一种基于跳频预约模式的RFID读写器网络MAC协议

王永华[1] 詹宜巨[2] 杨 健[1] 蔡庆玲[2]
(广东工业大学自动化学院 广州 510006)[1] (中山大学工学院 广州 510275)[2]

摘 要 在大量RFID读写器应用场合,会产生读写器冲突问题,从而影响整个系统的读取率。为了解决读写器冲突问题,提出了一个建立在慢跳频扩频(FHSS)上的MAC协议。该协议采用阅读器同步机制,读写器首先通过不同的时隙竞争预约信道,成功后使用与该时隙对应的频率进行通信,并通知相邻读写器,避免了相邻读写器同时与同一个标签通信,避免了读写器-标签冲突;采用读写器通信和标签通信按频谱分开的机制,使得读写器和标签之间不会产生频率冲突;采用多个频率跳频机制,避免了读写器频率冲突。对该协议进行的分析表明,在读写器负载较大及读写器平均通信时间较长时,该协议的系统输出较高。

关键词 射频识别,读写器,防冲突,MAC
中图法分类号 TN911.23 **文献标识码** A

New MAC Protocol Based on Frequency Hop-reservation for RFID Reader Networks

WANG Yong-hua[1] ZHAN Yi-ju[2] YANG Jian[1] CAI Qing-ling[2]
(Faculty of Automation, Guangdong University of Technology, Guangzhou 510006, China)[1]
(School of Engineering, Sun Yat-sen University, Guangzhou 510275, China)[2]

Abstract The RFID reader collision problem emerges in the large applications; it will decrease the read rate of the whole system. A MAC protocol based on the slow frequency hopping spread spectrum (FHSS) was proposed to resolve the reader collision problem. This MAC used reader synchronization mechanism. The reader used the corresponding frequency to communicate with tags if the reader competed with others and reserved the time slot successfully, and informed the neighbor readers to avoid communicating with tag simultaneously, thus prevented the tag interference. This MAC adopted the mechanism that reader transmissions and tag transmissions are on separate frequency channels and the muti-frenquency hopping, so tags collide with tags but not with readers and readers collide with readers but not with tags, and such separation solves the reader frequency interference. The analysis results of the algorithm show that when the reader load is bigger and the reader average correspondence time is longer, the system throughput is higher.

Keywords RFID, Reader, Anti-collision, MAC

射频识别(Radio Frequency Identification, RFID)技术是一种利用射频通信实现的非接触式自动识别技术[1],获得了广泛的应用。RFID由电子标签(Tag)、读写器(Reader)和数据管理系统构成。

在密集读写器环境下,由于读写器阅读区域的相互重叠或者由于采用相同的频率通信,会产生读写器冲突。读写器冲突(Reader Collision)是指由一个读写器检测到的、由另一个读写器引起的干扰,包含两种情况:读写器-读写器冲突\频率冲突(Reader to Reader Interference\ Reader Frequency Interference)和读写器-标签冲突(Reader to Tag Interference)[2,3]。读写器频率冲突发生在两个或更多读写器同时使用相同的频率与标签通信时;读写器-标签冲突是指两个或更多读写器同时与一个标签通信时发生的冲突。

由于无源标签的低功能特性,其在与多个读写器通信过程中无法对读写器冲突起作用。读写器冲突在大量使用手持式移动读写器时会大大加剧。读写器冲突问题会影响整个系统的读取率,因此需要研究不需要标签参与的读写器防冲突机制。

目前解决读写器冲突研究的方法主要有EPC CLASS-1 2代标准、ETSI EN 302 208标准、Colorwave算法、PULSE算法等。

EPC CLASS-1 2代标准[4]采用频谱规划(FDMA)的方法将读写器通信和标签通信按频谱分开,避免了读写器-读写器频率干扰,但多个读写器与标签的干扰仍然存在。解决方法之一就是采用准确的、基于时间的阅读器同步机制,该机制旨在防止两个读写器同时与同一个标签通信[5]。ETSI EN

到稿日期:2009-09-15 返修日期:2009-11-25 本文受广东省科技计划项目(2008B10200037),广州市科技计划项目(2008Z1-D141),国家自然科学基金(60673132),广东省自然科学基金(9151027501000076)资助。
王永华(1979-),男,博士,讲师,主要研究方向为射频识别技术、通信与网络技术,E-mail:sjzwyh@163.com;詹宜巨(1955-),男,博士,教授,博士生导师,主要研究方向为射频识别、控制网络技术;杨 健(1982-),男,博士,讲师,主要研究方向为通信与信息系统、射频识别技术;蔡庆玲(1966-),女,博士,讲师,主要研究方向为RFID技术及其安全问题。

302 208 标准[6]采用了基于载波侦听的"Listen before talk"方法，但是在密集读写器环境中，LBT 将使得整个读写器网络不能工作在最优模式[3]，因为 LBT 会使得很多本来能用的通道关闭。Colorwave 算法[7]是一种分布式在线 TDMA 算法，要求读写器之间时间同步，同时假设读写器能够检测冲突。如果有读写器移动，可能导致整个系统效率降低。PULSE 算法[8]将读写器的通信信道分为控制信道和数据信道，控制信道用来发送忙音信号，用于读写器之间的相互通信；数据信道用于读写器与标签的通信。

为了解决读写器冲突问题，本文提出了一个建立在慢跳频扩频（FHSS）上的基于预约的 RFID 读写器网络 MAC（FHR，Frequency Hop-Reservation）协议。FHR 协议采用读写器同步机制，读写器首先通过不同的时隙竞争信道，成功后使用与该时隙对应的频率进行通信，并通知相邻读写器，避免相邻读写器同时与同一个标签通信。同时，采用了读写器和标签分别使用不同通信频率的机制，使得读写器和标签之间不会产生冲突，并采用多个频率跳频机制，避免了读写器频率冲突。

1 FHR 协议

1.1 基本思路

FHR 协议是一种无需载波侦听的 MAC 接入协议。它是一种分时隙的预约协议，但是每个时隙都有其独立的频点[9,10]。

FHR 协议使用 L（奇数）个有效频点，选择其中一个频点（f_0）作为同步信道，用于读写器间交换同步、跳频及时隙号等信息。剩余的 $L-1$ 个频点分为 $M=[(L-1)/2]$ 个频率对，即（f_i，f_i^*），$i=1,2,\cdots,m$，其中 f_i 用于读写器发送数据，f_i^* 用于标签发送数据。

每帧的结构为：首先包括一个专用同步时隙，其长度与普通时隙相等，频点为 f_0；接着是 M 个不同频点的普通时隙。每个普通时隙由同步期、CLR 期、RTS 期、HR 期构成。这些更小的时间单位分别用于发送或是接收同步帧、CLR 帧、RTS 帧、HR 帧，如图 1 所示。所有不参与通信的读写器在每个时隙中都跳到同步频率上交换同步信息。

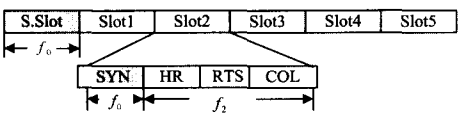

图 1 帧结构

1.2 读写器的接入过程

一个读写器刚开机的时候，必须先对同步信道侦听足够长时间，以获取系统的跳频模式及系统的定时信息，达到与系统同步。如果读写器没侦听到任何信息，也就是周围没其他读写器在工作，那么，该读写器可以广播自己的同步信息，并创建一个新的单节点系统[10]。

当一个空闲读写器在一个时隙的 RTS 期之前有通信需求时，需要先检查自己的 HR 标志。如果 HR 标志存在，说明有相邻的读写器在进行通信，所以该读写器暂时不能进行通信，要等待 HR 标志清除。如果不存在 HR 标志，则读写器就在 RTS 期发送 RTS，向邻读写器表明自己计划采用这个频点通信。如果未发生 RTS 冲突，则该读写器就在 HR 期发送 HR，向周围读写器表明自己接下来使用该频点进行通信，收到 HR 的邻居读写器随后保持与周围读写器的同步，但是不再请求通信，直到收到发送 HR 读写器发出的 CLR 信号为止。如果发生 RTS 冲突，则读写器要退避。退避时间为随机数，并且是时隙的整数倍，在退避结束后的时隙里准备重新发送。

当一个空闲读写器在 RTS 期开始后出现通信需求时，它已经不可能请求当前的频率点了，所以要进行退避。在一个时隙的 HR 期之后，所有不参与通信的读写器都跳到 f_0 频点上准备交互同步信息，然后跳到下一个时隙的频点上。

读写器占用该频点的时间可以任意长，可以与多个标签同时通信，但是该占用时间是在电信部门规定的最大跳持续时间内。当该读写器通信完之后，在 CLR 期发送 CLR，表明自己通信完成。收到 CLR 信号的读写器清除 HR 标志。

为了防止读写器错失 CLR 信号情况的发生，规定 HR 标志存在的时间不大于规定的最大跳持续时间，否则自动清除。

读写器通信的过程中，如果因为读写器移动的原因发现与其他读写器发生冲突，则马上停止通信，进行退避。

第一种情况：预约成功；第二种情况：预约失败，在 RTS 期发生了冲突。基本运行过程如图 2 所示。

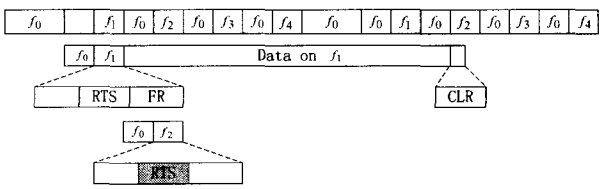

图 2 基本运行过程

1.3 读写器冲突问题的解决

图 3 所示为一个读写器网络例子。两个读写器有直线连接，表示有阅读区域重叠，即为相邻读写器，并且能相互通信。假设如果两个读写器至少相距两跳远，即中间间隔有读写器，并且无阅读区域重叠，那么这两个读写器即使同时使用同一频率通信，也不会发生读写器频率冲突。

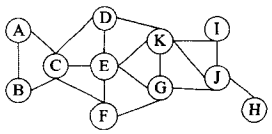

图 3 一个读写器网络

假设在第 m 个时隙，频率为 f_i，读写器 E 要通信，发送 RTS。如果同时 C,D,F,K,G 中有一个也发送 RTS，则在 E 通信范围内的读写器就会发生 RTS 冲突，结果是发送 RTS 的读写器进行随机退避。所以可以假设在频率为 f_i 的第 m 个时隙，只有 E 能够成功发送 RTS，并能占用该频点通信。该读写器发送 HR 信号后，相邻的读写器暂时不进行通信，避免了相邻读写器同时与同一个标签通信。如果该读写器通信的时间大于一帧，则由于周围读写器的 HR 标志未清除，因此在后续帧中，该读写器仍能进行无冲突的通信。

在 E 与标签通信的同时，在其相距两跳远之外的读写器可以与标签进行通信。并且由于采用多个频率跳频机制，因此避免了读写器频率冲突。

2 协议模型

假设系统有 M 个可用频率对，每个读写器周围有 N 个

读写器，网络拓扑是对称的。为了计算简单，忽略了传输延迟和数据的处理时间。假设读写器通信是理想信道，所以出错也只是由发生冲突导致。分析过程中假定读写器已进入读写器同步状态。

假设 CLR，RTS，HR 时间分别为 γ，并且同步时间 SYN 为 $(c-1)\gamma$，这样一个时隙长度就是 $\eta=(c+2)\gamma$。假设读写器通信的需求符合参数为 λ 的泊松过程，由泊松分布的性质可知读写器需要通信的概率为

$$P_A=1-e^{-\lambda\gamma} \tag{1}$$

假设每次通信的时间符合几何分布，平均通信时间是 d 个时隙，并且每次通信的时间是时隙的整数倍。因此读写器通信时间为在一个时隙内结束的概率 $q=\frac{1}{d}$；也可以得出不在一个时隙内结束的概率 $p=1-q$。

设读写器在一个时隙内通信的概率为 P_T，空闲的概率为 P_I。系统输出 S 定义为每个读写器的平均利用率，也即单位时间内读写器成功与标签通信的概率，所以

$$S=P_T=1-P_I \tag{2}$$

读写器空闲概率＝空闲时间/(通信时间＋空闲时间)，因为通信时间长度的分布符合几何分布，所以平均通信时间为 $\overline{T}=\frac{\eta}{q}$，平均空闲时间为 $\overline{I}=\frac{\eta}{P_{SHR}}$，其中 P_{SHR} 为读写器成功传送 HR 的概率。可以得出

$$P_I=\frac{\overline{I}}{\overline{T}+\overline{I}}=\frac{q}{P_{SHR}+q} \tag{3}$$

读写器成功传送 HR 的条件是：(1)该读写器在同步期或者 CLR 期有数据到达，需要通信；(2)该读写器没有 HR 标志，即周围不存在通信且未结束的读写器；(3)该读写器的相邻读写器都未发送 RTS 或者说未发生 RTS 冲突。所以

$$P_{SHR}=P_A(1-P_{HR})(1-P_{RTS})^{N-1} \tag{4}$$

读写器有 HR 标志的概率为该读写器相邻的读写器至少有一个正在通信，并且未在本时隙内结束。所以

$$P_{HR}=\binom{N-1}{1}pP_TP_{CF/T} \tag{5}$$

式中，$P_{CF/T}$ 是读写器在与标签通信的条件下持续到本频点的条件概率。

设 $P(i)$ 是表明读写器从时隙 i 开始通信的概率。设 $P(T/i)$ 是表明读写器从时隙 i 开始一直持续到当前时隙的概率，因为通信时间的长度分布符合几何分布，所以 $P(T/i)=p^{i-1}$。

$$P_{CF/T}=\frac{\sum_{i=1}^{\infty}P(T/jM)P(jM)}{\sum_{i=1}^{\infty}P(T/i)P(i)}=\frac{p^{M-1}q}{1-p^M} \tag{6}$$

读写器发送 RTS 的概率 P_{RTS} 为读写器处于空闲状态时有数据到达并且没有 HR 标志的概率。

$$P_{RTS}=P_IP_A(1-P_{HR}) \tag{7}$$

将式(5)、式(6)、式(7)代入式(4)，可得到

$$\begin{aligned}P_{SHR}&=P_A(1-P_{HR})(1-P_{RTS})^{N-1}\\&=P_A(1-\binom{N-1}{1}pP_TP_{CF/T})(1-P_IP_A(1-P_{HR}))^{N-1}\end{aligned} \tag{8}$$

由式(3)可得

$$P_I=\frac{\overline{I}}{\overline{T}+\overline{I}}=\frac{q}{P_{SHR}+q}=f(P_I) \tag{9}$$

现在得到 P_I 的一个非线性方程。此方程可用 $P_{Inew}=P_{Iold}$ 迭代解出，最后得到

$$S=P_T=1-P_I \tag{10}$$

3 数据结果

系统中读写器负载表示为 $G=\lambda\eta$，设 $\gamma=0.02$，$c=2$。下面分析在给定负载 G 的情况下 FHR 协议系统输出 S 随其他参数变化的情况。

在 18 个频率对可用且每个读写器周围有 5 个相邻读写器的情况下($M=18$，$N=5$)，给定不同的读写器平均通信时间长度 d 时，系统输出 S 随读写器负载的变化情况如图 4 所示。由图 4 可以看出，随着读写器平均通信时间长度 d 的增长，系统输出 S 增长很快。这是因为读写器在成功预约了频率后可以保证无冲突通信，这样就减少了由冲突引起的系统开销，增加了信道利用率。

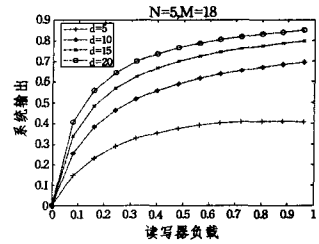

图 4 d 变化时 FHR 输出变化情况

在 18 个频率对可用并且读写器平均通信时间长度为 10 的情况下($M=18$，$d=10$)，给定不同邻居读写器数量 N 时，系统输出 S 随读写器负载的变化情况如图 5 所示。由图 5 可以看出，随着邻居读写器数量 N 的增长，系统输出 S 降低。这是因为读写器数量的增加导致预约时冲突随之增加，以及当一个读写器预约成功后相邻读写器暂时不能通信。

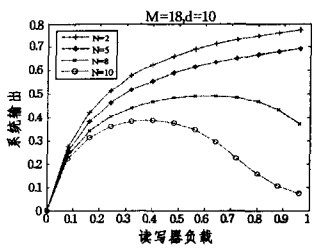

图 5 N 变化时 FHR 输出变化情况

在每个读写器周围有 5 个相邻读写器并且读写器平均通信时间长度为 10 的情况下($N=5$，$d=10$)，给定不同的 M 值时，系统输出 S 随读写器负载的变化情况如图 6 所示。由图 6 可以看出，随着读写器可用频率对 M 的增长，系统输出 S 增加，但是增加不明显。这是由于一个读写器预约成功后，相邻读写器暂时不能通信，因而不能充分利用频率资源。

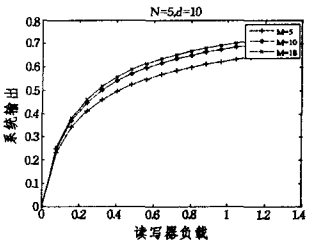

图 6 M 变化时 FHR 输出变化情况

在有 18 个频率对可用、每个读写器周围有 5 个相邻读写

器并且读写器平均通信时间长度为 10 的情况下($M=18$, $N=5$, $d=10$),在给定负载的基础上,FHR 协议系统输出 S 与 PULSE 算法和 Colorwave 算法的对比如图 7 所示。可以看出,开始三者的系统输出差不多,但是随着读写器负载的增大,FHR 协议的系统输出 S 要比 PULSE 算法和 Colorwave 算法高,这是因为 FHR 协议采用了多频率,避免了读写器冲突。

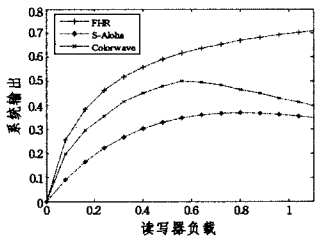

图 7　三种算法的对比

需要指出的是,在数据分析中假设读写器已经进入了同步状态,没考虑同步时间消耗,并且忽略了传输延迟和数据的处理时间,因此理论结果较理想。在实际中,性能会比此理论值低。

结束语　本文提出了一种基于跳频预约的 RFID 读写器网络 MAC 协议 FHR,并对此协议进行了分析。FHR 协议通过竞争预约时隙及对应的通信频率,并通知邻居读写器,避免了读写器-标签冲突;采用读写器和标签,并分别使用不同的频率通信机制及多频率跳频机制,避免了读写器频率冲突。对 FHR 协议进行的分析表明,此协议在读写器负载较大及读写器平均通信时间较长时,单位时间内读写器与标签通信成功概率高。FHR 协议不会产生读写器-标签冲突,并且频率利用率较高。

参 考 文 献

[1] 中华人民共和国科学技术部等. 中国射频识别(RFID)技术政策白皮书[OL]. http://www.rfidinfo.com.cn/,2006

[2] Engels D W, Sarma S E. The reader collision problem[C]// Proceedings of IEEE International Conference on Systems, Man and Cybernetics. Hammamet, Tunisia, October 2002:6-9

[3] Leong K S, Ng M L, Cole P H. The Reader Collision Problem in RFID Systems[C]// 2005 IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications Proceedings. Beijing, China, 2005: 658-661

[4] EPCGlobal. EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860MHz-960 MHz version 1.0.9 [OL]. http://www.epcglobalinc.org/Standards,2005

[5] RFID CHINA. 第二代 RFID 技术标签标准[J]. 中国防伪报道, 2006(5):39-44

[6] ETSI. ETSI EN 302 208-1 V1.1.1[OL]. http://www.esti.org,2004

[7] Waldrop J, Engels D W, Sarma S E. Colorwave: An Anti-collision Algorithm for the Reader Collision Problem [C]// IEEE Wireless Communications and Networking Conference (WCNC). New Orleans, Louisiana, USA, 2003:1701-1704

[8] Birari S M, Sridhar I. PULSE: A MAC Protocol for RFID Networks[C] //1st International Workshop on RFID and Ubiquitous Sensor Networks (USN). Nagasaki, Japan, 2005: 1036-1046

[9] Tang Z, Garcia-Luna-Aceves J J. Hop Reservation Multiple Access (HRMA) for Multichannel Packet Radio Networks[C]// Proc. IEEE IC3E'98, the Seventh International Conference on Computer Communications and Networks. Lafayette, Louisiana, US, 1998:388-395

[10] Tang Zhenyu, Garcia-Luna-Aceves J J. Hop Reservation Multiple Access (HRMA) for Ad-Hoc Net works[C]// Proc. of IEEE INFOCOM 1999, the Conference on Computer Communications, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. New York, USA, 1999: 194-201

(上接第 6 页)

[10] Yee B, Sehr D, Dardyk G, et al. Native Client: A Sandbox for Portable, Untrusted x86 Native Code[J]. Communications of the ACM, 2010, 53(1):91-99

[11] Douceur J R, Elson J, Howell J, et al. Leveraging Legacy Code to Deploy Desktop[C]// Applications on the Web. 8th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2008). USENIX Association, 2008

[12] Singaravelu L, Pu C, Härtig H, et al. Reducing TCB Complexity for Security-Sensitive Applications: Three Case Studies[C]// Proceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems (Eurosys 2006). Belgium, Apr. 2006

[13] Guttman J, Herzog A, Millen J, et al. Attestation: Evidence and Trust[R]. MTR080072. Mar. 2008

[14] Nibaldi G C. Specification of a Trusted Computing Base[R]. M79-228. MITRE Corporation, Bedford, MA, USA, 1979

[15] DoD 5200.28-STD, Department of Defense Standard. Department of Defense Trusted Computer System Evaluation Criteria [S]. National Computer Security Center, Ft. Meade, MD, USA, Dec. 1985

[16] Anderson J P. Computer Security Technology Planning Study Volume II[R]. ESD-TR-73-51. Vol. II, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA, USA, Oct. 1972

[17] Saltzer J H, Schroeder M D. The Protection of Information in Computer Systems[J]. Proceedings of the IEEE, 1975, 63(9): 1278-1308

[18] Seshadri A, Luk M, Qu N, et al. SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes[C]// The 21st ACM Symposium on Operating Systems Principles (SOSP 2007). Washington, USA, Oct. 2007:335-350

[19] McCune J M, Parno B, Perrig A, et al. Flicker: An Execution Infrastructure for TCB Minimization[C] // Proceedings of the ACM European Conference on Computer Systems (EuroSys). Glasgow, Scotland, Mar. -Apr. 2008

[20] Sharif M, Lee W, Cui Weidong, et al. Secure In-VM Monitoring Using Hardware Virtualization[C]// The 16th ACM Conference on Computer and Communications Security (CCS 2009). Chicago, IL, USA, Nov. 2009:477-487

[21] 石文昌, 梁朝晖. 信息系统安全概论[M]. 北京: 电子工业出版社, 2009:341-361