WIA-PA 网络的入网认证和密钥更新机制研究

Research on Network Access Authentication and Key Update Mechanism for WIA-PA Network

王　浩　杨　剑　刘　杰　王　平

(重庆邮电大学自动化学院网络控制技术与智能仪器仪表教育部重点实验室,重庆　400065)

摘　要：WIA-PA 是我国自主研发的、用于工业过程自动化的无线网络规范。研究了 WIA-PA 网络所处工业现场环境恶劣、节点资源非常受限的现状,提出并分析了由中间节点发起认证请求和散列函数生成安全信息的入网认证方案,以及使用单向散列函数的密钥更新方案。入网认证方案减小了通信消耗和组网时间,密钥更新方案实现了消息认证和消息源认证。分析结果表明,入网认证方案保证了所有入网节点的合法性,密钥更新方案保证了更新密钥的安全有效。

关键词：WIA-PA　入网认证　无线网络　路由设备　安全

中图分类号：TP309.7　　**文献标志码**：A

Abstract: WIA-PA is the wireless network specification researched and developed in our country for using in industrial process automation area. The current status of WIA-PA network such as the harsh environment of the industrial fields and limited node resource is studied. The strategy of network access authentication that is issuing request of authentication by intermediate node, and creating security information by hash function; and the dongle update strategy by using one-way hash chain function are proposed. The features of proposed strategies are analyzed; the network access authentication strategy reduces communication consumption and networking time; and the dongle update strategy implements authentication of message and message resource. The results of analysis indicate that network access authentication strategy ensures the legitimacy of all the nodes, and the dongle update strategy guarantees the security and effectiveness of dongle update.

Keywords: WIA-PA　Network access authentication　Wireless network　Routing equipment　Security

0　引言

WIA-PA(wireless networks for industrial automation-process automation)是基于 IEEE STD 802.15.4-2006 的标准,用于工业过程测量、监视与控制的无线网络系统[1]。该规范是我国自主研发的、用于工业过程自动化的无线网络规范,现已成为 IEC 国际标准。

WIA-PA 网络支持两层网拓扑结构。第一层是网状结构,由网关设备及路由设备构成;第二层是星型结构,由路由设备、现场设备和手持设备构成。用于系统管理的网络管理者和安全管理者在实现时可位于网关设备或主控计算机。本文中,安全管理者由主控计算机担任。同时,一种类型的物理设备可以担任多个逻辑角色。在星型和网状结合的两层拓扑结构中,网关设备可以担任网关、网络管理者以及安全管理者的角色;路由设备可以担任簇首的角色;现场设备和手持设备只能担任簇成员的角色。

作为一个开放系统,WIA-PA 存在潜在的安全风险[1],必须采取一定的安全措施,以保证 WIA-PA 用户的安全操作,保护系统内部的资源和维持正常的生产秩序。本文针对 WIA-PA 网络的实际应用中的安全问题,分别提出了入网认证方案和密钥更新方案。

1　单向散列链

单向散列链是一个散列值序列 $\{x_1,\cdots,x_j,\cdots,x_m\}$[4],序列中各元素满足:

$$x_j=F(x_{j-1},G)\qquad 1\leqslant j\leqslant m\qquad(1)$$

散列函数(映射)F 满足以下属性:①给定 x_{j-1} 和 G,很容易计算出 x_j;②若未给定 G,而给定了 x_{j-1},则很难计算出 x_j,若给定了 G,未给定 x_{j-1},也很难计算 x_j。

在该散列链里,如果要对一个给定的散列值 x_j 进行认证,可以采用如下方法:①已知 x_{j-k},由式(1)对 x_{j-k} 重复计算 k 次后得到 x'_j,将其与 x_j 进行比较;②已知 x_{j+k},由式(1)对 x_j 重复计算 k 次后将得到的 x'_{j+k} 与 x_{j+k} 进行比较。

在本方案里,称 G 为生成因子,第一次计算时参

国家科技重大专项课题基金资助项目(编号:2009ZX03006-001-03)。
修改稿收到日期:2010-10-27。

第一作者王浩,男,1975 年生,2007 年毕业于重庆大学计算机软件与理论专业,获博士学位,副教授;主要从事工业以太网及网络控制技术、无线传感器网络安全、智能仪表等方面的研究。

数 x_0 称为种子，散列链的每一个元素 x_j 称为链密钥。同时给出公共散列链的定义，对于节点 u 和节点 v，若 u 拥有散列链 C_i，同时 v 从 C_i 提取一个或多个链密钥，则称 u 和 v 共享一个公共散列链 C_i。

2　入网认证

对于需要进行安全认证的网络，所有节点都有与信任中心分别共享唯一加入密钥（KJ）。该加入密钥在部署网络前通过手持设备等安全方式写入节点设备[1]。WIA-PA 网络拓扑结构如图 1 所示。

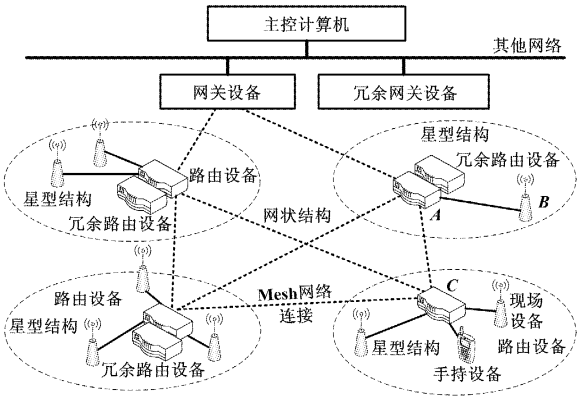

图 1　WIA-PA 网络拓扑结构

Fig. 1　Topology structure of WIA-PA network

2.1　单跳入网认证

对于单跳加入网络的节点，如图 1 中的节点 A，当信任中心收到 A 的入网请求后，发起对节点 A 的认证请求，在收到节点 A 的认证响应后对 A 进行认证。节点 A 的认证响应包含安全信息，安全信息由式（2）采用 F 函数计算得到。单跳节点入网过程如图 2 所示。

$$S_{\text{info}} = F(P_{\text{addr}} \mid T_{\text{devicetpte}},\ \text{KJ}) \tag{2}$$

式中：S_{info} 为计算得到的安全信息；P_{addr} 为设备的唯一标志地址；$T_{\text{devicetpte}}$ 为设备的类型，路由设备或现场设备；| 为字符串连接符号。

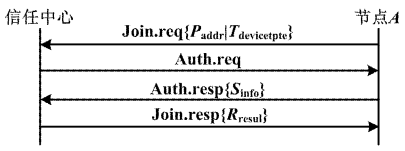

图 2　单跳节点入网认证

Fig. 2　Authentication of one hop node

图 2 中，通信报文用原语表示，Auth. resp 和 Join. resp 报文由密钥加密保护。

节点 A 首先发送入网请求 Join. req，其中包含自己的唯一标志和设备类型，信任中心根据网络属性判断是否对 A 认证，需要认证时保存 A 的标志和类型，发起认证请求 Auth. req。A 收到认证请求，根据式（2）计算安全信息 S_{info} 并响应信任中心 Auth. resp。信任中心收到 A 的认证响应，查询与 A 预共享的 KJ，由式（2）计算安全信息并与 S_{info} 比较，如果不等，拒绝 A 加入网络；否则，回复入网响应 Join. resp，置结果 R_{result} 为 1，告知节点 A 入网成功。

2.2　多跳入网认证

对于多跳入网的节点，如图 1 中节点 B 或节点 C 通过中间节点 A 加入网络，其认证过程如图 3 所示。

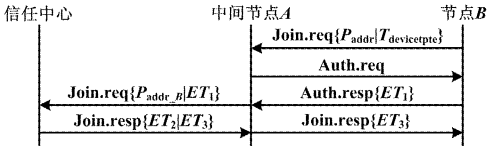

图 3　多跳节点入网认证

Fig. 3　Authentication of multi-hop node

节点 B 发送入网请求 Join. req，中间节点 A 发起认证请求 Auth. req。B 利用与信任中心预共享的 KJ，根据式（2）生成 S_{info}，并由式（3）计算给信任中心的数据 ET_1，然后发送认证响应 Auth. resp。

$$ET_1 = E_{\text{KJ}_B}(S_{\text{info}} \mid P_{\text{addr}} \mid T_{\text{devicetpte}}) \tag{3}$$

式中：KJ_B 为 B 与信任中心共享的加密密钥；E 为加密算法，采用对称加密，算法在此不作要求。

A 收到 B 的认证响应报文不做处理，构造关于 B 的入网请求报文 Join. req，包含 B 的标志 $P_{\text{addr\_}B}$ 和 ET_1，并发送给信任中心。

信任中心收到来自于 A 的报文后，首先判断 A 是否为经过认证的在网节点，如不是，则丢弃该报文；如是，则解析报文，并根据 $P_{\text{addr\_}B}$ 查找与 B 共享的 KJ，解密 ET_1 获得 B 的入网信息。采用同样的方法认证 B，如果认证成功，根据如下公式计算给 A 的密文 ET_2 和给 B 的密文 ET_3，并构造报文 Join. resp 发送给节点 A。

$$ET_2 = E_{\text{KJ}_A}(I_{B\_\text{trust}} \mid P_{\text{addr\_}B}) \tag{4}$$

$$ET_3 = E_{\text{KJ}_B}(I_{A\_\text{trust}} \mid R_{\text{reslut}}) \tag{5}$$

式中：$I_{B\_\text{trust}}(I_{A\_\text{trust}})$ 为节点 $B(A)$ 是否可信的标志，1 表示可信，0 表示不可信。

节点 A 在收到信任中心的入网响应报文后，首先解密 ET_2，根据 I_{B_trust} 判断 B 是否可信，不可信则不予处理，可信则根据 $P_{\text{addr\_}B}$ 将 ET_3 转发给 B。

当节点 B 收到来自 A 的响应报文时，对 ET_3 进行解密，并根据 I_{A_trust} 判断节点 A 是否可信，不可信则从新选择路径入网，可信则由 R_{result} 判断加入网络是否成功。

当节点 A 与信任中心之间是多跳链路时，节点 A 已入网，即确保了该链路是安全链路，节点 A 只需通

过此链路转发数据即可，无需对链路中节点再次认证。

2.3　方案分析

本方案在网络形成时确保了所有入网节点的合法性，保障了网络的整体安全性。虽然节点的入网时间短暂，但由于节点和网络所在区域环境恶劣，存在各种威胁的可能性，如非本网络节点、恶意攻击节点等，故假定所有入网节点都不可信，通过信任中心认证的节点才视为本网络的合法节点。

对于单跳入网，由信任中心认证节点。因信任中心与节点间共享唯一安全的加入密钥，通过认证则表明节点合法。

对于多跳认证，假如节点 B 是恶意节点，因 A、B 之间没有共享材料，节点 A 不能够认证 B，所以将 B 的认证信息发送给信任中心，信任中心认证 B 失败，即可告知节点 A 节点 B 不可信，且发送给 A 的报文由 KJ_A 加密保护；A 得知 B 不可信则可拒绝与 B 通信。假设 A 是恶意节点，而 B 的安全认证信息由 KJ_B 加密，A 在短时间内无法破解篡改，如果它把认证信息发送给信任中心，也会被信息中心发现其不可信，此时 A 便获取了合法节点的唯一标志和设备类型，但并不足以构成危害或者试图伪装加入网络。不管 A 是否转发认证信息，节点 B 在规定时间内未收到信任中心的入网响应，可认为其为恶意节点，从而选择其他路径入网。假若节点 A 和 B 同为恶意节点，也会因无法伪造加入密钥而被拒绝加入网络。同时，该认证方案在单跳入网时由信任中心发起认证请求，多跳入网时由中间节点而不是由信任中心发起认证请求，减小了信任中心和中间节点的通信次数和网络的通信开销。节点入网跳数与网络报文数的关系如图 4 所示。

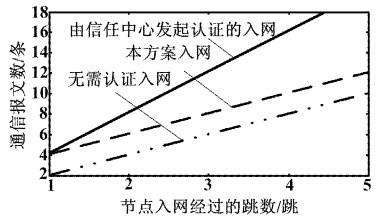

图 4　节点入网跳数与网络通信报文数关系

Fig. 4　Relationship between the numbers of hops and network communication messages

由图 4 可以看出，本方案和无需认证的入网相比只增加了两次通信，即两条报文，即第一跳的发起认证请求和认证响应，并且随着跳数的增加，通信量并没有显著增加；当由信任中心对入网的节点发起认证时通信次数显著递增且递增率大于本方案。对于大规模网络的形成，网络中将有大多数节点需多跳入网，本方案能够有效降低通信消耗，减小整体网络的组网时间。

3　安全的密钥更新

节点入网后，由信任中心为入网成功的节点分发相应的密钥并周期性地更新密钥。一旦有节点受损或者网络受到威胁，信任中心将立即剔除受损节点并更新密钥，或者当节点检测到密钥暴露时主动发起密钥更新服务。为确保节点通信中数据的安全，密钥的分发和更新必须正确而且安全有效，即密钥在传输中不被截取破解或经篡改后继续发送、发送方合法。本节给出密钥更新详细方案，会话密钥采用单向散列链模式，更新报文附带校验信息，从而保证数据包和密钥本身的正确性和数据来源的合法性。

3.1　密钥池

信任中心生成一系列单向散列链并构成密钥池。所有散列链共用一个种子(seed)，对于散列链 C_i，假设其生成因子为 G_i，则该散列链的第 j 个链密钥生成如式(6)所示。

$$k_{i,j} = F^j(\text{seed}, G_i) \tag{6}$$

式中：$F^j(\text{seed}, G_i) = F[F^{j-1}(\text{seed}, G_i), G_i]\ (1 \leqslant j \leqslant M)$。

为了生成密钥池，信任中心随机生成一个种子，并选择 L(等于网络节点个数)个不同的生成因子(这里我们选用与每个节点预共享的加入密钥)，通过反复执行上述散列链生成过程，生成 L 个散列链，同时删除种子。最终的密钥池将由 L 个散列链组成，其中每个散列链包含 M 个链密钥。密钥池的组成如图 5 所示。

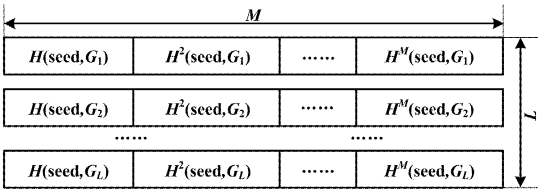

图 5　密钥池的组成

Fig. 5　Composition of the dongle pool

3.2　密钥更新

对于入网成功的节点，信任中心分发密钥给每个节点，与每个节点共享唯一的公共散列链，分发密钥加密密钥(key encryption key，KEK)时由加入密钥保护，分发数据密钥(data encryption key，KED)则由 KEK 保护。当网络到达密钥更新周期时，信任中心对网络节点进行密钥更新，节点的密钥更新过程如图 6 所示。

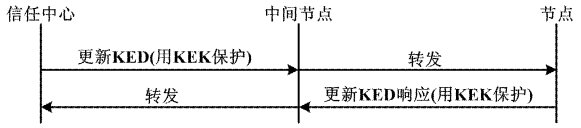

图 6　节点的密钥更新过程

Fig. 6　The updating process of node dongle

为保证密钥更新过程的安全及来源的合法性，信任中心一开始对节点分发密钥，即选择图 5 中的对应密钥链，将该密钥链的最后一个链密钥 K_M 及其他信息 D_1（如密钥类型、密钥长度等）装入报文 P_1（$P_1 = K_M \mid D_1$），并生成该报文的校验值 $MIC(P_1)$ 发送给节点。密钥更新报文格式如图 7 所示。节点先校验报文的正确性，然后对报文进行解密，获得会话密钥 K_M；在随后密钥更新过程中，信任中心依次发送 K_{M-1}、K_{M-2} 等。

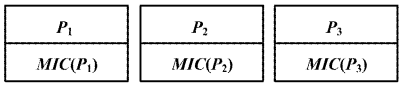

图 7　密钥更新报文格式

Fig. 7　The message format of dongle update

节点密钥更新流程如图 8 所示。

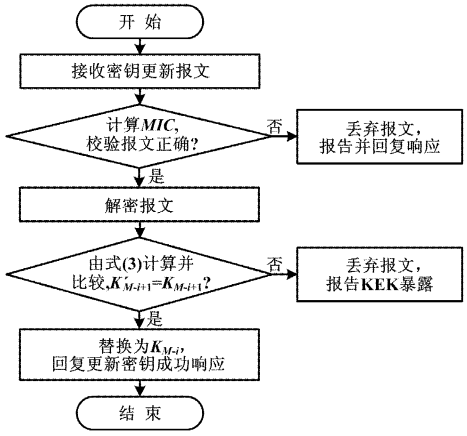

图 8　节点密钥更新流程图

Fig. 8　Flowchart of the dongle update

密钥更新时，节点接收到第（$i+1$）次更新报文 P_{i+1} 时，首先校验该报文是否正确，若不正确，直接回复更新密钥失败响应；否则，解密报文，获得 K_{M-i}。采用加入密钥并根据 $K'_{M-i+1} = F(K_{M+i}, \mathrm{KJ})$ 计算 K'_{M-i+1}，比较 K'_{M-i+1} 和已存储的第 i 次的密钥 K_{M-i+1}，如果相等，表明为合法的信任中心发送，未经过篡改，将已存储的 K_{M-i+1} 替换为 K_{M-i}，作为会话密钥；如果不等，则表明受到攻击，即报文来源不可信且 KEK 已暴露，此时，应向信任中心汇报。

3.3　安全性分析

在本方案中，密钥更新过程在不增加通信开销的情况下，只需节点进行一次散列函数运算，即可以实现数据报文的完整性、数据的机密性、数据本身的正确性和数据来源的合法性。本方案散列链的使用保证了所更新的密钥的安全性和有效性，与文献[5]相比，本方案增加了对数据源的认证。这是因为网络中只有信任中心和节点共享唯一公共散列链，在确保数据新鲜性的情况下可以认定该数据为信任中心所发送。根据散列链的特性——单向性[9]，攻击者即使破获了当前使用的会话密钥，在未知密钥链种子和加入密钥的情况下，不可能通过计算得到后续的会话密钥，而且也不可能获得散列链的种子。

由于节点的加入密钥是在网络部署前通过安全方式写入节点设备的，可认为是安全的，所以可以确保随后发送的密钥加密密钥是安全可靠的。由于密钥加密密钥也需进行周期性更新[1]，密钥加密密钥可以采用该方案中单向密钥链的形式进行下发和更新。

3.4　效率分析

本文从以下四个方面分析该方案的效率。

① 当网络中有新节点加入时，首先对其进行认证，认证通过，信任中心随机生成种子，并用该节点的加入密钥生成密钥链，然后进行密钥的分发和更新。

② 当有节点离开时，网络管理者删除与该节点共享的公共散列链，不影响网络中的其他节点正常通信，但离开的节点为簇首节点时，如果启用冗余簇首[7]，信任中心更新与冗余簇首共享的公共散列链即可。

③ 存储量及通信开销，该方案中节点只需存储三种类型的密钥，与文献[2]和[5]比较，本方案没有增加存储量和通信开销。

④ 生命周期，密钥链长度 M 期望值的选取根据式(7)计算。

$$M = T_{\mathrm{lifetime}} / T_{\mathrm{updatecycle}} + \delta_{\max} \tag{7}$$

式中：T_{lifetime} 为节点可以有效工作的存活时间；$T_{\mathrm{updatecycle}}$ 为密钥更新周期；$\delta_{\max}$ 为由网络状况预测节点遭遇攻击（含通信故障）的最大次数。

采用式(7)可解决链密钥在节点生命结束前用尽而无法进行后续密钥更新的问题，链密钥的长度 M 则满足了网络中节点的生命存活期。

3.5　丢包容忍性分析

当密钥更新节点已知如下信息：节点收到报文 P_i 并获得链密钥 K_{M-i+1}，丢失（$d-1$）次密钥更新报文，丢失期间 KEK 没有改变，暂存了更新密钥丢失期间所有不能解密的报文，收到正确的密钥更新报文 P_{i+d}，则节点将依次做出如下处理：①解密报文 P_{i+d}，得到

$K_{M-i-d+1}$;②对 $K_{M-i-d+1}$ 进行 d 次散列运算,分别得到 K'_{M-i+1},K'_{M-i},…,$K'_{M-i+d+1}$;③判断 $K'_{M-i-d+1}$ 是否与 K_{M-i+1} 相等,若不等,更新密钥失败,否则进入④;④可以确认所有更新密钥正确,依次用②中的密钥对相应期间的数据报文进行解密。

综上所述,该方案在特定期间内可以容忍一部分密钥更新报文的丢失,具有较好的容忍性,允许最大丢失个数由 KEK 的更新周期以及节点能够暂存的最大报文数量决定。

4　结束语

本文针对 WIA-PA 网络,提出了一种入网认证方案。在假定网络形成时所有节点都不可信情况下,保证了所有入网节点的合法性,并使用单向散列函数,提出了一种安全的密钥更新方案。这既保证了更新密钥的安全性,也保证了密钥来源的合法性,实现了消息认证和消息源的认证;同时,还具有较好的密钥更新报文丢失容忍性。经过分析,充分说明了该方案实现了对密钥的有效更新,大大增强了网络的安全性。该方案在保证网络安全通信的同时,对节点存储空间和通信量要求较低,并具有较好的可扩展性和灵活性,适合 WIA-PA 网络。

参考文献

[1] 工业无线网络 WIA 规范[S]. ICS 25.040,2008.

[2] 韩瑞,刘枫. 一种 WIA-PA 网络的密钥分配方案[J]. 计算机测量与控制,2010,18(1):186 - 188.

[3] 梁炜,张晓玲. WIA-PA:用于过程自动化的工业无线网络系统结构与通信规范[J]. 仪器仪表标准化与计量,2009(2):30 - 36.

[4] 苏忠,林闯,任丰原. 无线传感器网络中基于散列链的随机密钥预分发方案[J]. 计算机学报,2009,32(1):30 - 42.

[5] 田丰,王交峰,王传云,等. 无线传感器网络随机密钥预分配改进方案[J]. 计算机应用,2008,28(6):1388 - 1391.

[6] 王华,刘枫,杨颂华. 工业无线网络 WIA-PA 网络研究与设计[J]. 自动化与仪表,2009,24(7):1 - 4.

[7] 张丹,刘枫. WIA-PA 冗余簇首机制[J]. 计算机工程,2010,36(3):257 - 259.

[8] Perrig A,Szewczyk R,Tygar J D,et al. SPINS:security protocols for sensor networks[J]. Wireless Networks,2002,8(5):521 - 534.

[9] Bellare M,Canetti R,Krawczyk H. Keying hash functions for message authentication[J]. Advances in Cryptodogy-Crypto'96,Lecture Notes in Computer Science,1996,1109:1 - 15.

[10] Perrig A,Canetti R,Song D,et al. Efficient and secure source authentication for multicast[J]. Network and Distributed System Security symposium,2001:35 - 46.

[11] Perrig A,Canetti R,Tygar J D,et al. Efficient authentication and signing of multicast streams over lossy channels[C]// Proceedings of the 2000 IEEE Symposium on Security and Privacy,Berkeley,CA,USA,2000:56 - 74.

(上接第 5 页)

制方法,以缩短开发时间,降低开发成本;最后,开发有通用性、可重用性和升级扩充要求且需长期使用的测控程序时(如引言中提到的应用场合),使用基于 VISA 的 SCPI 字符串编程和使用 IVI 类驱动编程是两种强烈推荐的仪器控制编程模式,若程序规模较小,推荐使用前者以减小程序依赖项,否则,推荐使用后者,以降低程序开发难度。

参考文献

[1] 李宁,李进杰. 仪器控制技术在自动测量系统中的应用[J]. 工业控制计算机,2008,21(1):1 - 2.

[2] National Instruments Corp. Instrument control technologies for any bus, any language[EB/OL]. [2010 - 05 - 01]. http://sine.ni.com/np/app/culdesac/p/ap/ictrl/lang/en/pg/1/sn/n17:ictrl/docid/tut-3513.

[3] Sokoloff L. GPIB instrument control[C]//Proceedings of the 2002 ASEE Annual Conference,Montreal,Canada,2002:3107 - 3121.

[4] 罗光坤,张令弥,王彤. 基于 GPIB 接口的仪器与计算机之间的通讯[J]. 仪器仪表学报,2006,27(6):634 - 637.

[5] Maxim Corp. RS-485(EIA/TIA-485) differential data transmission system basics[EB/OL]. [2010 - 05 - 02]. http://pdfserv.maxim-ic.com/en/an/AN736.pdf.

[6] 肖风云,马廷卫,唐义清. 基于 VISA 标准的仪器驱动器设计[J]. 机械工程与自动化,2006(2):132 - 135.

[7] VXIplug&play Systems Alliance. The VISA library[EB/OL]. [2010 - 05 - 02]. http://www.ivifoundation.org/docs/vpp43.pdf.

[8] 朱波,李华. 基于 SCPI 语言的智能仪器 LabVIEW 驱动程序设计[J]. 仪表技术与传感器,2008(9):53 - 54.

[9] SCPI Consortium. Standard commands for programmable instruments [EB/OL]. [2010 - 05 - 01]. http://www.ivifoundation.org/docs/SCPI-99.pdf.

[10] 刘立,陈淑珍. 虚拟仪器系统与 VXI、VXIplug&play[J]. 国外电子测量技术,1999(2):28 - 29.

[11] National Instruments Corp. Developing LabVIEW plug and play instrument drivers[EB/OL]. [2010 - 05 - 01]. http://zone.ni.com/devzone/cda/tut/p/id/3271.

[12] IVI Foundation. Getting started with IVI drivers[EB/OL]. [2010 - 05 - 01]. http://www.ivifoundation.org/.

[13] Franklin P,Ryland J. IVI instrument driver guided tour[C]//AUTOTESTCON Proceedings,Cleveland,USA,2004:167 - 173.

[14] Cheij D. Using IVI drivers to increase test system performance[C]// AUTOTESTCON Proceedings,Anaheim,USA,2000:375 - 379.

[15] National Instruments Corp. How IVI-C instrument driver technology enables system longevity and platform portability[EB/OL]. [2010 - 05 - 11]. http://zone.ni.com/devzone/cda/tut/p/id/3433.