第37卷 第16期 计 算 机 工 程 2011年8月
Vol.37 No.16 Computer Engineering August 2011

·安全技术· 文章编号：1000—3428(2011)16—0140—03 文献标识码：A 中图分类号：TP309

一种超轻量级的RFID双向认证协议

彭 朋[1]，赵一鸣[1]，韩伟力[1]，金 波[2]

(1. 复旦大学软件学院，上海 200433；2. 公安部三所信息网络安全公安部重点实验室，上海 201204)

摘 要：给出一种针对Gossamer协议的拒绝服务攻击，据此提出一种超轻量级的无线射频识别(RFID)读写器-标签双向认证协议。对该协议的安全性和效率进行分析，结果表明，与SASI协议和Gossamer协议相比，该协议能抵抗拒绝服务攻击和代数攻击，只使用较少的标签存储空间，成本更低且具有更高的安全性。

关键词：超轻量级；无线射频识别；双向认证协议；拒绝服务攻击；代数攻击

Ultra-lightweight RFID Mutual Authentication Protocol

PENG Peng[1], ZHAO Yi-ming[1], HAN Wei-li[1], JIN Bo[2]

(1. Software School, Fudan University, Shanghai 200433, China;
2. Key Laboratory of Information Network Security, Ministry of Public Security,
The Third Research Institute of the Ministry of Public Security, Shanghai 201204, China)

【Abstract】This paper gives a Denial of Service(DoS) attack against the Gossamer protocol, and proposes a novel ultra-lightweight Radio Frequency Identification(RFID) reader-tag mutual authentication protocol. It analyzes the security and efficiency of the protocol, the results show that compared with the SASI protocol and the Gossamer Protocol, the proposed protocol is resistant to the DoS attack and algebra attack, and requires less storage capacity on tags, it is cheaper and securer.

【Key words】ultra-lightweight; Radio Frequency Identification(RFID); mutual authentication protocol; Denial of Service(DoS) attack; algebra attack

DOI: 10.3969/j.issn.1000-3428.2011.16.047

1 概述

无线射频识别(Radio Frequency Identification, RFID)是一种非接触式自动识别技术。它已逐渐在物品标识、电子票证、商品防伪、身份识别等各个领域得到广泛应用，但安全问题，特别是标签与读写器之间的认证问题，成为了制约其发展的重要因素。RFID系统的认证问题是指对标签和阅读器的合法性进行确认，包括防止对标签的克隆攻击、伪造等。由于RFID系统受到计算能力、存储空间和电源供给等诸多因素的限制，如何设计安全、高效、低成本的RFID安全认证协议是一个具有挑战性的课题[1]。

到目前为止，已经有多种RFID认证协议被提出[1]，例如Hash-Lock协议、随机化Hash-Lock协议、Hash链协议等。文献[2]将RFID认证协议可根据标签上的计算量和操作分为4类：全面认证协议，简单认证协议，轻量级认证协议，超轻量级认证协议。全面认证协议需要传统的对称加密算法、哈希函数，甚至非对称加密算法的支持；简单认证协议需要伪随机数和单向哈希函数的支持；轻量级认证协议需要伪随机数发生器和CRC校验码的支持；而超轻量级认证协议仅需要基本的位运算(与、或、非、异或、移位等)的支持，超轻量级的协议主要是针对低成本RFID标签而设计的。

文献[3]提出了一系列超轻量级的双向认证协议，都采用了假名来保证标签的匿名性，并且只需要异或、或、与以及模加操作的支持，但不能抵抗代数攻击。文献[2]提出了SASI协议，该协议能够提供更强的认证和完整性保障，但也被指出不能抵抗拒绝服务攻击[4]和代数攻击[5]。文献[6]针对SASI协议的缺陷又提出了Gossamer协议。

本文指出，Gossamer协议也不能抵抗拒绝服务攻击，而且，Gossamer协议在标签上的计算量和功耗都很大，不能满足低成本RFID标签的需求。针对Gossamer协议的拒绝服务攻击，以及SASI协议和Gossamer协议的漏洞，本文提出一种新的超轻量级认证协议。

2 预备知识

2.1 *ROT*函数

$ROT(x, y)$[6]：*ROT*函数是一个非线性函数，$ROT(x, y)$是指将x的值循环左移$(y \bmod N)$位，在SASI协议和Gossamer协议中，N等于96。

2.2 *MIXBITS*函数

$MIXBITS(x, y)$[6]：*MIXBITS*函数也是一个非线性的函数，它采用了右位移操作(>>)，$MIXBITS(x, y)$将执行的操作如下：

```
Z=x;
for(i=0; i<32; i++)
Z= (Z>>1)+ Z + Z +y ;
```

2.3 SASI协议

在SASI协议的初始状态，读写器中保存着标签的假名*IDS*、真实的*ID*，以及密钥K_1、K_2，标签中保存着标签的真实*ID*，当前以及上一轮的*IDS*、K_1、K_2:*ID* 、IDS^{next}、K_1^{next}、K_2^{next}、IDS^{old}、K_1^{old}、K_2^{old}。SASI协议的主要优点在于标签上的操作简单，标签上仅需要∨(或运算)、∧(与运算)、⊕(异或运算)、+(模加运算)和$ROT(x, y)$操作的支持。SASI协议包

基金项目：信息网络安全公安部重点实验室开放课题基金资助项目(C10612)

作者简介：彭 朋(1987－)，女，硕士研究生，主研方向：密码与信息安全；赵一鸣、韩伟力，副教授；金 波，研究员

收稿日期：2011-02-15 **E-mail：**pengpeng870903@gmail.com

括以下 3 个步骤：

(1)标签识别：读写器发送 Hello 请求给标签，标签收到请求之后首先返回 IDS^{next} 给读写器，如果读写器能够找到与 IDS^{next} 匹配的记录，则进入步骤(2)；否则读写器重新发送 Hello 请求，标签返回 IDS^{old} 给读写器。

(2)双向认证：读写器找到与 *IDS* 匹配的记录，并产生 2 个随机数 n_1 和 n_2，计算 $A=IDS\oplus K_1\oplus n_1$、$B=(IDS\vee K_2)+n_2$、$K_1{*}=ROT(K_1\oplus n_2, K_1)$、$K_2{*}=ROT(K_2\oplus n_1, K_2)$、$C=(K_1\oplus K_2{*})+(K_1{*}\oplus K_2)$，并发送 $A||B||C$ 给标签。标签接收到 $A||B||C$，并根据 *A* 和 *B* 计算出 n_1 和 n_2，用同样的公式计算 K_1^*、K_2^*和 C^*，比较 *C* 与 C^*来验证读写器的合法性。如果 *C* 与 C^*一致，则读写器认证通过；否则，协议中止。标签计算 $D=(K_2^*+ID)\oplus((K_1\oplus K_2)\vee K_1^*)$并发送给读写器。读写器收到 *D* 之后，通过 *D* 来验证标签的合法性。如果验证通过，则进入更新阶段，否则不更新。

(3)更新：标签发送消息 *D* 之后便进行如下更新：$IDS^{old}=IDS$、$IDS^{next}=(IDS+ID)\oplus(n_2\oplus K_1^*)$、$K_1^{old}=K_1$、$K_2^{old}=K_2$、$K_1^{next}=K_1^*$、$K2_{next}=K_2^*$。读写器验证消息 *D* 成功之后也进行如下更新：$IDS=(IDS+ID)\oplus(n_2\oplus K_1^*)$，$K_1=K_1^*$，$K_2=K_2^*$。

3　超轻量级的 RFID 双向认证协议

3.1　针对 Gossamer 协议的拒绝服务攻击

Gossamer 协议的初始状态与 SASI 协议一致，读写器中保存着 *IDS*、*ID*、K_1、K_2，标签中保存着 IDS^{next}、K_1^{next}、K_2^{next}、IDS^{old}、K_1^{old}、K_2^{old}、*ID*。Gossamer 协议也包括了 3 个步骤：标签识别，双向认证，更新。与 SASI 协议不同的是，Gossamer 引进了一个轻量级的非线性函数 *MIXBITS*，并利用 *MIXBITS* 函数产生了一个新的随机数 n_3 混淆了 *A* 与 *C* 之间的关联。此外，Gossamer 协议更改了 *A*、*B*、*C*、*D* 的计算方法以及 IDS 和 K_1、K_2 的更新方式，提高了计算的复杂度。

Gossamer 协议在标签中保存上一轮的(*IDS*、K_1、K_2)，目的是为了抵抗拒绝服务攻击，但实质上攻击者可以利用消息重放的方法来骗取标签的信任导致读写器与标签两边的 IDS 和密钥无法匹配，协议永远无法再进行。针对 Gossamer 协议实施拒绝服务攻击的过程如下：

(1)第 1 轮通信：攻击者窃听标签和读写器的通信过程，记录消息$(A_1||B_1||C_1)$并截获消息 D_1，此时读写器因为没有收到标签的消息 D_1 不更新 *IDS* 和密钥，而标签则正常更新。因此，此时标签和读写器两端 *IDS* 的情况为：

读写器：$IDS=IDS_1$；

标签：$IDS^{old}=IDS_1$，$IDS^{next}=IDS_2$。

(2)第 2 轮通信：当标签给读写器返回 IDS_2 的时候，由于读写器中没有 IDS_2，因此读写器会继续向标签发送请求，标签返回 IDS_1 给读写器，攻击者不采取任何行动，让通信双方正常通信，两边的 *IDS* 正常更新得到：

读写器：$IDS=IDS_3$；

标签：$IDS^{old}=IDS_1$，$IDS^{next}=IDS_3$。

(3)第 3 轮通信：攻击者发送 hello 请求给标签，标签返回 IDS_3，攻击者重发 hello，此时标签以为读写器没有找到匹配的记录返回 IDS_1 给读写器。攻击者重放第 1 轮通信时窃听到的消息$(A_1||B_1||C_1)$给标签，标签则相信对方是合法的读写器而进行 *IDS* 和密钥的更新，此时更新后的情况如下：

读写器：$IDS=IDS_3$；

标签：$IDS^{old}=IDS_1$，$IDS^{next}=IDS_2$。

此时，读写器的 *IDS* 与标签的 IDS^{old} 及 IDS^{next} 均不相同，之后的正常通信过程中 *IDS* 无法匹配，认证协议失效。

3.2　改进思路

针对 SASI 协议和 Gossamer 协议的缺陷，本文提出一种新的超轻量级 RFID 双向认证协议，改进思路如下：

(1)抗拒绝服务攻击：SASI 协议和 Gossamer 协议都不能抗拒绝服务攻击，改进协议的执行步骤，在阅读器更新 *IDS* 和密钥 K_1、K_2 之前不让标签更新，标签必须收到阅读器触发更新请求之后才能更新 *IDS* 和密钥 K_1、K_2。

(2)减少标签上的存储量：低成本电子标签的存储空间很有限，在 SASI 协议和 Gossamer 协议中，IDS^{old}、K_1^{old}、K_2^{old} 都是保存在标签里面，如果能将 IDS^{old}、K_1^{old}、K_2^{old} 保存在阅读器中而达到一致的效果，将有很大的意义。

(3)降低标签上的计算量：Gossamer 协议为了提高安全性，多次使用了 *ROT* 操作和 *MIXBITS* 操作，导致了协议在标签上的计算量和功耗增加，在保证与 Gossamer 协议相当的安全性的前提下，减少 *MIXBITS* 操作和 *ROT* 操作，降低标签上的计算量。

3.3　改进后的协议过程

改进后的协议也包括 3 个步骤：标签识别，双向认证，更新。改进的协议过程如图 1 所示。协议的初始状态，读写器中保存 IDS^{next}, IDS^{old}, *ID*, K_1^{next}, K_1^{old}, K_2^{new},K_2^{old}，标签中保存 *IDS*, *ID*, K_1, K_2。

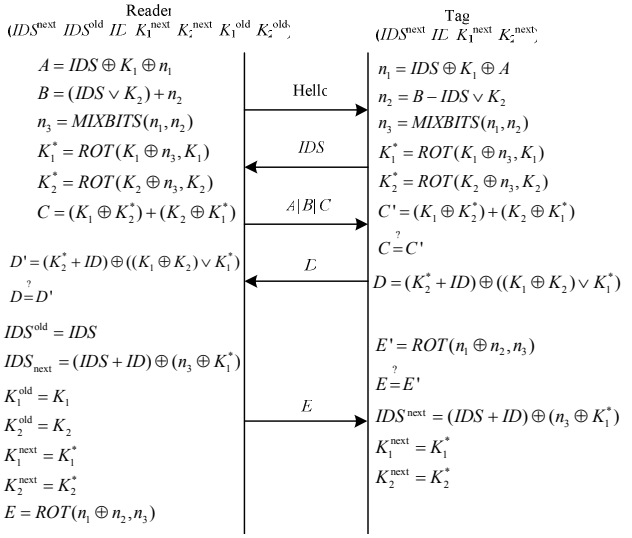


图 1　改进的协议过程

3 个步骤的具体描述如下：

(1)标签识别：读写器发送 Hello 给标签，标签返回 *IDS* 给读写器。

(2)双向认证：读写器在根据接收到的 *IDS* 在数据库中找到 $IDS=IDS^{next}$ 或 $IDS=IDS^{old}$ 的记录。找到之后，产生 2 个随机数 n_1 和 n_2，并用与 *IDS* 对应的 K_1 和 K_2 计算 $A=IDS\oplus K_1\oplus n_1$、$B=(IDS\vee K_2)+n_2$，利用 *MIXBITS* 函数计算一个新的随机数 $n_3=MIXBITS(n_1, n_2)$，计算 $K_1{*}=ROT(K_1\oplus n_3,K_1)$、$K_2{*}=ROT(K_2\oplus n_3,K_2)$、$C=(K_1\oplus K_2{*})+(K_1{*}\oplus K_2)$。读写器发送 $A||B||C$ 给标签，标签接收到 *A*、*B*、*C* 之后根据 *A* 和 *B* 计算出 n_1 和 n_2，用 *C* 来验证读写器的合法性。验证成功之后，计算 $D=(K_2^*+ID)\oplus((K_1\oplus K_2)\vee K_1^*)$，并发送消息 *D* 给读写器。

(3)更新：读写器收到 *D* 之后验证标签的合法性，验证成功之后更新 $IDS^{next}=(IDS+ID)\oplus(n_3+K_1^*)$，$IDS^{old}=ID$，$K_1^{next}=K_1^*$，$K_1^{old}=K_1$，$K_2^{next}=K_2^*$，$K_2^{old}=K_2$，并计算 $E=ROT(n_1\oplus n_2, n_3)$，发送确认更新消息 *E* 给标签。标签收到消息 *E* 之后，验

证 E 成功才更新 $IDS^{next}=(IDS+ID)\oplus(n_3+K_1^*)$，$K_1^{next}=K_1^*$和 $K_2^{next}=K_2^*$。

4 安全性与效率分析

本文基于 SASI 协议和 Gossamer 协议提出了一个改进的超轻量级安全协议，该协议可以抗拒绝服务攻击和代数攻击。具体分析如下：

(1)抗拒绝服务攻击：假设初始状态读写器和标签两端的 IDS 情况如下：

读写器：$IDS^{old}=IDS_0$，$IDS^{next}=IDS_1$；

标签：$IDS=IDS_1$。

攻击者对改进协议发起拒绝服务攻击[4]，那么：

1)第 1 轮通信：攻击者窃听标签和读写器的通信过程，记录消息$(A_1||B_1||C_1)$并截获消息 D_1，此时读写器因为没有收到标签的消息 D_1 不更新 IDS 和密钥，而标签也不会收到确认更新的消息，E 也不会进行更新。因此：

读写器：$IDS^{old}=IDS_0$，$IDS^{next}=IDS_1$；

标签：$IDS=IDS_1$。

2)第 2 轮通信：让通信双方正常通信，两边的 IDS 更新得到：

读写器：$IDS^{old}=IDS_1$，$IDS^{next}=IDS_2$；

标签：$IDS=IDS_2$。

3)第 3 轮通信：攻击者发送 hello 请求给标签，标签返回 IDS_2，攻击者重放第一轮通信时窃听到的消息$(A_1||B_1||C_1)$给标签，标签则相信对方是合法的读写器计算 D'发送给读写器，读写器收到 D'消息之后验证 $D'\neq D_1$，不进行任何更新操作，此时：

读写器：$IDS^{old}=IDS_1$，$IDS^{next}=IDS_2$；

标签：$IDS=IDS_2$。

因此，攻击者使用能够成功攻击 SASI 协议和 Gossamer 协议的攻击方法[4]来攻击改进协议是无效的，最终标签和读写器两端的密钥是同步的。主要原因在于，在每一轮通信协议过程当中，读写器总是在标签更新之前进行更新，而且读写器必须验证 D 通过之后才会更新，一旦读写器进行了更新，则说明读写器与标签之间必有 IDS 匹配，不管标签是否进行更新。

(2)抗代数攻击：与 SASI 协议相比较，改进协议引进了 Gossamer 协议中使用的 $MIXBITS$ 函数，利用 $MIXBITS(n_1, n_2)$ 产生了一个新的随机数 n_3 用来生成消息 C，混淆了 A 和 C 之间的代数关系，攻击者也无法利用 SASI 中 A、C 之间有对应关系的漏洞来对其进行攻击，因此能抵抗抗同步、ID 泄露和全泄露等代数攻击。

在标签的存储空间方面，SASI 协议和 Gossamer 协议都将上一轮的 IDS 和密钥 K_1、K_2 保存在标签上，而改进协议将这些信息保存在读写器中，节省了标签的存储空间。

与 SASI 协议相比较，改进协议增加了更新确认的步骤，引入了 $MIXBITS$ 操作，计算量有所增加。但与 Gossamer 协议相比较，改进协议虽然增加了更新确认的步骤，但大大减少了 $MIXBITS$ 和 ROT 在标签上的使用次数(Gossamer 协议在标签上需要 2 次 $MIXBITS$ 操作、8 次 ROT 操作，而改进协议在标签上仅需要 1 次 $MIXBITS$ 操作、3 次 ROT 操作)，计算量有所减少。因此，改进协议的计算量处于 SASI 协议和 Gossamer 协议之间。3 种协议的性能比较如表 1 所示，其中，L 为变量长度，此处 L=96 bit。

表 1 3 种协议的性能比较

协议	抗 DoS 攻击	抗代数攻击	标签上的存储量/bit	标签上的计算量
SASI 协议	否	否	7L	较小
Gossamer 协议	否	是	7L	较大
本文协议	是	是	4L	适中

5 结束语

由于 Gossamer 协议不能抵抗拒绝服务攻击，因此本文提出了一种适用于低成本 RFID 标签的超轻量级 RFID 双向认证协议，其安全性与效率较高。随着 EPCglobal C1 G2 标准的推广，国内外很多专家学者提出了基于 EPCglobal C1 G2 标准的 RFID 认证协议[7]，基于该标准的 RFID 认证协议的研究是下一步的工作方向。

参考文献

[1] 周永彬, 冯 登. RFID 安全协议的设计与分析[J]. 计算机学报, 2006, 29(4): 581-589.

[2] Chien H Y. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity[J]. IEEE Trans. on Dependable and Secure Computing, 2007, 4(4): 337-340.

[3] Li Tieyan, Deng R H. Vulnerability Analysis of EMAP: An Efficient RFID Mutual Authentication Protocol[C]//Proc. of ARES'07. Vienna, Austria: [s. n.], 2007.

[4] Cao Tianjie, Bertino E, Lei Hong. Security Analysis of the SASI Protocol[J]. IEEE Trans. on Dependable and Secure Computing, 2009, 6(1): 73-77.

[5] Hernandez-Castro J C, Tapiador J M E, Peris-Lopez P, et al. Cryptanalysis of the SASI Ultralightweight RFID Authentication Protocol[J]. IEEE Trans. on Dependable and Secure Computing, 2009, 6(4): 316-320.

[6] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. Advances in Ultralightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol[C]//Proc. of WISA'08. Jeju Island, Korea: [s. n.], 2008.

[7] 王益维, 赵跃华, 李晓聪. 基于 EPC-C1G2 标准的 RFID 认证机制[J]. 计算机工程, 2010, 36(18): 153-154.

编辑 顾姣健

(上接第 139 页)

参考文献

[1] 裴庆祺, 马建峰, 庞辽军, 等. 基于身份自证实的秘密共享方案[J]. 计算机学报, 2010, 33(1): 152-156.

[2] Benaloh J, Leichter J. Generalized Secret Sharing and Monotone Functions[C]//Advances in Cryptology-CRYPTO'88. Berlin, Germany: Springer-Verlag, 1988: 27-35.

[3] Ito M, Saito A, Nishizeki T. Secret Sharing Scheme Realizing General Access Structure[C]//Proceedings of IEEE Globecom'87. Tokyo, Japan: IEEE Press, 1987: 99-102.

[4] Hwang Shin-Jia, Chang Chin-Chen, Yang Wei-Pang. An Efficient Dynamic Threshold Scheme[J]. IEICE Transactions on Information and Systems, 1996, E79-D(7): 936-941.

[5] 申一迪, 张 威. 一般接入结构上的可自选子密钥的秘密共享方案[J]. 哈尔滨师范大学自然科学学报, 2008, 24(1): 45-47.

[6] 晋玉星, 茹秀娟. 一个新的广义秘密共享方案[J]. 计算机工程, 2009, 35(17): 155-156.

编辑 金胡考