对一种基于低成本 RFID 的强认证强完整性(ASASI)协议的攻击与改进

朱乃桄 吴宇啸 常湛
（南京邮电大学 南京 210003）

摘要 当今社会，RFID 系统是非接触双向数据通信领域的最具有发展潜力的信息技术之一。然而，RFID 系统的安全性和私密性受到极大的关注。本文对一种基于低成本 RFID 的强认证强完整性协议进行了脆弱性分析后利用多轮监听攻击成功攻破了此方案。之后，对原方案进行改进，得出新的改进方案。最后，对 ASASI 改进方案安全性分析表明其优于其他 UMAP 方案，因此可以很容易地在极轻量级的 RFID 标签上实现。

关键词 RFID 系统 物联网安全 超轻量级认证协议

Attack And Improvement on A Strong Authentication Strong Integrity (ASASI) Protocol for Low Cost Radio Frequency Identification

Zhu Naiguang Wu Yuxiao Chang Zhan
(Nanjing University of Posts and Telecommunications , Nanjing 210003)

Abstract In today's society, RFID system is one of the most potential information technologies in the field of non-contact bi-directional data communications. However, the security and privacy of RFID systems are of great concern. This paper analyzes the vulnerability of a strong authentication strong integrity (ASASI) protocol for low cost radio frequency identification and the scheme was successfully breached by utilizing multiple rounds of Sniffering attacks. After that, the original scheme is improved to get the advance one. Finally, the security analysis of the advance ASASI scheme shows that it is superior to other UMAP schemes and can be easily implemented on extremely lightweight RFID tags.

Key Words RFID systems, IoT security, Ultralightweight authentication protocol

1 引言

物联网(IoT)通过连接多个电子设备来共享数据。物联网基于应用的目标，采取适当的措施，彻底改变了普适计算的概念。国际上针对物联网安全和隐私的研究已展开。Mulligan 等[1]对物联网的现状进行了总结和分析,并对物联网安全进行了讨论和展望。Medaglia 等[2]给出物联网目前面临的隐私与安全问题综述,并对将来可能出现的安全问题进行了讨论。Leusse 等[3]给出一个物联网服务安全模型, 并对其包含的模块进行了介绍和分析。Hamad 等[4]针对目前已有的物联网加密算法, 从电池能量消耗等资源消耗方面进行了对比分析。[5]射频识别(RFID)系统和无线传感器网络(WSN)是现如今用于物联网身份管理的技术。RFID 技术出现至今已经 70 多年了。然而，RFID 系统因其扫描距离远、扫描速度快而广受人们的青睐。RFID(Radio Frequency Identification) 是非接触双向数据通信，通过无线射频方式对记录媒体（电子标签或射频卡）进行读写，从而达到识别目标和数据交换的目的。[6]为了提高 RFID 系统的安全性，研究者们把密钥方法应用到 RFID 认证协议中，但是 RFID 标签其储存空间和计算能力都有限，无法实现复杂的高安全加密算法。另一方面，RFID 系统采用超轻量级相互认证协议(UMAPs)，为可靠识别问题提供了高效解决方案。[7-15]

基于协议中使用的操作符，UMAPs 可以分为两大类: Triangular UMAPs 和 Non-Triangular UMAPs。经过关于 UMAPs 的详细密码分析，发现了协议中使用的方程和内存结构的方面存在弱点。据我们所知，所有现有的 UMAPs 都容易受到许多安全威胁。对于超轻量级的协议，SASI[16]在 UMAP 相互认证协议族的基础上，提出了改进的 UMA-RFID 相互认证协议。而 SASI[16]针对 UMA-RFID 协议的安全性漏洞进行了分析，并提出了相应的改进协议。然而,文献[17]中 SASI 协议也存在着明显的安全性漏洞。这证明 RFID 系统缺乏安全的标准身份验证协议。所以，Madiha Khalid 和 Umar Khokhar 等人对 Non-Triangular UMAPs 进行了详细的密码分析，利用概率攻击 SASI[16]证明其因不平衡地使用 AND,OR 等操作符，使得协议易被充分披露攻击攻破。于是，文献[17]在 SASI[16]基础上提出了一种基于低成本 RFID 的强认证强完整性协议(ASASI)[17]。

然而，文献中改进协议也存在着明显的安全性漏洞。本文针对于文献中提出的基于低成本 RFID 的强认证强完整性协议(ASASI)[17]，提出了一种简单有效的攻击方案。并通过编程实现此攻击方案，验证了方案的可行性。本文进一步在文献的基础上，提出了一种改进的基于低成本 RFID 的强认证强完整性协议，证明了其正确性和安全性。

2 ASASI 方案简介

2.1 符号说明

(1)Tag：标签；

(2)Reader：阅读器；

(3)ID：标签唯一标识符(96bit)；

(4)K_1，K_2：动态密钥(96bit)；

(5)IDS：伪识别符(96bit)；

(6)Rot(x,y) ：x 左循环移位，移动长度为 y 的汉明重量。

2.2 协议概述

文献中的方案，为了避免诸如 AND,OR 等不平衡的运算符的使用。仅在方案

中使用了 XOR 和 Rot(x,y)。方案流程如下：

(1) 阅读器通过向标签发送“$Hello$”信息标签开始认证过程。

(2) 标签接到“$Hello$”消息,发回最新IDS。

(3) 阅读器在数据库搜索收到的IDS,如果读者的数据库中能够匹配IDS。则生成伪随机数m_1(96bit),m_2(96bit)和计算公共消息(A,B,C):

$$A=Rot(m_1 \oplus K_1, K_2)$$

$$B=Rot(m_2 \oplus K_2, K_1 \oplus m_1)$$

$$C=Rot(m_1 \oplus m_2, K_1 \oplus K_2)$$

否则,阅读器将发送另一个“$Hello$”信息标签,将使用之前的IDS的值。

(4) 收到 A,B,C 后，标签先利用 A,B,C 计算出m_1,m_2.

$$m_1=Rot^{-1}(A, K_2) \oplus K_1$$

$$m_2=Rot^{-1}(B, K_1 \oplus m_1) \oplus K_2$$

接着将本地储存的 C 的值与接收到的 C 的值进行对比。如果两个值匹配，则标签认证成功。并通过消息 D 隐秘地把 ID 发送给阅读器。否则，标签将中断与阅读器之间的交流。

$$D=Rot(ID \oplus m_1 \oplus K_2, K_2 \oplus m_2)$$

(5) 为了验证标记,读者将本地储存的 D 的值与接收到的 D 的值进行对比。如果两个值匹配，则阅读器认证成功，否则阅读器中断与标签之间的交流。认证成功后，使用以下公式更新双方的动态变量:

$$IDS^{next}=Rot(IDS \oplus m_1, K_1 \oplus m_2)$$

$$K_1^{next}=Rot(K_1 \oplus K_2, m_2)$$

$$K_2^{next}=Rot(m_1, K_2 \oplus m_2)$$

协议的区块图如图 1 所示：

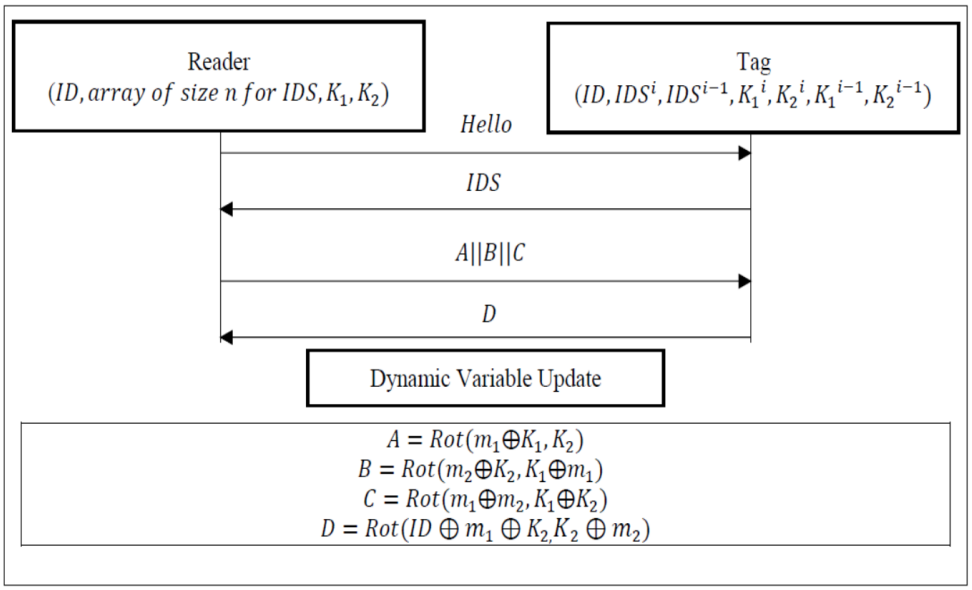

图 1 ASASI 协议区块图

3 对 ASASI 方案进行攻击

3.1 原方案的脆弱性分析

原方案中，Reader 原意是想通过 A 和 B 向 Tag 传送伪随机数m_1和m_2，且未

防止被篡改，通过 C 来验证伪随机数m_1和m_2的完整性，Tag 回传一个 D 告知 Reader 自己得到了正确的伪随机数m_1和m_2。

原方案的脆弱性主要体现在以下方面：首先，原方案的计算公式 Rot(x,y)中的 y 仅 96bit 长度，且取用的是 y 的汉明重量的值。给枚举所有情况提供了可能性。用到的左移方法并不会改变汉明重量，也就是说，比特串左移前的汉明重量和比特串左移后的汉明重量是相等的。其次，由于有 IDS^{next}=Rot(IDS⊕m_1,K_1⊕m_2)该表达式。可通过连续监听两轮通信，依次得出 IDS 和 IDS^{next} 的值。A、B 的公式相对简单，因此 B 和 D 中左移的汉明重量可根据上一个脆弱性直接得到。为攻击提供便利。最后，C 左移的比特串只含有m_1⊕m_2的简单性为破获得到 ID 提供了直接快速的方案，具体方法详见攻击方案。

3.2 攻击方案

分析 A、B、C 的三个公式，可以得到以下信息：A 是由m_1⊕K_1后的值左移 K_2的汉明重量得到的，然而右移并不改变m_1⊕K_1后的值的汉明重量，因此 A 的汉明重量和m_1⊕K_1的汉明重量是一样的，据此我们监听了 A 便可知道m_1⊕K_1的汉明重量，根据 B 的公式，根据监听到的 B，结合m_1⊕K_1的汉明重量，便可确切的得到m_2⊕K_2的值。有了m_2⊕K_2的值后，根据 D 的公式，可确切得到 ID⊕m_1⊕K_2的值。根据如下公式：

$$ID=ID\oplus m_1\oplus K_2\oplus m_1\oplus K_2=ID\oplus m_1\oplus K_2\oplus m_1\oplus m_2\oplus m_2\oplus K_2$$

破获 ID 需要得到m_1⊕m_2的值，在 C 的公式中有所需要的此项，需将 C 右移 K_1⊕K_2后的值的汉明重量。又因，K_1与 K_2均为 96 比特数。因此仅需遍历 96 次就可得到 ID 的所有可能性。监听下一轮阅读器和标签之间的通信，执行相同的操作，比较两次得到的 ID 所有可能性，找到两次攻击相同结果即攻击得到的 ID。

3.3 攻击方案分析

本攻击方案以 C 作为突破口，并利用循环移位前后，汉明重量不变这个特点。为各表达式之间建立关系，得到了m_2⊕K_2和 ID⊕m_1⊕K_2的值。并将 ID 转换成 ID⊕$m1$⊕K2⊕$m1$⊕$m2$⊕$m2$⊕K2 的形式。代入已知值，发现仅需枚举 K_1⊕K_2的汉明重量，再通过两轮监听。就能破解 ID 的值。

此攻击方案总体过程简单，易于操作。通过个人计算机的编程和计算可以破解出 ID 的值。通过高级程序语言编程实现 ASASI 方案的初始化截图如图 2 所示：

```
int ID[96]= {0,1,1,1,0,1,0,1,0,0,1,0,1,0,0,1,0,1,0,1,1,1,1,1,0,1,0,1,0,1,1,0,1,0,0,1,0,1,1,1,0,1,1,1,1,1,1,1,1,1,
             0,0,1,1,0,1,1,0,1,1,0,0,1,0,0,1,1,1,0,1,1,1,1,0,0,1,0,1,1,1,0,0,1,0,1,1,1,0,1,1,0,0,0,0,0,1,0,1};
int K1[96]= {1,0,0,0,1,1,0,0,1,0,1,1,0,0,0,0,0,1,1,1,1,1,1,0,0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,0,1,0,0,1,0,0,1,0,0,1,0,
             1,0,0,0,0,1,0,1,0,1,1,0,1,1,0,0,0,0,0,1,1,0,1,1,0,0,0,0,1,1,1,0,1,0,0,0,1,0,1,0,1,1,1,1,1,1,0,0,1};
int K2[96]= {0,0,1,1,0,1,1,0,0,1,0,1,0,1,1,0,1,0,0,0,1,1,0,1,1,1,0,0,1,1,0,1,0,1,1,1,1,1,1,0,0,0,0,1,0,1,0,0,0,0,
             1,0,0,1,0,0,1,0,1,0,0,0,0,1,1,0,1,1,0,1,0,0,1,0,1,0,0,1,1,1,0,0,1,0,0,1,0,1,1,0,0,1,0,1,0,0,1,0};
int IDS[96]={1,1,0,1,0,0,1,0,0,0,1,1,0,0,0,0,1,0,1,1,1,0,0,0,1,1,0,1,0,1,0,1,0,1,0,0,1,1,1,1,1,0,1,1,0,1,0,0,0,1,0,
             1,0,0,1,1,0,1,1,0,1,0,1,1,0,1,1,1,1,1,1,1,0,1,1,0,1,0,1,1,1,0,1,1,1,0,1,1,0,0,1,1,0,1,1,1,1,1,0,1,1};
```

图 2 ASASI 方案的初始化图

此攻击方案的攻击成功截图如图 3 所示

```
A1为:        10000011011111010010100100011111101101111011110001011111100010000111111011000010011101001000110
B1为:        00010001100011011000001110000100101010001111100110010110101100010111011001011100101110010101
C1为:        00010010000010101101010000101011001011100001110110110000010100000101011011100011010100000000110111
D1为:        10001011011110001101010110010001001000011011010110011011101001000011000001110001111111100010010
IDS_next为: 01010011110010101010001010111011101110101000111101001100000011100101000111011001100100010010000
A2为:        00110001101010010111001100101110100111011111100100001010111110010100100111100110001010111000111
B2为:        10101100111100100000000111001111001111111001111100001000001000101110001110100011010101100010100000
C2为:        00111011011011011110100001010000111100100001000110011010110001000010100110001001000110010101001
D2为:        00110010101001111011001000010110000011000001000111110011100111000000100001100111010111001110111
IDS_next_next为: 11011110010111101111111101100001100110001010110000000001011010101100001101010010001010001111101000
ID为: 01110101001010010111101010110100101110111111111001101101100100111011110010110001011010011000000101

--------------------------------

Process exited after 0.1673 seconds with return value 0
请按任意键继续. . .
```

图 3 攻击方案的攻击成功图

4 改进方案设计

4.1 改进方案

通过对之前的原方案脆弱性分析和攻击方案分析，可以发现 ASASI 协议的易受攻击的主要原因是阅读器发给标签的 C 的公式的脆弱性。所以，本改进方案从 C 入手，通过对校验用的公共消息 C 进行修改，来抵抗监听攻击。

修改的具体内容如下：

(1)修改 ASASI 方案的顺序,在原方案第三步阅读器在数据库搜索收到的IDS,如果读者的数据库中能够匹配IDS。则生成伪随机数m_1(96bit),m_2(96bit)后，计算K_1^{next}和K_2^{next}。K_1^{next}和K_2^{next}计算公式不发生改变。

(2)计算出K_1^{next}和K_2^{next}后，添加新动态密钥(96bit)K_3，K_3计算公式如下：

$$K_3=K_1^{next}\oplus K_2^{next}$$

(3)之后计算公共消息 C 时，将 C 的计算公式修改如下：

$$C=Rot(K_3\oplus m_1\oplus m_2,K_1\oplus K_2)$$

(4)不用再计算原方案第五步时计算的K_1^{next}和K_2^{next}，直接沿用改进方案第二步计算出的K_1^{next}和K_2^{next}。

本改进方案主要从公共消息 C 入手，结合之前的原方案脆弱性分析和攻击成功的原因。将 C 的值改为$K_3\oplus m_1\oplus m_2$左移$K_1\oplus K_2$的汉明重量。再次利用表达式：

$$ID=ID\oplus m1\oplus K2\oplus m1\oplus K2=ID\oplus m1\oplus K2\oplus m1\oplus m2\oplus m2\oplus K2$$

后发现由于 C 增加了动态密钥K_3。导致再次$K_3\oplus m_1\oplus m_2$无法直接套入该表达式，直接使得本文攻击方案无效。

同时，由于K_1^{next}和K_2^{next}表达式：

$$K1^{next}=Rot(K1\oplus K2,m2)$$

$$K2^{next}=Rot(m1,K2\oplus m2)$$

可以看出$K_3\oplus m_1\oplus m_2=Rot(K1\oplus K2,m2)\oplus Rot(m1,K2\oplus m2)\oplus m_1\oplus m_2$，直接影响了多轮监听攻击获得$m_1$，$m_2$，$K_1$，$K_2$一系列相关 XOR 的值。给其他攻击方案带来了极大的难度。

5 结语

本文对基于低成本 RFID 的强认证强完整性(ASASI)协议进行了脆弱性分析。利用多轮监听的攻击方法攻击了 ASASI 方案，证明了其存在安全缺陷。并给出改进方案来抵御上述攻击。对 ASASI 改进方案的安全性分析表明其优于其他 UMAP 方案。与其他 UMAP 方案一样，ASASI 改进方案在其设计中只涉及一个非三角形功能，因此可以很容易地在极轻量级的 RFID 标签上实现。

参考文献：

[1] Mulligan G. The Internet of Things:Here now and coming soon[J]. IEEE Internet Computing, 2010, 14(1), 1:35-36.

[2] Medaglia C M, Serbanati A. An overview of privacy and security

issues in the Internet of things[C]//Proceedings of the 20th Tyrrhenian Workshop on Digital Communications.Sardinia, Italy:Springer, 2010:389-395.
[3] Leusse P, Periorellis P, Dimitrakos T. Self managed security cell, a security model for the Internet of Things and services [C]// Proceedings of the 1st International Conference on Advances in Future Internet. Athens/Glyfada, Greece:IEEE, 2009:47-52.
[4] Hamad F, Smalov L, James A. Energy-aw are security in M-commerce and the Internet of Things[J]. IEEE Technical review, 2009, 26(5):357-362.
[5]杨光,耿贵宁,都婧,刘照辉,韩鹤.物联网安全威胁与措施[J].清华大学学报(自然科学版),2011,51(10):1335-1340.
[6]郑晓琳.基于 RFID 技术的图书借阅系统的设计与实现[J].计算机产品与流通,2019(11):161.
[7]付俊,严新荣,付强.一个超轻量级的 RFID 认证协议[J].舰船电子工程,2019,39(03):107-110.
[8]刘立波,郑巧珍,付强.一种增强型 RFID 双向认证协议[J].舰船电子工程,2019,39(10):96-100+105
[9] Rabaninejad R, Ahmadian M,Asaar M R, et al. A Lightweight Auditing Service for Shared Data With Secure User Revocation in Cloud Storage[J]. IEEE Transactions on Services Computing, 2019.
[10] Sidorov M, Ong M T, Sridharan R V, et al. Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains[J]. IEEE Access, 2019, 7: 7273-7285.
[11]左黎明,夏萍萍,林楠.对一个无证书签密方案的攻击与改进[J].华东交通大学学报,2019,36(04):119-123.
[12]周克元.对一种改进的 ElGamal 数字签名方案的攻击与改进[J].计算机应用与软件,2019,36(04):323-325+333.
[13]吴孟霖.基于物联网和云计算的物流发展模式分析[J/OL].现代营销(下),2019(11):96-97[2019-12-05].
[14]蒋皓石,张成,林嘉宇.无线射频识别技术及其应用和发展趋势[J].电子技术应用,2005(05):1-4.
[15]胡向东.物联网研究与发展综述[J].数字通信,2010,37(02):17-21.
[16] Chien, Hung-Yu. Sasi: A new ultralightweight rfid authentication protocol providing strong authentication and strong integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007,4(4): 337-340.
[17]Khalid M, Khokhar U, Najam-ul-Islam M. Advance Strong Authentication Strong Integrity (ASASI) Protocol for Low Cost Radio Frequency Identification[C]//2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE). IEEE, 2018: 1-6.