥，因此需要设计安全管理器用于管理密钥。安全管理器是无线 HART 网络安全技术重要的组成部分[1]，其架构，功能以及实现方式具有特殊性，本文之后将针对无线 HART 安全管理器提出具体的设计和实现方案。

1.4 其他安全措施的功能拓展及安全性与系统性能的权衡

从上文无线 HART 面临的安全威胁及措施中，可以看到工业无线网络仍然面对许多威胁。工业无线网络的另外一种协议 ISA100.11a 比无线 HART 提供了更好的安全性，如ISA100.11a 采用非对称加密机制[9]。与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（public key）和私有密钥(private key)，加密和解密采用不同的密钥，与对称密钥加密相比，优点在于无需共享的通用密钥，解密的私钥不发往任何用户。即使公钥在网上被截获，如果没有与其匹配的私钥，也无法解密，所截获的公钥是没有任何用处的。因此非对称加密机制提供更高的安全性。文献[10]提到可以在无线 HART 安全子层通过保留安全位来实现这一功能，但由于非对称加密算法相对复杂，对嵌入式平台加密效率以及网络的实时性都是一个挑战。此外，网络接入认证机制也有待加强。

网络的实时性，可靠性以及安全性之间无法达到各自最优，文献[11]讨论了安全性与系统性能之间权衡的关系，如何针对具体的应用环境的特点和需求去调节性能与安全的关系，可进一步研究以完善工业无线安全体系及技术。

2 无线 HART 安全管理器设计

2.1 安全管理器概述

根据无线 HART 标准，安全管理器的核心任务是管理安全密钥。安全管理器在管理安全密钥的过程中，主要负责产生、存储、撤销和更新安全密钥，但并不负责将密钥分发给无线设备而是将安全密钥提供给网络管理器，由网络管理器将密钥分发给设备[12]。

无线 HART 标准只是简要地介绍了安全管理器的功能，但标准中并没有定义安全管理器的架构及在其网络中的组织形式，标准中对于安全管理器有如下规定[12]：

1)一个网络中只能存在一个网络管理器,但一个安全管理器可以服务于多个无线 HART 网络;

2)网络管理器作为一个独立的实体,可以作为一个主机应用功能,也可以集成在网络管理器中;

3)安全管理器与网关没有通信关系,且不能直接与现场设备通信。

文献[10]中设计了一种针对无线 HART 的安全管理机制,但其设计与测试主要利用 Java Cryptographic Extension 实现于主机应用,与当前主流的网络管理器、网关、安全管理器三者嵌入式一体化的实现方式有所不同,受平台性能局限较小。本文在此提出一种适合于嵌入式平台的安全管理器实现方案,其中的关键技术包括密钥生成机制,安全管理器服务流程维护和密钥的存储与管理。

2.2 安全管理器密钥生成机制

密钥生成是安全管理器的核心步骤,无线 HART 数据流使用了工业通信领域常用的 AES-128 加密算法,其算法强度使得攻击者无法在有效时间内使用暴力方法破解数据。而安全管理器密钥生成机制需要更高的加密强度,以防止统计型攻击在更短的时间内将其破解,因此安全管理器密钥生成机制利用随机源生成随机密钥。

具体地,无线 HART 中使用的密钥根据功能可以分为八种,每一种密钥的功能如表 2 所示。

表 2 无线 HART 密钥类型与功能

密钥类型	密钥功能
Join Key 加入密钥	安全管理器在现场仪表加入前生成,由安全管理员分配给现场仪表从而通过网络管理器的认证
Unicast-Gateway key 单播-网关密钥	网关与设备单播通信密钥
Unicast-NM key 单播-网络管理器密钥	网络管理器与现场仪表单播通信密钥,网络管理器使用该密钥向设备请求健康报告,分配时隙等。
Broadcast-Gateway key 广播-网关密钥	网关广播通信密钥,用以广播一般通知及时间信息
Broadcast-NM key 广播-网络管理器密钥	网络管理器广播通信密钥,发布路由信息及网络调度
Handheld key 手持密钥	分配给手持设备,使其与现场仪表设备的链接通过验证关系
Network key 网络密钥	用于提供针对外界的防御,用以计算 MIC,在所有设备中共享
Well Known key 公认密钥	用于对加入请求/回复信息计算 MIC,其值为 777 772E 6861 7274 636F 6D6D 2E6F 7267

根据密钥类型及作用的不同,可以将密钥分为三大类,非实时密钥、实时密钥和固定密钥。固定密钥即 Well Known key,该密钥为固定值,采用硬编码方式存储,无需通过安全管理器生成和存储;非实时密钥包括 Join Key、Hangheld key、Network key,主要处理设备的认证和授权机制,网络管理器对该类密钥的生成和获取实时性要求较低;实时密钥即会话密钥,包括 Unicast-Gateway key、Unicast-NM key、Broadcast-Gateway key、Broadcast-NM key,应用于实时通信双方,网络管理器对该类密钥的获取有较高的实时性要求,要求在向安全管理器提出密钥请求后 10ms 内获得生成的密钥,受处理器性能限制。

对于加入密钥及网络密钥的生成,方案考虑使用管理员口令与随机源的异或运算生成明文。人为设定密钥为 8 位 16 进制数,包含数字和字母,由网络管理员人为认定,具有保密性。然后对明文采用合适的加密算法进行密钥的生成,最后采用相关方法截断或提取 128 位密钥。随机源有多种选择,比如响应时间、系统时间、即测实时数据等,在本方法中,使用无线 HART 协议中 ASN 字段作为随机源[13],协议中对 ASN 规定如下:

Absolute Slot Number(ASN):64 位,为从网络建立开始经历的所有时隙总数,ASN 只能递增且不能被重置。可见 ASN 是理想的随机源。

会话密钥的生成与加入密钥类似,加入密钥和 ASN 的异或运算结果作为明文,然后采用合适的加密算法生成会话密钥具体密钥生成流程如图 2 所示。

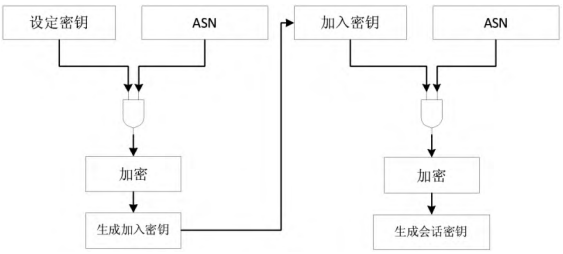

图 2 安全管理器密钥生成机制流程

针对上述密钥的生成方式,基于 AT91S9200[14](处理频率 128MHz)嵌入式平台,采用各种常用加密算法生成密钥进行测试,如图 3 所示,横轴表示从网络管理器向安全管理器提出密钥请求至获取密钥的延时时间。

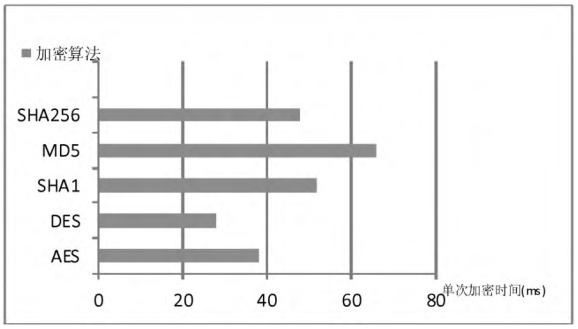

图 3 各种加密算法的密钥生成延时时间

由图 3 可以看出,安全等级高的加密算法由于其算法复杂,在嵌入式平台上应用时,基本无法满足无线网络对于会话密钥的实时性要求,因此本方案设计在处理器空闲时段定时在安全管理器中预先生成一批实时密钥,当网络管理器提出密钥申请时,安全管理器只需要相关的密钥读取操作,即可将已生成的密钥反馈至网络管理器。采用这种机制,网络管理器提出申请后,安全管理器只需要进行获取及数据返回操作,几乎不存在时延,可以很好地满足实时性要求。

2.3 安全管理器服务流程维护

根据无线 HART 协议的需求,无线 HART 安全管理器需要提供以下服务或接口:

init_key_generation:安全管理器初始化。

Pre_key_generation:key 值的预先生成及存储,预先生成一个 Join Key 和 Network key,检查已生成但没被使用的 session key 数量,判断下一次更新前所需要密钥数量是否充足,按需预先生成一批密钥。

Key_request:安全管理器提交 key 值申请并绑定。对于不同类型的密钥请求安全管理器有不同的操作方式,对于加入密钥和网络密钥,安全管理器即时生成一个新的密钥值并返回;对于会话密钥的请求,安全管理器检索密钥库属性,若发现已分配,直接返回原密钥,若发现需要分配一个新的密钥,则取一个

预先生成的新密钥关联属性并返回。图 4 所示为安全管理器在接受到各类密钥请求后的操作流程。

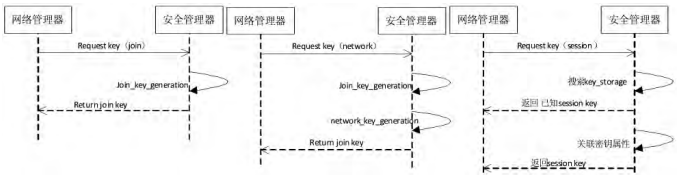

图 4 密钥请求操作流程

Key_renewel：按需更新密钥值。按需更新密钥值与 Key_request 类似，对于加入密钥和网络密钥，安全管理器生成一个新的密钥值并返回，对于会话密钥的更新，安全管理器取一个预先生成的新密钥关联原密钥属性并返回新密钥值。

Key_Revocation：密钥值销毁并解除属性关联。对于对于加入密钥和网络密钥操作与 Key_renewel 相同；对于会话密钥，则解除当前密钥的关联属性并删除该密钥，返回密钥销毁是否成功。

key_update：由于密钥具有时效性，所以必须由网络管理器触发，定期检查所有 key 值是否过期失效并更新，同时启动预留密钥程序 Pre_key_generation。

2.4 安全管理器的存储与管理

建立一个完善的数据库有助于安全管理器中密钥值与密钥信息的存储与管理，但同时也消耗了大量的资源。在资源有限的嵌入式平台上，需要采用简单有效的方法提高密钥管理的执行效率。本文使用一种简单的结构体数组存储方式，以会话密钥（session key）为例，密钥值、关联密钥值和关联密钥属性存入数组单元中，其中关联密钥属性主要包括 NetworkID（网络号），Nichname（设备名字），DeviceID（设备编号），Generation_Date（密钥生成时间），Expiry_Date（密钥失效时间）等。如图 5：

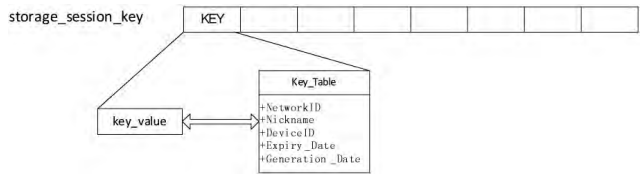

图 5 会话密钥存储格式

考虑到实时密钥采用预先生成的机制，服务实现时采用了一种数组交换策略，避免密钥整体转存，有效减少了密钥存储变动所占用的资源和操作复杂度。具体方法是设定已分配密钥指针（allocated）以及已生成密钥指针（generated）来标记密钥数组中的当前存储位置的后一个位置。具体的服务操作以下列伪代码为例：

Key_Renewel（密钥更新如图 6 所示）：

```
storage_sessionkey[i] = storage_sessionkey[generated-1];
sgenerated-1;
```

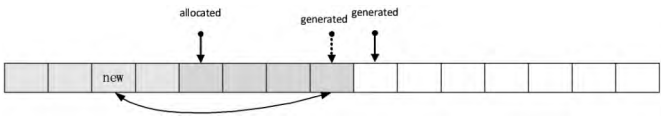

图 6 密钥更新操作方法

Key_Revocation（密钥销毁如图 7 所示）：

```
swap(&storage_sessionkey[i],&storage_sessionkey[allocated-1]);
allocated-1;
swap (&storage_sessionkey [allocated],&storage_sessionkey [generated-1]);
generated-1;
```

通过这种数组交换方法，只需要进行简单的交换操作，就可

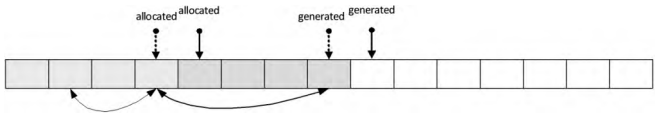

图 7 密钥销毁操作方法

以实现安全管理器存储和相关服务，操作简便，占用的资源少，特别适用于资源受限的嵌入式平台。

3 结束语

无线 HART 网络协议是第一个正式发布的工业无线网络协议，本文通过对其安全技术方面的特点分析，分析协议在解决各种网络威胁时还存在的问题，指出在与相关工业安全协议的结合，其他安全措施的功能拓展及安全性与系统性能的权衡，安全数据融合的拓展等方面还存在研究的空间和价值。同时，本文设计并实现了一种安全管理器，采用合适的密钥生成算法，预先生成的机制以及数据交换的操作方式，满足了协议规定的实时性要求，适合在资源有限的嵌入式环境下长期运行，具有借鉴价值。

参考文献

[1]Song, Jianping, et al.WirelessHART: Applying wireless technology in real-time industrial process control.Real-Time and Embedded Technology and Applications Symposium,2008. RTAS'08. IEEE. IEEE, 2008

[2]Hayashi, Hisanori, Toshi Hasegawa, and Koji Demachi.Wireless technology for process automation.ICCAS-SICE,2009. IEEE, 2009

[3]余群，张建明.无线传感器网络中的 Sybil 攻击检测[J].计算机应用，2006，26(12)：2897-2902

[4]裴庆祺，沈玉龙，马建峰.无线传感器网络安全技术综述[J].通信学报，2007，08：113-122

[5]Buttyán, Levente, and Jean-Pierre Hubaux. Security and cooperation in wireless networks. Vol. 188. Cambridge University Press, 2007

[6]Bilal, Zeeshan, Ashraf Masood, and Firdous Kausar.Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags:Gossamer protocol.Network-Based Information Systems,2009.NBIS'09.International Conference on.IEEE,2009

[7]Chen,Xiangqian,et al.Sensor network security:a survey. Communications Surveys & Tutorials, IEEE 11.2 (2009): 52-73

[8]Raza, Shahid,et al.Security considerations for the wirelesshart protocol.Emerging Technologies & Factory Automation,2009. ETFA 2009. IEEE Conference on. IEEE, 2009

[9]Petersen,Stig,and Simon Carlsen.Wirelesshart versus isa100.11a: The format war hits the factory floor. Industrial Electronics Magazine, IEEE 5.4 (2011): 23-34

[10]Raza, Shahid, et al.Design and implementation of a Security Manager for WirelessHART networks.Mobile Adhoc and Sensor Systems,2009. MASS'09. IEEE 6th International Conference on. IEEE, 2009

[11]Haleem,Mohamed A.,et al.Opportunistic encryption: A trade-off between security and throughput in wireless networks. Dependable and Secure Computing,IEEE Transactions on 4.4 (2007): 313-324

[12]HART Wireless Devices Specification (HCF_SPEC-290,Revion1.1)[S].2008.5

[13]TDMA Data Link Layer Specification (HCF_SPEC-075,Revion1.1)[S].2008.5

[14]www.atmel.com/Images/doc1768.pdf

[收稿日期：2014.6.4]