第 35 卷 第 2 期 计 算 机 工 程 2009 年 1 月
Vol.35 No.2 Computer Engineering January 2009
·安全技术· 文章编号：1000—3428(2009)02—0159—03 文献标识码：A 中图分类号：TP393

基于离散 ID 序列的 RFID 标签认证协议

刘志亮[1]，薛小平[1,2]，王小平[1]
(1. 同济大学电子与信息工程学院，上海 200092；2. 北京交通大学电子信息工程学院，北京 100044)

摘 要：针对 RFID 的安全问题，提出一种基于离散 ID 序列的 RFID 标签认证协议——DSTAP，在此基础上，将 DSTAP 协议与其他认证协议进行比较分析，采用 BAN 逻辑对所提出的协议进行形式化分析。分析结果表明，DSTAP 协议达到指定的安全设计要求，同时可减少计算量。

关键词：无线射频识别技术；认证；逻辑运算；形式化分析

Tag Authentication Protocol for RFID Based on Discrete Sequence of ID

LIU Zhi-liang[1], XUE Xiao-ping[1,2], WANG Xiao-ping[1]
(1. College of Electronics and Information Engineering, Tongji University, Shanghai 200092;
2. School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044)

【Abstract】 Aiming at security and privacy of Radio Frequency Identification(RFID), a discrete sequence of tag ID-based authentication protocol for RFID-DSTAP is proposed. This paper uses it to compare with other authentication protocols and analyzes it with BAN logic. Result of analysis shows that DSTAP meets the specified safety design requirements and the calculation is greatly reduced.

【Key words】 Radio Frequency Identification(RFID); authentication; logical operation; formal analysis

1 概述

无线射频识别技术(Radio Frequency Identification, RFID)在存货管理、物流系统等领域得到广泛应用。但由于 RFID 阅读器与标签之间采用无线通信技术，攻击者可采用窃听、重放、标签或阅读器的假冒、篡改数据和拒绝服务(DoS)等非法手段来攻击 RFID 系统，非法获知标签信息并对带有标签的对象进行秘密跟踪，这对持有标签的对象存在严重的安全威胁。对此，研究人员已提出多种有效的标签认证协议，包括基于 *Hash* 函数的认证协议和基于异或运算的认证协议。

标签认证协议通常基于 *Hash* 函数对标签进行认证，通过 *Hash* 函数，增加闭锁和开锁状态，从而使标签和阅读器之间可进行安全通信。研究人员提出多种基于 *Hash* 函数的标签认证协议，如固定读取控制 *Hash* 锁协议、随机读取控制 *Hash* 锁协议和 *Hash* 链协议等。但该认证协议仍存在许多安全隐患与缺陷，如固定读取控制 *Hash* 锁协议缺乏随机性，标签容易受到攻击者的跟踪、哄骗和重放攻击，*Hash* 链计算复杂、不易实现等。

基于异或运算的认证协议通过寻找比 *Hash* 函数更简单的加密算法，使 RFID 标签认证协议更简单可靠。文献[1]和文献[2]基于异或运算，分别提出 AINSP 标签认证协议(An Improved Approach to Security and Privacy of RFID Application System)和基于异或运算的随机数移位标签认证协议(XOR with Random Number Shift, XRNS)；文献[3]在基于异或运算的基础上，提出基于连续 ID 序列思想的标签认证协议——SPAP 标签认证协议(Security and Privacy on Authentication for Low-cost RFID)，利用随机数对标签 ID 进行连续的序列截取(分别从标签 ID 的始端与末端开始截取)，并将截得的 ID 序列进行异或运算，从而达到增加认证过程中的新鲜性和消除明文的目的。

上述协议都放弃使用 *Hash* 运算，采用异或运算，其目的是降低标签的计算量，从而降低标签的制造成本。但由于认证过程中存在明文传输、复杂的密钥更新程序或需要有可读写的存储器等，这都会增加标签的成本和安全风险。

针对上述标签认证协议的不足，本文提出基于离散 ID 序列思想的 RFID 标签认证协议——DSTAP。

2 DSTAP 协议

2.1 主要思想

DSTAP协议的主要思想是将标签ID与等长的随机数进行“逻辑与”运算，获得离散ID序列，以达到加大敌对破译标签ID难度的目的，并在认证过程中采用临时服务器[4]的解决方案(当阅读器需要识读标签时，阅读器可从数据库中下载带有要识读的所有标签信息的数据文件，以临时脱离中央数据库的束缚。这样可在没有RFID中央数据库链接的偏远地区也正常使用RFID系统，并避免敌对者对中央数据库的DoS攻击)。

假设协议中的基本密码构造如 *Hash* 函数等都是安全的，DSTAP 协议的认证过程如图 1 所示，其中，“AND”表示逻辑与，“XOR”表示异或。

阅读器在进行标签识读之前，须在认证管理中心的数据

作者简介：刘志亮(1980－)，男，硕士研究生，主研方向：计算机网络安全，通信与信息系统；薛小平，副教授、博士研究生；王小平，教授、博士

收稿日期：2008-02-21 **E-mail：**liuzhiliang@gmail.com

库中下载数据库文件，其中包括阅读器须识读的所有标签的ID信息,并且在标签中,须事先存入其 *TagID* 和 *Hash*(*TagID*)用来进行标签的身份识别。

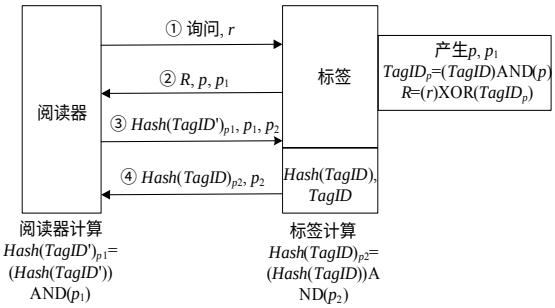

图 1　DSTAP 认证过程

认证步骤如下：

(1)阅读器产生随机数 r，然后发出询问，并将随机数 r 一同发送给标签。

(2)标签也产生随机数p和p_1。 p是一个与*TagID*一样长的随机数，p_1是同*Hash*函数一样长的随机数，然后，将p与*TagID*进行AND运算，得到$TagID_p$=(*TagID*)AND(p)，从而得到一个随机的离散*TagID*序列。为增加消息的新鲜性，再将其与随机数r进行异或运算，得到结果R，将R, p, p_1发送给阅读器。

(3)阅读器接收到后，进行反运算得到$TagID_p$，通过查找存储在自己存储器中的数据库文件，找到所有自身被授权可识读标签的$TagID_i$，i为标签标号。依次进行相同的运算得到$TagID_{ip}$=($TagID_i$)AND(p)，并判断$TagID_{ip}$是否与$TagID_p$相同，这是为了更容易地找到目标$TagID_i$。如果有，则将此$TagID_i$记为 *TagID*’，认证继续，计算 *Hash*(*TagID*’) 和 *Hash*(*TagID*’)$_{p1}$=(*Hash*(*TagID*’))AND(p_1)，阅读器再产生一个与*Hash*函数等长的随机数p_2，将*Hash*(*TagID*’)$_{p1}$, p_1, p_2发给标签；如果没有，则认证终止。

(4)标签接收到信息后，将*Hash*(*TagID*)与p_1进行计算，得到*Hash*(*TagID*)$_{p1}$=*Hash*(*TagID*)ANDp_1，比较*Hash*(*TagID*)$_{p1}$与*Hash*(*TagID*’)$_{p1}$是否相同，如相同则继续认证，计算Hash(*TagID*)$_{p2}$=(*Hash*(*TagID*))AND(p_2)，将*Hash*(*TagID*)$_{p2}$，p_2发送给阅读器；如不相同则终止认证。

(5)阅读器接收到信息后，将*Hash*(*TagID*’)和p_2进行计算，得到*Hash*(*TagID*’)$_{p2}$=*Hash*(*TagID*’)ANDp_2，比较*Hash*(*TagID*’)$_{p2}$与*Hash*(*TagID*)$_{p2}$，如相同则通过认证，否则终止认证。

2.2　协议讨论

在协议中，标签将$TagID_p$发给阅读器，是为了使让阅读器能尽快找到相对应的*TagID*’。由于*Hash*值是定长的，并且标签的数量可能很大,因此可能出现不同的*TagID*拥有相同的*Hash*(*TagID*)。如遇到这种情况，可根据不同的标签标准，如EPC标签标准来选择或是制定不同的*Hash*函数以避免出现相同*Hash*(*TagID*)的情况。本文中暂不考虑有*Hash*(*TagID*)相同的情况；在比较$TagID_{ip}$和$TagID_p$是否相同时，可能出现多个$TagID_i$相符合的情况，此时则须依次进行多轮询问　认证。

考虑到标签到阅读器的通信距离很短，敌对者并不容易窃听到信息，因此，在认证步骤(3)中，阅读器产生的随机数p_2可以是比特位全 1 的数，这样在步骤(4)中，标签会将整个*Hash*(*TagID*)传给阅读器，阅读器对其进行精确匹配认证，就不会存在误读标签的情况。即使被窃听到*Hash*(*TagID*)，敌对者也无法破译*TagID*。

3　性能与安全协议分析

3.1　各协议特性比较

本文对已有的一些算法：固定 Hash 锁，随机 Hash 锁，Hash 链，SPAP, XRAS, AINSP 和 DSTAP，分别针对计算量，存储器容量，是否需要可读写存储器，是否需要共享密钥，是否存在明文或固定信息特征这 5 个关于安全性和标签成本的特性进行比较，如表 1 所示。其中，标签长度为 L，*Hash* 长度为 L。

表 1　各安全协议性能分析

	计算量	存储器容量	可读写存储器	基于共享密钥	明文或固定信息特征
固定 Hash 锁	1×Hash	2L	有	是	有
随机 Hash 锁	1×Hash	L	无	否	有
Hash 链	2×Hash	2L	有	是	无
SPAP[	4×XOR	L	无	否	有
XRAS[	1×XOR+ 1×移位	2L	有	是	无
AINSP[1]	1×XOR+ 1×加密	2L	有	是	无
DSTAP	2AND+ 1×XOR	2L	无	否	无

通过对比可见，在满足 RFID 安全需求的条件下，DSTAP 计算量最小，可降低标签的成本；并且 DSTAP 无需可读存储器、没有采用共享密钥、没有明文或固定信息特征，这些都起到了降低标签成本并增强标签安全性能的作用。

3.2　基于 BAN 的安全协议分析

BAN (Burrows, Abadi, Needham)是一种基于信念的模态逻辑[5]，在BAN逻辑的推理过程中，参加协议的主体的信念随着消息交换的发展而不断变化和发展。本文采用BAN逻辑对协议进行形式化的分析[6]，以证明其可达到协议的设计要求。

定义 1 标签认证协议安全性要求

Tag $|\equiv$ {if *Hash*(*TagID*)$_{p1}$=*Hash*(*TagID*’)$_{p1}$ then *Tag*$|\equiv$*Hash*(*TagID*’)$_{p1}$}

Reader $|\equiv$ {if *Hash*(*TagID*’)$_{p2}$=*Hash*(*TagID*)$_{p2}$ then *Reader*$|\equiv$*Hash*(*TagID*)$_{p2}$}

如果标签接收到阅读器发给它的离散 *HashID* 序列(是标签随机指定的)与自己的离散 *HashID* 序列相同，那么标签相信阅读器拥有和自己相同的离散 *HashID* 序列。同样，如果阅读器接收到标签发给它的离散 *HashID* 序列(是阅读器随机指定的)与自己的离散 *HashID* 序列相同，那么阅读器相信标签拥有和自己相同的离散 *HashID* 序列。

原始协议的初始假设集合如下：

Y_1 *Tag*$|\equiv\#(p_1)$

Y_2 *Reader*$|\equiv\#(p_2)$

Y_3 *Reader*$|\equiv$*Tag*$|\rightarrow$*Hash*(*TagID*)$_{p2}$

Y_4 *Tag*$|\equiv$*Reader*$|\rightarrow$*Hash*(*TagID*’)$_{p1}$

Y_5 *Reader*$|\equiv$*Tag*$|\sim\{$*Hash*(*TagID*)$_{p2}$,$p_2\}$

Y_6 *Tag*$|\equiv$*Reader*$|\sim\{$*Hash*(*TagID*’)$_{p1}$,p_1,$p_2\}$

其中，Y_1为标签相信随机值p_1是新鲜的；Y_2为阅读器相信随机值p_2是新鲜的；Y_3为阅读器相信标签对*Hash*(*TagID*)$_{p2}$有管辖权；Y_4为标签相信阅读器对*Hash*(*TagID*’)$_{p1}$有管辖权；Y_5为阅读器相信标签曾经发送过*Hash*(*TagID*)$_{p2}$, p_2；Y_6为标签相信阅读器曾经发送过*Hash*(*TagID*’)$_{p1}$, p_1, p_2。

由于协议未采用基于共享密钥的体制，因此假设Y_5和Y_6是协议须付出的必要代价。

定义 2 理想 RFID 认证协议模型

M_0: $Reader \rightarrow Tag$: $\{Query, r\}$

M_1: $Reader \leftarrow Tag$: $\{\{TagID\}_{r,p}, p, p_1\}$

M_2: $Reader \rightarrow Tag$: $\{Hash(TagID')_{p1}, p_1, p_2\}$

M_3: $Reader \leftarrow Tag$: $\{Hash(TagID)_{p2}, p_2\}$

根据具体认证协议得到认证协议的BAN模型。M_0为阅读器向标签发出$Query, r$；M_1为标签向阅读器发出$\{TagID\}_{r,p}, p, p_1$；M_2为阅读器向标签发出$Hash(TagID')_{p1}, p_1, p_2$；$M_3$为标签向阅读器发出$Hash(TagID)_{p2}, p_2$。

形式化分析从理想化模型中$Reader$接收到Tag的M_1开始，得到$Reader \lhd \{\{TagID\}_{r,p}, p, p_1\}$，然后$Reader$在数据库文件中寻找$TagID_i$，并计算$\{TagID_i\}_{r,p}$，将$\{TagID\}_{r,p}$与$\{TagID_i\}_{r,p}$进行比较，如相同，则进行下一步认证，此时，把$ID_i$记为$ID'$，否则认证终止。

Tag接收到$Reader$的M_2，得到

$$Tag \lhd \{Hash(TagID')_{p1}, p_1, p_2\} \tag{1}$$

Tag用$Hash(TagID)_{p1}$与$Hash(TagID')_{p1}$进行比较，如果$Hash(TagID)_{p1}= Hash(TagID')_{p1}$，将进行下一步认证，根据初始假设$Y_1$和式(1)，运用BAN消息新鲜性原则，得到

$$Tag \mid\equiv \#(Hash(TagID')_{p1}, p_1, p_2) \tag{2}$$

根据Y_6和式(2)，运用BAN临时值验证规则，得到

$$Tag \mid\equiv Reader \mid\equiv \{(Hash(TagID')_{p1}, p_1, p_2)\} \tag{3}$$

对式(3)，运用 BAN 信念规则，得到

$$Tag \mid\equiv Reader \mid\equiv \{Hash(TagID')_{p1}\} \tag{4}$$

根据Y_4和式(4)，运用BAN管辖原则，得到

$$Tag \mid\equiv \{Hash(TagID')_{p1}\}$$

否则M_2无效，认证终止。

$Reader$接收到Tag的M_3，得到

$$Reader \lhd \{Hash(TagID)_{p2}, p_2\} \tag{5}$$

$Reader$用$Hash(TagID')_{p2}$与$Hash(TagID)_{p2}$进行比较，如果$Hash(TagID')_{p2}=Hash(TagID)_{p2}$，则根据$Y_2$和式(5)，运用BAN消息新鲜性原则，得到

$$Reader \mid\equiv \#(Hash(TagID)_{p2}, p_2) \tag{6}$$

根据Y_5和式(6)，运用BAN临时值验证规则，得到

$$Reader \mid\equiv Tag \mid\equiv \{Hash(TagID)_{p2}, p_2\} \tag{7}$$

对式(7)运用 BAN 信念规则，得到

$$Reader \mid\equiv Tag \mid\equiv \{Hash(TagID)_{p2}\} \tag{8}$$

根据Y_5和式(8)，运用BAN管辖原则，得到

$$Reader \mid\equiv \{Hash(TagID)_{p2}\}$$

根据协议模型和初始假设推理可知，标签相信阅读器拥有与自己相同的离散 *HashID* 序列，阅读器相信标签拥有与自己相同的离散 *HashID* 序列。

4 结束语

RFID 已在很多领域如零售、物流等展示出其强大的优越性，但安全和隐私问题一直是困扰其大规模应用的主要问题之一。研究人员就此提出了多种有效的标签认证协议，也取得了一定效果， 但这些方法都有各自的优缺点，不能完全满足 RFID 系统的安全需求。原因主要在于要大规模推广使用 RFID 技术，必须严格限制标签的成本，而低成本的标签又极大限制了其安全和隐私问题的解决。本文提出的 DSTAP 协议，可做到以最小的标签计算量换来最大的安全性能，从而为进一步探求 RFID 系统的安全解决方案打下了基础。

参考文献

[1] Zhang Lan, Zhou Huaibei, Kong Ruoshan, et al. An Improved Approach to Security and Privacy of RFID Application System[C]//Proc. of International Conference on Wireless Communications, Networking and Mobile Computing. Wuhan, China: [s. n.], 2005.

[2] Chen Y C, Wang Weilin, Hwang M S. RFID Authentication Protocol for Anti-counterfeiting and Privacy Protection[C]//Proc. of the 9th International Conference on Advanced Communication Technology. Phoenix Park, Korea: [s. n.], 2007.

[3] Li Y Z, Cho Y B, Um N K, et al. Security and Privacy on Authentication Protocol for Low-cost RFID[C]//Proc. of Computational Intelligence and Security. International Conference. Guangzhou, China: [s. n.], 2006: 3-6.

[4] Chiu C T, Sheng Bo, Li Qun. Serverless Search and Authentication Protocols for RFID[C]//Proc. of the 15th Annual IEEE International Conference on Pervasive Computing and Communications. White Plains, New York, USA: [s. n.], 2007.

[5] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10): 1743-1756.

[6] 胡游君. RFID 安全协议形式化分析研究及 DRAP 协议的建立与实现[D]. 秦皇岛: 燕山大学, 2007.

(上接第 158 页)

而距离不变保证变换后数据的相异矩阵不变，即不会对聚类的结果产生影响。与RBT[3]不同的是，本文讨论的离散余弦变换可同时选择多个属性进行变换，并通过对隐私保护度的评估，在多次变换后选择最优的变换结果，使其在多数情况下具有较好的隐私保护效果。

参考文献

[1] 吕　品, 陈年生, 董武世. 面向隐私保护的数据挖掘技术研究[J]. 计算机技术与发展, 2006, 16(7): 147-149.

[2] Oliveira S R M, Zaïane O R. Privacy Preserving Clustering by Data Transformation[C]//Proc. of the 18th Brazilian Symposium on Databases. Manaus, Amazonas, Brazil: [s. n.], 2003: 304-318.

[3] Oliveira S R M, Zaïane O R. Achieving Privacy Preservation When Sharing Data for Clustering[C]//Proc. of the International Workshop on Secure Data Management in a Connected World in Conjunction with VLDB. Toronto, Canada: [s. n.], 2004.

[4] Vaidya J, Clifton C. Privacy-Preserving K-Means Clustering over Vertically Partitioned Data[C]//Proc. of the 9th ACM SIGKDD Intl. Conf. on Knowledge Discovery and Data Mining. Washington D. C., USA: ACM Press, 2003: 206–215.

[5] Jha S, Kruger L, McDaniel P. Privacy Preserving Clustering[C]//Proc. of the 10th European Symposium on Research in Computer Security. Milan, Italy: [s. n.], 2005: 397-417.

[6] Blake C L, Merz C J. UCI Repository of Machine Learning Databases[D]. California, USA: University of California, 1998.