基于码分多址防碰撞的射频识别认证协议

王云峰* 张 斌 刘 洋 费晓飞
(解放军信息工程大学 郑州 450001)

摘 要：该文针对射频识别(RFID)领域中的安全认证协议和多标签防碰撞算法两个研究热点，设计了一种基于码分多址防碰撞算法的 RFID 安全认证协议。协议支持密钥的动态更新并引入标志位机制选择备用密钥来抵御数据库同步攻击，同时结合码分多址技术，应用重传随机数进行扩频码的选择，实现一次重传解决多标签识别中因数据碰撞造成的标签不识别的问题。首先，描述协议的流程及防碰撞原理；其次，应用 SVO 逻辑对认证协议的正确性进行证明；最后，对应用该认证协议的系统吞吐效率进行数值分析，分析表明其吞吐效率高于传统防碰撞算法。

关键词：射频识别；码分多址；认证协议；防碰撞
中图分类号：TN91 **文献标识码**：A **文章编号**：1009-5896(2014)06-1472-06
DOI: 10.3724/SP.J.1146.2013.01337

Radio Frequency Identification Authentication Protocol Based on CDMA Anti-collision Algorithm

Wang Yun-feng Zhang Bin Liu Yang Fei Xiao-fei
(*PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: For addressing the two focus issues under research , security authentication protocol and the multi-tag anti-collision algorithm in the field of Radio Frequency IDentification (RFID), a Code Division Multiple Access (CDMA)-based anti-collision algorithm of the RFID authentication protocol is presented in this paper. The authentication protocol supports dynamic updates of the key and resists database synchronization attacks by using flag mechanism to select spare key. Meanwhile, by combining with CDMA and by retransmitting random number to select spreading code, the authentication protocol solves recognition of tags due to data collisions during the multi-tag identification by one-time retransmission. Firstly, the process of the authentication protocol and an anti-collision theory is described. Secondly, the SVO logic is used to prove correctness of the protocol in theory. Finally, numerical analysis of the system throughput applying the protocol shows that its throughput efficiency is higher than the traditional one.

Key words: Radio Frequency Identification (RFID); Code Division Multiple Access (CDMA); Authentication protocol; Anti-collision

1 引言

射频识别 RFID(Radio Frequency Identify)技术是通过无线射频方式对目标进行自动识别的非接触双向数据通信技术。其特有的非接触式自动识别性能，使其被广泛应用到交通、物流供应链管理和零售行业等领域[1]。

RFID 系统中，由于无线信道的开放特性，导致标签与阅读器之间的信息传输易遭到窃听、干扰、欺骗和篡改。为解决 RFID 系统存在的安全问题，目前已提出多种认证协议，一般可分为两类：一类是静态机制认证协议，主要包括分布式 RFID 询问-响应协议[2]、轻量级同步认证协议[3]和基于 DES 加密的认证协议[4]等。该类协议能够抵御窃听、跟踪、重放和欺骗等常见攻击，但不能对密钥进行更新，使用该类协议的系统存在标签密钥泄露，进而导致系统内所有标签标识 ID 被攻击者窃取的安全隐患，同时计算复杂、成本较高。另一类是动态机制认证协议，包括 Hash 链协议[5]、基于杂凑 ID 变化协议[6]和基于流密码的协议[7]等，此类协议考虑对 ID 的保护，每次认证后都更新 ID，但存在标签与阅读器之间数据不同步的隐患。因此，设计支持不断更新密钥并能消除数据不同步隐患的认证协议已成为研究热点。

设计高效的防碰撞算法是多标签识别问题的另一热点。常用的防碰撞算法一般可分为两类：一类是基于时隙随机分配的 ALOHA 算法，包括帧时隙 ALOHA 算法[8]、分群时隙 ALOHA 算法[9]和分组动

2013-09-04 收到，2013-12-24 改回
*通信作者：王云峰 wangyunfengieu@126.com

态帧时隙算法[10]等。此类算法简单、便于实现、成本低，但系统吞吐量小，且存在标签无法被识别的情况。另一类是基于二进制树搜索的算法，主要包括自适应四叉树搜索算法[11]、自适应多叉树算法[12]和基于识别码分组的算法[13]等。该类算法能够识别读写器有效通信范围内所有标签，但计算复杂、延时较长。

文献[14]提出了一种基于码分多址技术的RFID防碰撞算法，算法可以同时识别系统中的多个标签，但未明确指出多标签碰撞情况下扩频码的选择方法，无法避免数据再次碰撞。结合文献[14]的设计思路，针对数据碰撞问题，本文提出一种基于码分多址防碰撞的 RFID 认证协议。该协议将静态和动态机制的优点相结合，支持密钥的动态更新并引入标志位机制选择备用密钥来抵御数据库同步攻击。同时，协议结合码分多址技术，应用重传随机数进行扩频码的选择，实现一次重传解决多标签识别中因数据碰撞造成的标签不识别的问题。

2　基于码分多址防碰撞 RFID 认证协议

基于码分多址防碰撞的 RFID 协议认证流程如图 1 所示，文中符号见表 1。

表 1 符号描述

符号	描述
ID	标签身份标识
K,K'	标签密钥 K 和备用密钥 K'
PRNG	随机数发生器
R_T	标签产生的随机数
R_R	阅读器产生的随机数
$R_R^{'}$	重传机制中阅读器产生的新随机数
Flag	1 bit 防数据同步攻击标志位
N	系统内置扩频码数量
M	扩频码
$\otimes$	扩频运算
H_K^L	密钥为 K 的 Hash 运算值的左半部
$H_{K'}^R$	密钥为 K'的 Hash 运算值的右半部

协议中阅读器存储着 ID, K 和 K'，标签存储着 ID, K, K', R_T和 Flag。

认证和密钥更新流程如下：

(1)阅读器向标签发送认证请求和 R_R;

(2)标签收到请求和 R_R，生成范围在 1 至 N之间的随机数 R_T 并将其储存，同时计算$(R_R+R_T)\ \mathrm{mod}N$的值 x，标签选择内置对应的第 x个 Gold 序列作为扩频码 M;

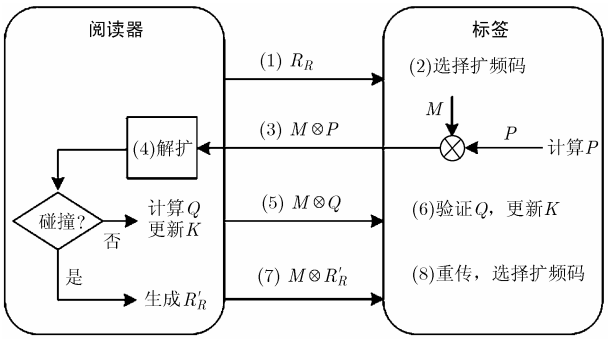

图 1 基于码分多址防碰撞的协议认证流程

(3)若 Flag=0，标签计算 $P=H_K^{\mathrm{L}}(\mathrm{ID}\,||\,R_R)$，将 P扩频发送给阅读器；若 Flag=1，计算 $P=H_{K'}^{\mathrm{L}}(\mathrm{ID}\,||\,R_R)$，将 P扩频发送给阅读器，Flag 置 0;

(4)阅读器收到扩频信息后，依次使用内置扩频码进行解扩。若在同一时刻或数据处理过程中，存在两个或以上数据应用同一扩频码进行解扩，则发生碰撞，转向流程(7)；否则继续执行；

(5)阅读器在数据库中查找满足 $H_K^{\mathrm{L}}(\mathrm{ID}\,||\,R_R)=P$ 的 ID 和密钥 K 的信息对，若存在对应信息对，则实现阅读器对标签的认证，将 $M\otimes Q$(其中$Q=H_K^R(\mathrm{ID}\,||\,R_R)$)发送给标签，同时更新 K 为 $K\oplus R_R$;

否则，进一步查找满足 $H_{K'}^{\mathrm{L}}(\mathrm{ID}\,||\,R_R)=P$ 的 ID 和密钥 K'的信息对，若存在对应信息对，则实现阅读器对标签的认证，将 $M\otimes Q$(其中$Q=H_{K'}^{\mathrm{R}}(\mathrm{ID}\,||\,R_R)$)发送给标签，同时更新 K 为 $K'\oplus R_R$;

若以上两种信息对都不存在，则认证失败，结束；

(6)标签收到扩频信息进行解扩得到 Q，验证对应的 $H_K^{\mathrm{R}}(\mathrm{ID}\,||\,R_R)$或 $H_{K'}^{\mathrm{L}}(\mathrm{ID}\,||\,R_R)$是否与 Q 相等。若相等，则实现标签对阅读器的认证，相应地更新 K 为 $K\oplus R_R$或 $K'\oplus R_R$；否则认证失败，结束；

(7)阅读器重新生成随机数 $R_R^{'}$发送给碰撞标签，通知重传；

(8)标签收到信息后解扩，计算$(R_R^{'}+R_T+\mathrm{ID})\ \mathrm{mod}N$的值 x，其中 R_T为流程(2)中的储存值。选择内置对应的第 x个 Gold 序列作为扩频码，解扩不会再发生碰撞，转向流程(3)。

3　安全性能分析

3.1 SVO逻辑分析证明

协议的分析证明采用形式化验证逻辑 SVO[15]，通过认证协议运行过程中消息的接收和发送，从初始假设逐渐推导出协议的目标。证明过程中，R 代表阅读器，T 代表标签，公理 A_1, A_2, A_3, A_4参见参考文献[15]中 SVO 逻辑推理规则。

RFID 双向认证协议流程分析如下：

(1)初始假设

P_1: $\mathrm{R}|\equiv \#R_R$, $\mathrm{T}|\equiv \#\mathrm{ID}$

P_2: $\mathrm{T}|\equiv \mathrm{T}\xleftrightarrow{K}\mathrm{R}$

(2)证明目 $\mathrm{R}|\equiv \mathrm{R}\xleftrightarrow{K}\mathrm{T}$ 标

G_1: $\mathrm{R}|\equiv (\mathrm{T}\ni K)$

G_2: $\mathrm{R}|\equiv (\mathrm{T}\ni \mathrm{ID})$

G_3: $\mathrm{T}|\equiv (\mathrm{R}\ni K)$

G_4: $\mathrm{T}|\equiv (\mathrm{R}\ni R_R)$

(3)消息接收

P_3: $\mathrm{T}\lhd R_R$

P_4: $\mathrm{R}\lhd \{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{L}}$

P_5: $\mathrm{T}\lhd \{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{R}}$

(4)主体对接收到消息的理解　由于阅读器在接收到消息前不知道标签对应的密钥和 ID，因此不知道接收的内容，故

P_6: $\mathrm{R}|\equiv \mathrm{R}\lhd *1$

P_7: $\mathrm{T}|\equiv \mathrm{T}\lhd \{*2\}_K$

(5)接收者对消息的解释

P_8: $\mathrm{R}|\equiv (\mathrm{R}\lhd *1\supset \mathrm{R}\lhd \{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{L}})$

P_9: $\mathrm{R}|\equiv (\mathrm{R}\lhd \{X^{\mathrm{T}}\}_K\wedge \mathrm{R}\xleftrightarrow{K}\mathrm{T}\supset \mathrm{T}|\sim X)$

P_{10}: $\mathrm{T}|\equiv (\mathrm{T}\lhd \{*2\}_K\supset \mathrm{T}\lhd \{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{R}})$

P_{11}: $\mathrm{T}|\equiv (\mathrm{T}\lhd \{X^{\mathrm{R}}\}_K\wedge \mathrm{R}\xleftrightarrow{K}\mathrm{T}\supset \mathrm{R}|\sim X)$

(6)使用 SVO 逻辑推导

NEC 规则：由 $|-\varphi$ 可以推导出 $|-P|\equiv\varphi$

MP 规则：φ 和 $\varphi\supset\psi$ 可以推导出 ψ

由 P_6, P_8 和信任公理 A_1: $P|\equiv\varphi\wedge P|\equiv(\varphi\supset\psi)\supset P|\equiv\psi$ 可得：

$\mathrm{R}|\equiv \mathrm{R}\lhd \{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{L}}$　(推论 a)

由 P_2, P_9，推论 a 和 A_1 可得：

$\mathrm{R}|\equiv \mathrm{T}|\sim\{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{L}}$　(推论 b)

$\mathrm{R}|\equiv (\mathrm{T}\ni K)$, G_1 得证。

由 P_1, A_1, 消息新鲜性公理 A_2: $\#(X_{\mathrm{i}})\supset\#(X_1\cdots X_n)$ 和 NEC 规则可得：

$\mathrm{R}|\equiv \#\{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{L}}$　(推论 c)

由推论 b，推论 c, NEC 规则和临时值验证公理 A_3: $(\#(X_{\mathrm{i}})\wedge P\,|\sim X)\supset P|\approx X$ 可得：

$\mathrm{R}|\equiv \mathrm{T}|\approx \{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{L}}$　(推论 d)

由推论 d 和消息发送公理 A_4: $P|\approx(X_1\cdots X_n)\supset P\,|\sim(X_1\cdots X_n)\wedge P\ni X_i$ 可得：

$\mathrm{R}|\equiv (\mathrm{T}\ni \mathrm{ID})$, G_2 得证。

由 P_7, P_{10}, A_1 可得：

$\mathrm{T}|\equiv \mathrm{T}\lhd \{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{R}}$　(推论 a′)

由 P_2, P_{11}，推论 a′和 A_1 可得：

$\mathrm{T}|\equiv \mathrm{R}|\sim\{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{R}}$　(推论 b′)

$\mathrm{T}|\equiv (\mathrm{R}\ni K)$, G_3 得证。

由 P_1, A_2, A_1 和 NEC 规则可得：

$\mathrm{T}|\equiv \#\{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{R}}$　(推论 c′)

由推论 b′，推论 c′, A_3, A_1 和 NEC 规则可得：

$\mathrm{T}|\equiv \mathrm{R}|\approx \{\mathrm{ID}\,||\,R_R\}_K^{\mathrm{R}}$　(推论 d′)

由推论 d′和 A_4 可得：$\mathrm{T}|\equiv (\mathrm{R}\ni R_R)$, G_4 得证。

3.2 抗攻击分析

(1)防窃听和跟踪攻击：单向 Hash 函数的加密，使攻击者无法还原标签与阅读器间信息明文，因此协议可抵御窃听攻击。同时，标签在每次通信中传递的信息不固定，所以不能实现对标签的跟踪。

(2)防重放和欺骗攻击：由于阅读器每次通信时都产生随机数，攻击者无法预知和控制，所以记录并重放泄漏的消息，伪装成合法用户的方法对系统无效，数据库不会给予认证。

(3)防数据库同步攻击：为解决数据库和标签的数据同步问题，协议提出了一种基于标志位 Flag 选择密钥 K 或备用密钥 K'的认证机制。协议初始，标签检查 Flag 标志位。若 Flag=1，表明前一轮协议认证中阅读器与标签之间实现了合法认证；若 Flag=0，说明系统受到攻击导致数据不同步，系统将自动采用备用密钥 K'进行加密。这样，协议不仅实现了对标识 ID 的保护，同时解决了不断更新加密密钥带来的数据库不同步的安全问题。

(4)防内部篡改：内部篡改是指合法标签有意地篡改自身 ID 值，伪装成其它合法标签，骗取阅读器的认证。但由于每个标签的认证密钥独立且不断更新，伪装的标签无法产生与阅读器对应的合法信息，不能通过认证。同时，即使攻击者获得加密算法的硬件结构和标签数据信息，可无法掌握密钥的更新，同样无法通过阅读器的认证。

(5)ID 的保护与相互认证：不固定的密文传输及密钥的实时更新等诸多保护措施，实现了对标签 ID 的保护。同时，阅读器和标签之间的双向认证使得系统安全性更加可靠。

(6)重传机制：当多个标签同时认证发生碰撞时，通过信息的重传机制有效地解决了扩频码的选择难题。在扩频码选择过程中，为满足安全要求，防止标签被追踪，由标签随机生成选择因子 R_T 参与扩频码的选择。当有两个以上标签生成的 R_T 相同时，解扩过程发生碰撞，启动重传机制。标签计算 $(R_R^{'}+R_T+\mathrm{ID})\mathrm{mod}N$，因碰撞标签的 $R_R^{'}$ 和 R_T 都相同，此时引入 ID 作为选择因子，实现不同扩频码的选择，解决碰撞。若取消重传机制，认证初始即计算 $(R_R+R_T+\mathrm{ID})\mathrm{mod}N$ 选择扩频码，解扩过程还是会发生碰撞，因此重传机制的存在是必要的。

协议安全性对比如表 2(其中，×代表无法防御，○代表有效防御)。

表 2 协议安全性对比

协议名称	窃听	跟踪	重放	欺骗	ID 保护	数据同步	内部篡改	认证方式
Hash-lock	×	×	×	×	×	○	×	单向
随机 Hash-lock	×	○	×	×	×	○	×	单向
基于 Hash 的 ID 变化	○	○	○	×	○	×	×	双向
LCAP	○	○	○	○	○	×	×	双向
分布询问应答	○	○	○	○	○	○	×	双向
本文协议	○	○	○	○	○	○	○	双向

协议计算量对比如表 3(其中，N_H表示 Hash 函数次数，N_R表示产生随机数次数，n 表示系统中标签的数量)。

与其它协议相比，标签和阅读器的计算量没有增加，且查找过程是在计算能力强的数据库进行，因此协议在保证安全性的同时，未给系统带来多余计算负荷。

表 3 协议计算量对比

协议	标签		阅读器		数据库	
	N_H	N_R	N_H	N_R	N_H	N_R
Hash-lock	1	0	0	0	0	0
随机 Hash-lock	1	1	$(n+1)/2$	0	1	0
基于Hash的ID变化	3	0	0	0	3	1
LCAP	2	0	0	1	1	0
分布询问应答	2	1	0	1	$(n+3)/2$	0
本文协议	1	1	0	1	$(n+1)/2$	0

4　防碰撞性能分析

4.1 认证协议防碰撞原理

本文认证协议基于码分多址技术，在待识别的标签数量较多时，有效地增加系统吞吐量，减少识别时间，提高搜索效率，其原理如图 2 所示。某时刻有 K 个标签同时向阅读器发送数据，系统随机分配 K 个扩频码(M_1～M_K)供碰撞数据使用，阅读器端采用同样的扩频码对信息解扩，以恢复标签数据。当有两个或以上标签选择的扩频码相同时，标签数据发生碰撞，此时启动重传机制，标签重新选择扩频码实现其数据的识别。协议中重传机制的数据帧与确认帧发送时间关系如图 3 所示，其中阅读器和标签封装的帧格式如图 4，图 5 所示。

反向链路，即标签响应阅读器的命令并向其发送数据的链路。t_T是标签数据帧的发送时间，由图 4 可知其帧长 L=112 bit，在中高频系统中，上行速率通常为 C=40 kbit/s[16]，因此数据帧发送时间 t_T=L/C=0.0028 s，同理 t_R=0.0028 s。数据帧沿反向链路传到阅读器还要经历物理链路造成的传播时延 t_P，同时阅读器收到数据帧要经历处理时间 t_{Pr}。阅读器接着发送前向链路的确认帧，其发送时间为 t_R，传播时延为 t_P，标签收到确认帧需要时间 t_{Pr}进行处理，再重新发送数据帧。为方便问题研究，设标签与阅读器的处理时间 t_{Pr} 远小于数据帧发送时

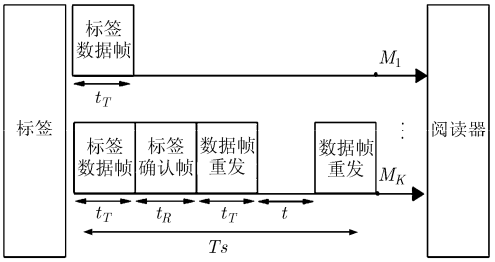

图 2 协议的多标签识别原理

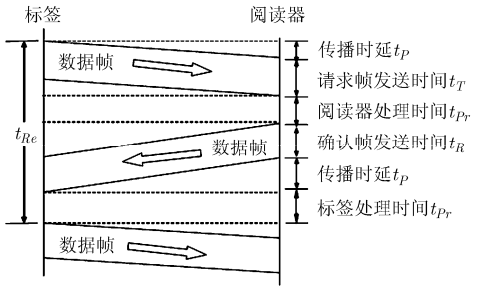

图 3 协议中数据帧与确认帧发送时间关系

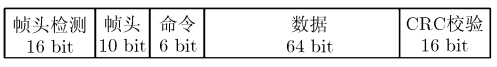

图 4 标签数据帧格式(前向链路)

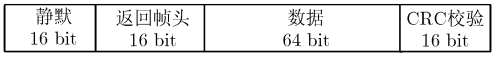

图 5 阅读器确认帧格式(反向链路)

间，且由于标签与阅读器间作用距离短，传播时延 t_P 为 0，因此一次重传时间可视为 $t_T+t_R+t_T$。

进一步理解通信过程，当系统中有足够多的标签，可以把标签数据帧的到达看成泊松分布。Ts 为单个标签完成将其数据帧完整地发送给读写器所需的时间，定义系统负载 G 为 Ts 时长内读写器识别范围到达数据帧的平均数目。则 Ts 时长到达 K 个标签数据帧的概率为 $Q(K)=(G^K e^{-G})/K!$，且某一数据帧从系统内置的 N 个扩频码中随机选择扩频码 M_K 进行扩频，并在阅读器端成功解扩的概率为 $(1-1/N)^{K-1}$。若解扩过程发生碰撞，则对数据帧进行重传。

按照负载 G 和扩频码数量 N 大小关系，数据帧的重传分两种情况。当 $G<N$ 时，一次重传后解扩不会再发生碰撞，因此重传成功的概率为 $S(K)=(1-1/N)^{K-1}+[1-(1-1/N)^{K-1}]\cdot 1$；当 $G>N$ 时，一次重传后仍会发生数据碰撞，此时采用时隙 ALOHA 算法中的随机退避机制[8]，每个数据帧各自随机延时一段时间后再发送，利用各数据帧的随机退避时间的不同来降低再次碰撞的概率。随机退避机制下数据帧的重传是一个排队过程。依据排队论原理，重传数据帧需排队的时延 t 服从指数分布，概率密度为 $f(t)=Ge^{-Gt}$，其排队时延 t 应不少于一帧的发送时间 T，即 $F(T)=F(t\geq T)=\int_T^\infty Ge^{-Gt}\mathrm{d}t=e^{-GT}$。因此，数据帧经历多次重传成功被阅读器识别的概率为 $R(K)=(1-1/N)^{K-1}+[1-(1-1/N)^{K-1}]\cdot e^{-GT}$。综上，$K$ 个标签被成功识别的概率为

$$P(K)=Q(K)\cdot S(K)\frac{G^K e^{-G}}{K!}\cdot\left(\left(1-\frac{1}{N}\right)^{K-1}+\left[1-\left(1-\frac{1}{N}\right)^{K-1}\right]\cdot 1\right),\quad G<N$$

$$P(K)=Q(K)\cdot R(K)\frac{G^K e^{-G}}{K!}\cdot\left(\left(1-\frac{1}{N}\right)^{K-1}+\left[1-\left(1-\frac{1}{N}\right)^{K-1}\right]\cdot e^{-GT}\right),\quad G>N$$

定义系统的吞吐量 S 为时间 Ts 内能成功解扩的标签数据帧的均值，则其可以表示为

$$S=\sum_{K=1}^{\infty}K\cdot P(K)=\sum_{K=1}^{\infty}K\frac{G^K e^{-G}}{K!}\left(\left(1-\frac{1}{N}\right)^{K-1}+\left[1-\left(1-\frac{1}{N}\right)^{K-1}\right]\cdot 1\right)=G,\quad G<N$$

$$S=\sum_{K=1}^{\infty}K\cdot P(K)=\sum_{K=1}^{\infty}K\frac{G^K e^{-G}}{K!}\left(\left(1-\frac{1}{N}\right)^{K-1}+\left[1-\left(1-\frac{1}{N}\right)^{K-1}\right]\cdot e^{-GT}\right)=Ge^{-\frac{G}{N}}+Ge^{-GT}-Ge^{-G\left(\frac{1}{N}+T\right)},\ G>N$$

4.2 认证协议吞吐量分析

由吞吐量公式可知，由于发送时间 $T\neq 0$，因此吞吐效率函数在 $G=N$ 处并不连续，当 $G<N$ 时，$S=G$，吞吐效率为直线 $\eta=1$；当 $G>N$ 时，吞吐效率为下降曲线，取帧发送时间 $T=t_T=0.0028$ s，系统吞吐量与负载和扩频码数量的关系如图 6 所示。

其吞吐效率 $\eta=\dfrac{S}{G}=e^{-\frac{G}{N}}+e^{-GT}-e^{-G\left(\frac{1}{N}+T\right)}$，仿真结果如图 7 所示。

由图 6 可知，当扩频码数量 N 一定时，系统吞吐量 S 会随着负载 G 的增加而先增大达到峰值再逐渐减小。同时负载 G 一定时，吞吐量 S 会随着扩频码数量 N 的增加而逐渐增大；图 7 吞吐效率 η 随着 G 的增加而逐渐减小，随着 N 的增加而逐渐增大，且 $\eta=e^{-\frac{G}{N}}+e^{-GT}-e^{-G\left(\frac{1}{N}+T\right)}>e^{-\frac{G}{N}}\geq e^{-G}$，因此系统吞吐效率高于时隙 ALOHA 吞吐效率。协议算法与传统算法吞吐效率对比如图 8 所示，其中 $N=100$，$T=0.0028$ s。由图可知，本文算法吞吐效率曲线并不连续，当 $G<100$ 时，吞吐效率 $\eta=1.0$，明显高于传统算法；$G>100$ 时，吞吐效率为下降曲线，但仍高于传统算法。

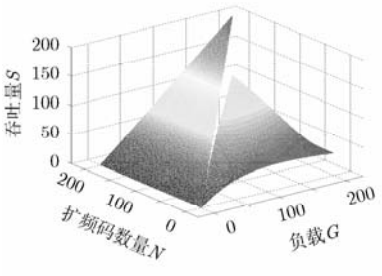

图 6 系统吞吐量与负载和扩频码数量的关系

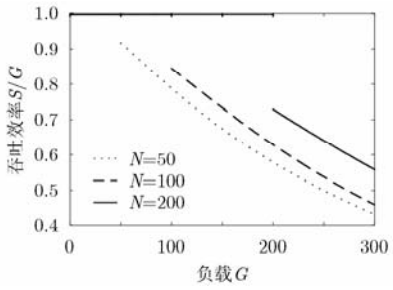

图 7 吞吐效率与负载和扩频码数量的关系

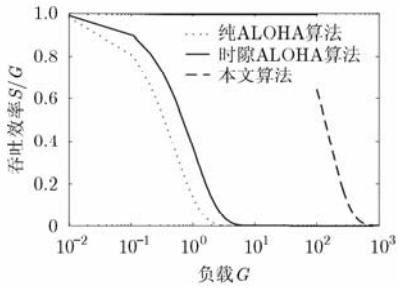

图 8 本文协议算法与传统算法吞吐效率对比图

5　结束语

本文针对 RFID 领域中的安全认证协议和多标签防碰撞算法两个研究热点，设计了一种基于码分多址防碰撞算法带有重传机制的 RFID 安全认证协议。文中利用 SVO 逻辑对该协议进行形式化分析，在理论上证明其正确性与安全性，并在此基础上分析了协议对各种攻击的有效抵御。在防碰撞算法的分析中，分析了防碰撞算法中扩频码数量和标签数量对吞吐量的影响，并应用 Matlab 实现算法仿真。仿真结果证实了算法的正确性，其吞吐量高于传统防碰撞算法。

参 考 文 献

[1] 谢磊, 殷亚凤, 陈曦. RFID 数据管理: 算法、协议与性能评测[J]. 计算机学报, 2013, 36(3): 457–470.
Xie Lei, Yin Ya-feng, and Chen Xi. RFID data management: algorithms, protocols and performance evaluation[J]. *Chinese Journal of Computers*, 2013, 36(3): 457–470.

[2] Rhee K, Kwak J, Kim S, *et al*.. Challenge-response based RFID authentication protocol for distributed database environment[C]. Proceedings of International Conference on Security in Pervasive Computing, Boppard, Germany, 2005(3450): 70–84.

[3] Ha J C, Ha J H, Moon S J, *et al*.. LRMAP: lightweight and re-synchronous mutual authentication protocol for RFID system[C]. Proceedings of the International Conference on Ubiquitous Convergence Technology, Berlin, Germany, 2007: 80–89.

[4] Wang Z, Xin W, Xu Z, *et al*.. A secure RFID communication protocol based on simplified DES[C]. Proceedings of the 2012 International Conference on Information Technology and Software Engineering, Berlin, Germany, 2013: 351–357.

[5] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Hash-chain based forward-secure privacy protection scheme for low cost RFID[C]. Proceedings of the 2004 Symposium on Cryptography and Information Security (SCIS 2004), Sendai, Japan, 2004: 719–724.

[6] Henrici D and Muller P. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers[C]. Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops, Washington, USA, 2004: 149–153.

[7] 龚洁中, 陈恭亮, 李林森, 等. 基于流密码的 RFID 安全认证协议[J]. 计算机工程, 2013, 38(13): 126–129.
Gong Jie-zhong, Chen Gong-liang, Li Lin-sen, *et al*.. RFID secure authentication protocol based on stream cipher[J]. *Computer Engineering*, 2013, 38(13): 126–129.

[8] Finkenzeller K. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification[M]. New York: John Wiley & Sons, 2003: 151–158.

[9] Hwang Tae-wook, Lee Byong-gyo, and Kim Young-Soo. Improved anti-collision scheme for high speed identification in RFID system[C]. First International Conference on Innovative Computing, Information and Control, Beijing, China, 2006, 2: 449–452.

[10] 庞宇, 彭琦, 林金朝, 等. 基于分组动态帧时隙的射频识别防碰撞算法[J]. 物理学报, 2013, 62(14): 148401-1–148401-8.
Pang Yu, Peng Qi, Lin Jin-chao, *et al*.. Reducing tag collision in radio frequency identification systems by using a grouped dynamic frame slotted ALOHA algorithm[J]. *Acta Physica Sinica*, 2013, 62(14): 148401-1–148401-8.

[11] Shih B Y, Lo T W, Chen C Y. The research of quadtree search algorithms for anti-collision in radio frequency identification systems[J]. *Scientific Research and Essays*, 2011, 6(25): 5342–5350.

[12] 张学军, 蔡文琦, 王锁萍. 改进型自适应多叉树防碰撞算法研究[J]. 电子学报, 2012, 40(1): 193–198.
Zhang Xue-jun, Cai Wen-qi, and Wang Suo-ping. One anti-collision algorithm based on improved adaptive multi-tree search[J]. *Acta Electronica Sinica*, 2012, 40(1): 193–198.

[13] 张学军, 王娟, 王锁萍. 基于标签识别码分组的连续识别防碰撞算法研究[J]. 电子与信息学报, 2011, 33(5): 1159–1165.
Zhang Xue-jun, Wang Juan, and Wang Suo-ping. An uninterrupted anti-collision algorithm with ID-based grouping for RFID system[J]. *Journal of Electronics & Information Technology*, 2011, 33(5): 1159–1165.

[14] 梁彪, 胡爱群, 秦中元. 一种新的 RFID 防碰撞算法设计[J]. 电子与信息学报, 2007, 29(9): 2158–2160.
Liang Biao, Hu Ai-qun, and Qin Zhong-yuan. A novel design for RFID anti-collision technique[J]. *Journal of Electronics & Information Technology*, 2007, 29(9): 2158–2160.

[15] Syverson P F, and Cervesato I. The logic of authentication protocols[J]. *LNCS*, 2001, 2171: 63–137.

[16] 周晓光, 王晓华. 射频识别(RFID)技术原理与应用实例[M]. 北京: 人民邮电出版社, 2006: 113–114.
Zhou Xiao-guang and Wang Xiao-hua. Radio Frequency Identification (RFID) Technology Theory and Practical Examples[M]. Beijing: Posts & Telecommunications Press, 2006: 113–114.

王云峰：　男，1990 年生，硕士生，研究方向为安全认证协议.

张　斌：　男，1969 年生，教授，硕士生导师，研究方向为网络信息安全.

刘　洋：　男，1980 年生，博士生，研究方向为 SOA 安全、无线通信安全.