工业以太网控制系统中网络节点位置信息自动绑定协议研究

周纯杰 於光灿 秦元庆 陈 开
(华中科技大学控制科学与工程系 武汉 430074)

摘 要 在DHCP协议基础上提出p_DHCP协议。p_DHCP继承DHCP的传输协议,具体化DHCP的地址分配机制。在现场维护人员按照规定的流程为控制系统更换和添加网络节点的情况下,p_DHCP协议能够实现工业以太网控制系统中网络节点逻辑位置信息的自动绑定。

关键词 工业以太网,逻辑位置,自动绑定

Position Information Automatically Binding Protocol of Network Nodes in the Industry Ethernet Control System

ZHOU Chun-jie YU Guang-can QIN Yuan-qing CHEN Kai
(Department of Control Science & Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Position based dynamic host configuration protocol(p_DHCP) was proposed based on the dynamic host configuration protocol(DHCP). The p_DHCP inherits the protocol for delivering host-specific configuration parameters from a DHCP server to a host, and specifies mechanism for allocation of network addresses to hosts. If network nodes in the industry Ethernet control system are maintained following the given rules, p_DHCP can achieve position information automatical binding of network nodes.

Keywords Industry Ethernet, Logic position, Automatically binding

工业以太网络控制系统融合了计算机技术、通信技术与控制技术,体现了控制系统的网络化、集成化、节点智能化的发展趋势,是控制界研究的热点之一,已经在工业控制领域、楼宇自动化等方面得到了广泛应用[1]。工业以太网主要是通过采用减轻以太网负荷、提高网络速度、交换式以太网和全双工通信、流量控制及虚拟局域网等技术提高网络的实时响应速度,而在技术上与商用以太网兼容的控制网络,符合IEEE802.3标准[2,3]。为了实现与传统以太网的无缝连接,工业以太网通常都支持网络层IP协议、传输层TCP和UDP协议以及应用层的FTP、DHCP等协议。为工业以太网控制系统中的网络节点正确配置IP地址,是系统正常的前提条件。用人工进行IP地址配置,既不方便又容易出错,对现场维护人员有较高要求,而且网络节点不一定具有显示界面和用户交互接口,因此往往需要采用自动协议配置的方法。

动态主机配置协议(The Dynamic Host Configuration Protocol,DHCP)能够为工业以太网络控制系统中的网络节点自动配置网络参数(如IP地址)[4]。在工业以太网络控制系统中,要对各个网络节点分别进行控制,除了需要掌握所有网络节点的IP地址外,还需要掌握每个IP地址所对应的网络节点的设备类型及其逻辑位置。本文将IP地址和网络节点的类型及其逻辑位置的对应关系简称为节点位置信息绑定。在为网络节点分配IP地址过程中,通过消息的交互可以获取设备类型(DHCP交互消息的选项部分可以实现该功能)[5]。如果控制系统中每种类型的设备只有一个的话,那么根据IP地址就可以确定设备的类型和逻辑位置(因为系统中仅有一个该类型的节点)。但是,如果控制系统中有多个某个类型节点,而且这些节点在控制系统中所担负的控制功能有所不同,比如设备A,B分别用于控制两个不同的水泥转窑,虽然设备A,B是相同类型的设备,但是所控制的对象不同,必须分别加以控制,那么必须进行节点位置信息绑定。本文对DHCP协议进行扩展,以实现工业以太网络控制系统中网络节点逻辑位置的自动绑定。

1 DHCP协议简介

DHCP采用客户机-服务器(Client/Server)模式,由传输协议和网络地址分配机制两部分组成。传输协议用于将网络配置参数由DHCP服务器传递到网络上的客户机,地址分配机制为网络上的客户机分配网络地址。DHCP是一种机制,而不是一种策略,能够通过DHCP这种手段为网络节点分配并传递网络参数。但是,如何分配网络参数,DHCP没有解决,需要由网络管理员根据实际情况制订相关的配置策略。

DHCP协议中客户机和服务器主要交互过程如下:

(1)客户机广播一个DHCPDISCOVER消息,用于查找DHCP服务器,消息的chaddr域携带客户机的物理地址(MAC地址),消息的选项域可以携带设备的类型信息。

(2)DHCP服务器以DHCPOFFER消息响应,在消息的

到稿日期:2008-12-24 返修日期:2009-03-05 本文受国家自然科学基金项目(60674081,60834002)资助。

周纯杰 教授,博士生导师,主要研究方向为现场总线技术及应用、嵌入式控制系统、计算机网络;於光灿(1974-),男,博士,主要研究方向为网络安全控制系统,E-mail:xgygcan@tom.com;秦元庆 博士,主要研究方向为智能图像处理;陈 开 硕士生,主要研究方向为嵌入式控制系统。

yiadder 域中携带一个有效的 IP 地址，将该 IP 地址预分配给对应客户机。

(3)客户机收到 DHCPOFFER 消息后，对分配的 IP 地址进行有关的检查，如用 ARP 命令查看本网段中是否已有主机占用该 IP 地址。检查合格后，向服务器发送 DHCPREQUEST 消息，正式请求使用该 IP 地址。

(4)服务器收到 DHCPREQUEST 消息后，对请求参数进行验证，如何验证客户机请求对该 IP 的使用期限。验证通过后，向客户机发送 DHCPACK 消息，正式将该 IP 地址分配给客户机。如果验证没有通过，向客户机发送 DHCPNAK 消息，拒绝客户机使用该 IP 地址。

(5)客户机收到 DHCPACK 消息后，使用该 IP 地址配置本地网络，配置过程结束。客户机收到 DHCPNAK 消息后，表明服务器不允许其使用该 IP 地址或申请期限不合要求。延时一段时间后，从步骤 1 开始重新申请过程。整个交互过程如图 1 所示。

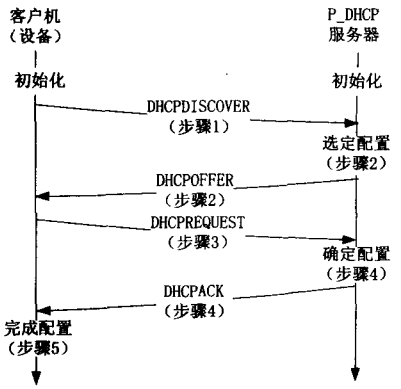

图 1　DHCP 服务器与客户机消息交换时序图

如果客户机重新启动后继续使用上次分配的 IP 地址，地址申请过程就不需要从步骤 1 开始，直接从步骤 4 开始即可，DHCPREQUEST 消息携带上次分配的 IP 地址和客户机的物理地址。

2　设备逻辑位置信息自动绑定协议

解决以太网控制系统的网络自动配置及节点逻辑位置自动绑定问题的一个有效解决办法是，在设计阶段，首先确定网络的逻辑结构，对每个网络节点接入点进行编号并给出该接入点的 IP 地址及设备类型，即 IP 地址反映网络节点在控制系统中的逻辑位置。在控制系统施工维护阶段，现场维护人员根据接入点设备类型信息将设备一一接入到对应的接入点。节点被正确接入到控制系统后，下面的问题就是如何将接入点的 IP 地址分配给接入点对应的设备，即现场总线上每个节点接入点的 IP 地址要能正确地分配给从该接入点接入的网络节点。下面对 DHCP 进行扩展，以满足节点逻辑位置信息自动绑定的需要。

2.1　对 DHCP 协议的扩展及相关算法

为了描述方便，将扩展后的协议称为 p_DHCP(Position based Dynamic Host Configuration Protocol)。p_DHCP 继承 DHCP 的所有消息类型和消息格式，客户机与服务器交互过程与 DHCP 基本相同，只是对步骤(2)和(4)加以扩展，其他几个步骤保持不变。

首先定义工业以太网控制系统网络配置及设备状态表(简写为 CFG_STAT)，数据结构如表 1 所列。该表存放于 p_DHCP 服务器中，各数据项分别解释如下。

表 1　网络配置及设备状态表(CFG_STAT)

接入点编号	节点类型	IP 地址	是否已接入	MAC 地址	是否在线

接入点编号：工业以太网控制系统中每个网络节点接入点的唯一编号，代表控制系统中的逻辑位置。上层应用程序根据接入点编号查询设备类型及 IP 地址，获取这些信息后即可通过以太网络进行相关控制。

节点类型：网络节点的生产厂家(联盟)对节点的分类。相同类型节点的功能和网络接口相同，比如分别用于控制两个不同水泥转窑的节点 A，B，属于同一个类型。具体来讲，就是客户机和服务器交互的第一步骤中，客户机发送的 DHCPDISCOVER 消息中选项域携带的设备类型相同的设备属于同一类型。

IP 地址：为每个网络节点接入点预先分配的 IP 地址。通过下面的算法，将接入点 IP 地址分配给从该接入点接入现场总线的网络节点。

是否已接入：表示接入点的网络节点已经接入并被分配该接入点对应的 IP 地址。

MAC 地址：登记接入点网络节点所使用的物理地址。

是否在线：表示对应接入点网络节点在线情况。该数据项主要用于控制系统的节点保护协议。节点保护是指通过定时向节点发送探测消息，以探测节点目前是否在线。节点保护协议能够对控制系统的网络配置起辅助作用，两者之间的配合关系将在下面论述。

工业以太网控制系统的网络结构设计完成后，上述网络配置及设备状态表的节点接入点编号、节点类型、IP 地址等 3 个数据项即同时设置完成。控制系统网络配置完成后是否已接入和 MAC 地址两个数据项同时设置完成，控制系统运行过程中节点保护程序根据探测结果实时修改是否在线数据项。

p_DHCP 协议中将网络配置过程明确划分为节点接入准备阶段和节点接入阶段。网络配置完成后，系统进入正常运行阶段，服务器端提供用户交互界面或拨码开关等硬件接口，用于管理员明确指定系统目前所处的阶段。

p_DHCP 对 DHCP 协议中客户机和服务器的主要交互过程步骤(2)修改细化如下：

(2)服务器处于正常运行阶段和节点接入准备阶段时，DHCP 服务器收到从客户端发出的 DHCPDISCOVER 消息后，取出消息 chaddr 域携带的客户机 MAC 地址，在 CFG_STAT 表中查询该 MAC 地址对应的 IP 地址，以 DHCPOFFER 消息响应，在消息的 yiadder 域中携带查询到的 IP 地址，将该 IP 地址预分配给对应客户机。系统处于设备接入阶段时，本步骤细化为以下 3 个步骤：

(2.1)定义接入工业以太网控制系统节点的最大启动时间为 Max_T。系统进入节点接入阶段后，循环等待，以收集从客户机发送来的 DHCPDISCOVER 消息。当等待时间到达 Max_T 时，结束等待，从收集到的 DHCPDISCOVER 消息集(去除重复消息)中抽取出每条消息携带的设备类型及 MAC 地址信息，去除已经存在于 CFG_STAT 表中的 MAC 地址及其对应设备类型，余下的 MAC 地址及设备类型为新

接入系统的节点。将新接入系统节点的 MAC 地址按从小到大的顺序排序，排序后的 MAC 地址、设备类型形成表 2 所列数据结构。

表 2　MAC 地址、设备类型对应表(MAC_TYPE)

MAC 地址	设备类型

(2.2) 从 MAC_TYPE 表中从前至后依次取出每条记录，在 CFG_STAT 表中从前至后搜索设备类型域。当 CFG_STAT 表和 MAC_TYPE 表当前记录的设备类型域匹配且 CFG_STAT 表当前记录的 MAC 地址为空时，将 MAC_TYPE 表当前记录的 MAC 地址填入到 CFG_TYPE 表当前记录的 MAC 地址域，表示将该行的 IP 分配给 MAC 地址对应的节点。以此类推，直至整个过程完成。IP 地址分配算法伪代码如图 2 所示。

(2.3) 从 CFG_STAT 表中依次取出新加入节点(CFG_STAT 表 MAC 地址域不为空而是否已接入域为空行所对应的设备)的 MAC 地址和 IP 地址，针对 MAC 地址回复 DHCPOFFER 消息，在消息的 yiadder 域中携带 IP 地址。

p_DHCP 对 DHCP 协议中客户机和服务器主要交互过程步骤(4)修改如下：

(4)服务器收到 DHCPREQUEST 消息后，对请求参数进行验证。取出 DHCPREQUEST 消息中携带的 MAC 地址。在 CFG_STAT 表中查找该 MAC 地址，如果该 MAC 地址在表中没有登记，则向客户机发送 DHCPNAK 消息，拒绝客户机的请求；如果在表中查找到该 MAC 地址，取出对应的 IP 地址，向客户机发送 DHCPACK 消息，正式将该 IP 地址分配给客户机。同时，如果是否已接入数据域为“否”，则将其修改为“是”。

```
For i=1 to MAC_TYPE. length
  For j=1 to CFG_STAT. lenght
        if CFG_STAT(j). 设备类型==MAC_TYPE(i).
设备类型
and CFG_STAT(j). MAC 地址==NULL then
        CFG_STAT(j). MAC 地址==MAC_TYPE(i).
MAC 地址
    End if
  End for
```

说明：MAC_TYPE. length 表示 MAC_TYPE 表的行数

CFG_STAT. lenght 表示 CFG_STAT 表的行数

CFG_STAT(j). 设备类型表示 CFG_STAT 表第 j 行的设备类型域

MAC_TYPE(i). MAC 地址表示 MAC_TYPE 表第 i 行的 MAC 地址域

图 2　步骤(2.2)中 IP 地址分配算法

2.2　设备接入或更换有关限制及操作流程

为了配合上述算法，实现节点逻辑位置信息自动绑定，现场维护人员在接入设备时要遵循以下规定：如果同一类型的节点在控制系统中仅有一个，在往控制系统中接入该类型节点时，用户只需将节点接入该类型节点对应的接入点即可；如果同一类型节点在控制系统中有多个，那么接入节点前需先对待接入节点的 MAC 地址进行排序，将经过排序后的设备按由小到大的顺序依次接入控制系统接入点编号由小到大的该类型设备接入点中。通过这种方式来确保将控制系统接入点 IP 地址正确地分配给从该接入点接入的设备，实现节点逻辑位置信息自动绑定。

工业以太网控制系统中的节点不可避免要老化损坏。设备损坏后一般要求以最快的速度修理或更换，工业现场的特性要求可以用多种方式更换节点，包括：

(1)用新的节点替换损坏的节点；

(2)从其他的相同或相似控制系统中卸下的节点替换损坏的节点；

(3)节点经维修后再次接入控制系统(不一定从原来的接入点接入)。

对于上述第一种情况，新节点没有被配置过网络，使用 p_DHCP 协议能够为其正确配置网络；对于第二种情况，从其他相同或相似控制系统中卸下的节点已经被配置过网络，但是其 MAC 地址在服务器的 CFG_STAT 表中没有登记，算法会重新为其分配新的 IP 地址，以替换旧的 IP 地址，也能被正确配置网络；对于第三种情况，如果节点被卸下，经维修后又被接入原来的控制系统，且新的接入点与原来的接入点不同，因为其 MAC 地址和 IP 地址在服务器的 CFG_STAT 表中已登记，可能会造成其 IP 地址和接入点 IP 地址不一致的情况，破坏节点逻辑位置信息的绑定，所以上文将控制系统网络配置过程强制划分为节点接入准备阶段和节点接入阶段。网络配置完成后，系统进入正常运行阶段。通过这 3 个阶段的划分，再配合节点保护协议，可以解决上述问题。下面详细介绍这 3 个阶段进行的操作及达到的目标。

节点接入准备阶段是往现场总线中接入节点前的准备阶段。在这个阶段，节点保护系统依次探测 CFG_STAT 表中登记的所有节点(探测策略在此不再详细论述)。对于探测不到的节点，将其在 CFG_STAT 表中的登记项删除，即清除对应行的 MAC 地址、IP 地址、是否已接入、是否在线等数据域，并向管理员报告。管理员根据报告从控制系统中卸下损坏的节点。在这个阶段只允许从控制系统中卸下节点，严禁接入新的节点。即使接入新的节点，也不会被分配 IP 地址。本阶段达到的目标是确认 CFG_STAT 表中登记的所有节点都能正常工作(至少能响应节点保护的探测消息)。

节点接入阶段是往控制系统中添加节点的阶段。在这个阶段，现场维护人员按照上述接入节点规则将需要接入系统的节点一一接入。这个阶段的目标是为所有新加入节点分配 IP 地址，而保留原有节点 IP 地址不变。

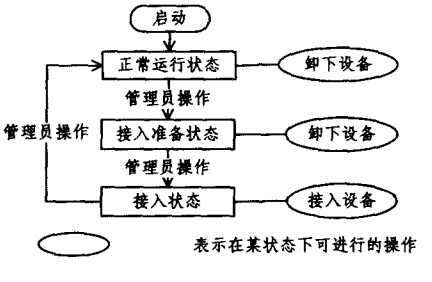

图 3　节点接处准备、节点接入及正常运行 3 个阶段状态转换图

正常运行阶段是指控制系统网络配置完毕，进入正常运行状态。节点保护系统探测各节点运行情况，将出现故障的节点在 CFG_STAT 表对应行的是否在线域更改为“否”，同时通知管理员处理故障节点。节点恢复正常后，将其是否在

线域更改为“是”。

以上3个阶段是针对控制系统网络配置过程而言，在各个阶段进行切换不影响上层控制系统的运行。因为在各个阶段之间切换只是为新接入节点分配IP地址，控制系统的原有节点在各阶段切换过程中其IP地址会保持不变。在系统正常运行时，对于由于节点掉电等原因引起短暂故障的节点，p_DHCP能够确保在故障排除后保留其原有IP，保证其逻辑位置信息正确绑定。网络配置3个阶段状态转换如图3所示。

2.3 p_DHCP与DHCP的对比分析

如上所述，DHCP由传输协议和网络地址分配机制两部分组成。传输协议用于将网络配置参数由DHCP服务器传递到网络上的客户机，地址分配机制为网络上的客户机分配网络地址。P_DHCP协议完整继承DHCP的传输协议，即继承了DHCP的所有消息类型和消息格式以及客户机与服务器交互过程，具体化了地址分配机制。

P_DHCP根据工业以太网控制系统节点逻辑位置信息自动绑定的需要具体化了地址分配机制，将网络配置过程明确划分为节点接入准备和节点接入两个阶段。网络配置完成后，系统进入正常运行阶段。在节点接入准备阶段和系统正常运行阶段，p_DHCP与DHCP完全相同，只是具体化了地址分配机制。服务器收到客户端发来的DHCPDISCOVERY消息后根据CFG_STAT表中的登记分配IP地址。而在节点接入阶段与DHCP不同之处在于，DHCP针对每个DHCPDISCOVERY消息进行响应，以为客户机分配IP地址；而p_DHCP需等待Max_T时间，以收集DHCPDISCOVERY消息，根据MAC地址的大小顺序进行IP地址分配。配合现场维护人员在接入设备时遵循的有关规定，实现节点逻辑位置信息自动绑定。

结束语 本文在DHCP基础上提出p_DHCP协议。P_DHCP协议完整继承了DHCP的传输协议，具体化了DHCP的地址分配机制，实现工业以太网控制系统中节点逻辑位置信息的自动绑定。p_DHCP需要得到现场维护人员的配合。一次更换多个同种类型的节点时，要保证节点MAC地址和节点接入点编号有相同的顺序，即较小的MAC地址接入编号较小的接入点，较大的MAC地址接入编号较大的接入点。p_DHCP在实现节点逻辑位置信息自动绑定的前提下，尽量减少对DHCP协议的修改。p_DHCP与DHCP的客户端完全一致，服务器端也只是在步骤(2)上有一个小的变动，协议实现起来较为容易，不需要修改现有的客户端网络节点。

参 考 文 献

[1] 王平，谢昊飞，向敏，等. 工业以太网技术[M]. 北京：科学出版社，2007

[2] 冯冬芹，黄文君. 工业通信网络与系统集成[M]. 北京：科学出版社，2005

[3] 阳宪惠. 工业数据通信与控制网络[M]. 北京：清华大学出版社，2002

[4] Droms R. Dynamic Host Configuration Protocol[S]. RFC1541. Bucknell University, October 1993

[5] Alexander S, Droms R. DHCP Options and BOOTP Vendor Extensions, RFC 1533. Lachman Technology, Inc., Bucknell University, October 1993

(上接第107页)

个方面：

(1) 协议的安全性主要是通过进行hash函数运算和模2加运算来保证的。但是模2加运算计算简单，这就导致了一旦进行模2加法运算的某些值泄漏，就会导致整个协议被攻击。

(2) 协议为了增加对口令的保护，服务器也不知道用户的口令，所以当用户传送过来计算 $h^2(S||P||N_{i+1})$ 时，服务器也不知道该值是否正确，无法对该信息的正确性进行验证。

3.2 漏洞改进的方法

上节已经分析了协议能够被攻击的原因，本节探讨如何修改协议，使其成为一个安全的密码协议。

协议能够被攻击的第一个原因是模2加运算简单。也就是说，当 $M=M_1 \oplus M_2$ 时，在已知 M 的前提下只要知道 M_1 (或 M_2)就可以通过对 M 模2加法运算求出 M_2 (或 M_1)，那么要克服这个缺陷，可以采取以下两种策略：①加强对信息 M_1，M_2 的保密，增强其机密性；②增加计算的复杂性，即类似 $M=M_1 \oplus M_2 \oplus M_3$。这样，攻击者要想获得 M_1，M_2，M_3 中某个机密信息，就必须先获得其中的另外两条信息，从而增加攻击的难度。

协议能够被攻击的第二个原因是服务器方无法对信息 $h^2(S||P||N_{i+1})$ 的正确性进行判断。要克服这个缺点，可以采用以下两种策略：①让服务器知道用户的密码，这样服务器也能生成 $h^2(S||P||N_{i+1})$，自然也就能验证该信息的正确性；②采用公钥密码技术，让用户对 $h^2(S||P||N_{i+1})$ 连同一个新鲜因子一起进行数字签名，从而保证信息来源的真实性，再通过新鲜因子的新鲜性来保证整条签名信息的新鲜性；③采用对称密码技术，用服务器与用户的预共享对称密钥来加密关键信息。

结束语 本文研究了基于散列函数的强口令密码认证协议，分析了目前该类协议中具有较高安全性的SPAS协议。通过分析，发现协议存在安全漏洞。产生安全缺陷的主要原因，是协议中使用的密码技术过于单一。在具体使用过程中，为了达到安全要求，必须综合使用其他密码技术。

参 考 文 献

[1] 虞淑瑶、叶润国，等. 一种安全高效的强口令认证协议[J]. 计算机工程，2006，32(6)：146-147

[2] 泰小龙，杨义先. 强口令认证协议的组合攻击[J]. 电子学报，2003，32(7)：1043-1045

[3] 李莉，薛锐，等. 基于口令认证的密钥交换协议的安全性分析[J]. 电子学报，2005，33(1)：166-170

[4] 陈开渠. 基于口令的认证：协议和应用[D]. 北京：中国科学院软件研究所，2000

[5] Halevi S, Krawczyk H. Public-key Cryptography and Password Protocols[C]// Proceedings 5th ACM Conference on Computer and Communications Security. San Francisco, CA, 1998：122-131

[6] Ku W C, Chen S M. Weaknesses and improvements of an efficient password base remote user authentication scheme using smart cards [J]. IEEE Transactions on Consumer Electronics, 2004, 50(1)：204-206