一种增强型基于低成本的 RFID 安全性认证算法

孙 麟 刘彦明 西安电子科技大学 710071

摘 要：本文在引入“物元网”的基础上提出一个增强型低成本 RFID 安全性认证算法，它有效解决了目前阻碍 RFID 系统广泛应用于超市等对单个射频标签造价要求很低的场合的问题，该认证算法在节约射频标签的资源的同时，利用单向认证技术以及变址技术阻止了消息泄漏，伪装，地址跟踪等安全性攻击，使得该系统非常具有实用性。

关键字：RFID；物元网；认证

1. 低成本 RFID 算法介绍

目前，RFID(Rdiao frequency identification)系统被广泛应用于物流管理，门禁系统，自动收费系统，超市，银行信用卡等领域中，使我们得到一个共识，RFID 的世界离我们是越来越近了。虽然 RFID系统给我们的生产生活带来了许多的便利，但是在RFID系统中目前存在着一个致命的“硬伤”——RFID标签的造价太贵，目前一个RFID标签的造价要控制在0.05美元左右，只有这样，RFID标签才能被广泛应用于超市，银行支票，物流管理等系统中，而以目前的 CMOS 电路的制造工艺来看，如此低廉的生产成本下很难保证RFID系统具有完善的安全认证算法，在这种低成本的要求下，射频标签的存储量只有几百个字节，芯片内只有大约 500——5000 个逻辑门，作用范围也就是几米而已。而对称性数据加密算法——AES 算法，至少需要 20000——30000 个逻辑门，其他一些数据加密算法 DES，NTRU，SHA-1等，都远远超出了5000个逻辑门的上限。本文的重点就是提出一个满足低成本的RFID系统的读卡器和射频标签之间相互认证的方案。

2. 主要流程

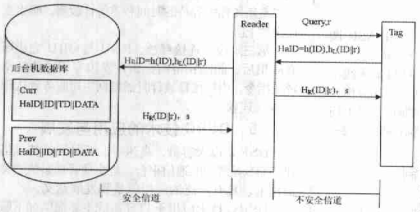

图 1 低成本 RFID 算法流程

当射频标签进入读卡器工作范围以后，读卡器和标签之间开始相互认证，其工作流程如图 1 所示。

1) 读卡器将查询信号和随机数r发送给射频标签。

①. 一旦射频标签被激活，射频标签使用hash函数以及自己的ID和收到的随机数r来计算HaID=h(ID)，h_LID(ID||r)，这里h_L(ID||r)表示h(ID||r)的左半部分数据，其长度为1/2bit。

②. 读卡器收到射频标签的数据 HaID=h(ID)，hLID(ID||r)后将数据转发给后台机数据库中。

③. 后台数据库检查 Prev 中的 HaID 是否与从读卡器转发过来的 HaID 相同，如果相同则表示从标签到读卡器的认证成功，后台机使用发给读卡器的随机数 r 以及 Prev 中的 ID 来计算 h_R(ID||r)，其中 h_R(ID||r) 表示 h(ID||r) 的右半部分数据，长度为1/2bit，然后将 h_R(ID||r) 发送给读卡器。

④. 读卡器将接收到的 h_R(ID||r) 和随机数 s 转发给射频标签。在这里随机数 s 并不是完全随机的，它的选择有一定的规则，我们将在第 3 部分详细说明。

⑤. 射频标签将检验接收到的 h_R(ID||r) 的正确性，其方法是利用标签自己的ID和前面接收到的随机数 s 计算标签自己的 h_R(ID||r)，比较两个值是否相同，如果相同则读卡器到标签的认证成功，然后射频标签利用随机数s和自己的ID将其ID改为ID⊕s。

2) 基于 EPC 的物元网模型

整个物元网的构成如图 2 所示：

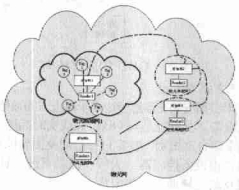

图 2：RFID 物元网结构图

在前面由于我们采用了动态 UID 的方法，所以我们必须解决地址重复问题，采用简单的 IP 地址分配方法来进行UID分配是非常可靠的，并且，UID 的分配是在后台机上进行的，所以不会影响射频标签的成本。这里的 s 的选择规则是根据标签目前的ID号查询物元网的 UID 分配信息，保证满足（新 ID）=s（原 ID）的新 ID 是未使用的 ID。

3). 低成本RFID算法的安全性和效率分析

对于可能存在的消息泄露，替代，地址跟踪这三类安全性威胁，我们所提出的低成本 RFID 算法能有效的解决，现在简单分析说明一下，由于在读卡器和射频标签中传输的都是经过Hash函数加密后的数据：HaID=h(ID)，h_L(ID||r)，H_R(ID||r)等，这些数据即使被攻击者侦听到也没有办法破解出标签的ID，所以消息泄露这样的安全性威胁在该算法中是不存在的，另外，在算法的具体流程中已经提到了，这个算法采用的是读卡器和标签相互认证的方法，并且 r 是随机变化的，因此，假冒的标签在不知道合法标签的ID的情况下根本无法回应 hL(ID||r)给读卡器，上面所说的第二种威胁也不会存在，最后，由于我们采用的是动态 ID 方法，虽然攻击者不停的尝试找出合法标签的 ID，但是，即使当他成功找到其ID并建立连接后根据我们的动态ID规则，一旦成功通信就改变标签的 ID 值，从而使刚刚建立的连接断开，攻击者不得不又一次进入到无限的 ID 尝试中，这样，对于想进行地址跟踪的攻击者来说，这样只能是徒劳无功。

由于这个算法中将 ID 分割为左右两半进行运算，因此算法的复杂度大大降低了，并且卡片内存储的信息非常少，只有卡片 ID 和单向的 Hash 函数，非常符合低成本 RFID 系统的要求。

3. 结论

在这篇文章中，我们提出了一个非常实际有效的RFID安全性算法，我们仅采用两个单向 Hash 函数来进行相互认证，并且计算的数据基本上都是标签ID长度的二分之一，这大大节约了射频标签的资源，同时，该算法能有效的避免消息外泄，假冒，地址跟踪等安全性方面的威胁，有效地解决了目前生产成本和安全性方面的矛盾，最后，我们在物元网的高度上引入IP地址分配的方法来解决可能存在的地址重复问题。

参考文献

[1] Richard Boss, Library RFID technology. Library Technology Reports, Nov/Dec 2003.

[2] 王育民，刘建伟著.通信网的安全——理论与技术.2002 年

[3] R.Damith and E.Daniel and C.Peter Low--cost RFID Systems: Confronting Security and Privacy. Auto-ID Labs Research Workshop, 2004.

[4](美) 斯托林斯著；刘玉珍等译.密码编码学与网罗安全.原理与实践,第三版.2004.1

（上接第 13 页）

电子收费等。

DSRC通信主要应用了射频技术、低功耗技术、封装技术和安全技术，随着这些技术的深入研究，DSRC技术在未来的几十年内将获得重大发展。

6. 结束语

DSRC 技术以其传输快速、实时、稳定、可靠的数据传输特点在ITS系统中获得了广泛应用，推动着我国公路管理技术的不断提高。为此，我们还要对DSRC通信中的技术问题继续研究，如数据的安全保密、红外DSRC技术以及DSRC公网和专网建设等。

参考文献

[1] 刘利频,徐建闽,陈欢.DSRC技术在ITS服务领域的应用[J].广东公路交通.2004(3)

[2] 彭逸荣，钟慧玲，徐建闽. 专用短程通信(DSRC)协议研究及应用展望[J]. 移动通信[J].2003年增刊

[3] 马钺. 基于DSRC的多功能不停车收费系统[J].计算机工程与应用.2002 年 10 月

[4] 陈红华，李洁，王文骐. ETC技术及其发展[J].公路交通科技. Vol.18 No.3 2001年6月

[5] 王媛媛. ITS系统中DSRC协议的时窗管理分析[J]. Radio Engineering VO. 33 NO. 4. 2003年