基于标签编组的 RFID 相互认证协议

张学军,常 昆,王 玉
(南京邮电大学 电子科学与工程学院,江苏 南京 210003)

摘 要:探究了当前 RFID 安全认证协议中较少涉及的标签编组领域,分析了典型标签编组协议 Yoking Proof 的安全问题,提出了基于标签编组的 RFID 相互认证协议(MATG)。MATG 协议将同类标签进行编组,在协议相互认证过程中,阅读器能选择特定的标签组,并在一次协议过程中自动完成对组中所有标签的识别。对所提出协议的安全性进行了分析和 BAN 逻辑证明,并用 C 语言编程进行了重放攻击仿真。理论分析和仿真结果显示,MATG 协议克服了 Yoking Proof 协议的缺陷,提高了成组商品标签的识别效率和安全性。

关键词:射频识别技术;相互认证协议;标签编组;BAN 逻辑
中图分类号:TP391.45;TP309.2 **文献标识码**:A **文章编号**:1673-629X(2015)04-0102-06
doi:10.3969/j.issn.1673-629X.2015.04.024

An RFID Mutual Authentication Protocol Based on Tag Grouping

ZHANG Xue-jun, CHANG Kun, WANG Yu
(School of Electronic Science and Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Explore the tag grouping field less involved in current RFID security authentication protocol, Yoking Proof protocol's security problems are analyzed. An RFID Mutual Authentication protocol based on Tag Grouping (MATG) was proposed. The same tags are grouped by MATG, reader can select a group of tags in the mutual authentication process, and then identify targets automatically in a protocol processing. Safety of the proposed protocol is analyzed and proved with the BAN logic, and then attack simulation is performed using C programming language. Theoretic analysis and simulation results show that MATG protocol overcomes Yoking Proof protocol's shortcomings and improves working efficiency and safety when dealing with a group of tags.

Key words: radio frequency identification; mutual authentication protocol; tag grouping; BAN logic

0 引 言

RFID(Radio Frequency IDentification)是一种非接触式的自动识别技术,基本原理是利用射频信号自动识别目标对象并读写相关数据。这种技术具有识别过程无需人工干预、数据读取方便快捷、有效识别距离远、抗污染能力强的优点,在物流、跟踪、定位等领域得到了广泛应用。典型 RFID 系统包含标签(Tag)、阅读器(Reader)和后端数据库(Data Base),标签和阅读器通过无线信道传递信息,数据完全暴露在空气中,因此容易遭受外界攻击。为了保证用户的安全和隐私,各国专家积极研究基于加密算法的 RFID 安全协议。Ari Juels 提出了一种 Yoking Proof 协议(以下简称 YP 协议)[1],该协议可以使两个标签同时被认证,但是被证明无法抵御重放攻击[2]。

文中分析了 YP 协议存在的安全问题,提出了基于标签编组的 RFID 相互认证协议(RFID Mutual Authentication protocol based on Tag Grouping, MATG)。MATG 协议中阅读器能选择特定的一组标签,并在一次协议过程中自动完成对组中所有标签的识别。新提出的协议具有两种工作模式,组标签模式可以同时读写一组标签,单标签模式用于对单个标签读写。文中对所提出协议的安全性进行了分析和 BAN 逻辑证明,并用 C 语言编程进行攻击仿真。结果显示,MATG 克服了 YP 协议无法抵御重放攻击的缺陷,提高了对成组商品标签的识别效率,具有较高的实用性。

收稿日期:2014-06-12 **修回日期**:2014-09-17 **网络出版时间**:2015-02-23
基金项目:国家自然科学基金资助项目(61001077,61170276,61271334)
作者简介:张学军(1969-),男,教授,博士,研究方向为无线射频识别技术、通信网络的性能分析、流量控制、QoS 理论与技术;常 昆(1988-),男,硕士,研究方向为无线射频识别。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150223.1241.036.html

1　YP 协议及存在问题

YP 协议的核心思想是将一对标签的证言进行连接,最终在阅读器端完成认证,阅读器能够同时扫描一对标签,提高电子标签的读写效率,但是 YP 协议存在下述问题:

(1)YP 协议通过证言 P_{AB} 同时认证一对标签,如果其中一个标签被破坏,阅读器就判定认证的标签对无效。若将一对标签扩展为一组标签,则可能出现标签组中某个标签出错导致整组标签无法识别的情况,降低了同组其他合法标签的识别效率。

(2)协议中标签未对阅读器的合法性进行认证,一旦某个阅读器内部信息泄露,攻击者很容易伪造能够和标签进行会话的非法阅读器。

(3)文献[2]证明了 YP 协议无法抵御重放攻击。

2　标签编组相互认证协议(MATG)

2.1　标签工作模式定义

MATG 协议定义两种标签工作模式:组标签模式和单标签模式。组标签模式是指将一类商品的标签进行编组,阅读器在一次协议过程中读写组中所有标签,标签组之间用组编号识别[3-5]。针对 YP 协议只能同时认证两个标签的缺陷引入单标签模式,单标签模式下阅读器能够对特定目的标签进行读写操作[6]。MATG 协议中使用异或(⊕)、与(∧)、Hash 运算[7-8],下文所涉及标记符号的含义如表 1 所示。

表 1　符号说明

符号	含义
ID	标签标识符
K	标签密钥
M	掩码
GID	广播组编号
RGID	实际组编号
$H(m)$	对消息 m 进行 Hash 运算
r_d	数据库生成的随机数
r_i	标签 T_i 生成的随机数
ACK	标签更新完成确认消息
T_{max}	标签认证时间阈值

2.2　协议初始化

后端数据库中存储 $(ID_i, K_i, GID, M, RGID)$,其中广播组编号 GID、掩码 M、密钥 K 的值在每次认证过程中都会更新。数据库在协议过程中设立临时 buffer,用于缓存标签更新成功信息。数据库为每个标签保留两份表:$(ID_i, K_i, GID, M, RGID)_{old}$ 和 $(ID_i, K_i, GID, M, RGID)_{new}$,当标签 T_i 认证成功后,数据库删除对应 T_i 的 $(ID_i, K_i, GID, M, RGID)_{old}$。文中假设阅读器和后端数据库之间的信道是安全的。含有 8 个标签的标签组 GID 格式如图 1 所示,该格式满足组标签模式和单标签模式间的相互切换。标签 T_i 有 1 个独立的密钥值 K_i,内部存储 (ID_i, K_i, M)。标签具有随机数发生器,能够生成随机数,可以进行异或(⊕)、与(∧)、Hash 运算。

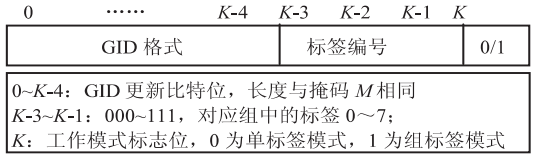

图 1　含 8 个标签的标签组 GID 格式

2.3　两种标签模式的认证过程

(1)组标签模式相互认证过程。

步骤 1:数据库唤醒标签,DB → R → T。

数据库确认需要唤醒的标签组,根据组中成员数目确定本轮协议需要唤醒的标签总数。数据库生成随机数 r_d,计算 $m_d = RGID \oplus M$,将 GID、m_d 和 r_d 经阅读器广播至标签。

标签利用本地保存的 M 计算 $RGID' = GID \wedge M$,$m_d' = RGID' \oplus M$。

标签比较 m_d 和 m_d',若相等,说明标签是应当被唤醒的标签组中成员。

标签根据 GID 末位的标志位判断本次协议工作模式,1 为组标签模式,0 为单标签模式。

步骤 2:标签认证数据库的合法性[9-10],DB → R → T_i。

以标签组中第 1 个标签 T_1 为例,数据库计算 $c_1 = H(RGID, ID_1, K_1, r_d)$,将 c_1 经阅读器发送至标签 T_1。

标签 T_1 收到 c_1 后,计算 $c_1' = H(RGID', ID_1, K_1, r_d)$。然后比较 c_1 和 c_1',若相等,说明数据库合法,否则发送 Fail 信号。

步骤 3:数据库认证标签的合法性,T_i → R → DB。

标签 T_1 确认数据库的合法性后产生随机数 r_1,计算 $t_1 = H(r_d, RGID', ID_1, K_1, r_1)$,将 t_1、r_1 经阅读器发送至数据库。

数据库收到 t_1、r_1 后,计算 $t_1' = H(r_d, RGID, ID_1, K_1, r_1)$。然后比较 t_1 和 t_1',若相等,说明标签 T_1 合法,否则拒绝 T_1。若 T_1 在规定时间内没有回送消息,数据库就认为本次协议失败。

步骤 4:更新广播组编号 GID,掩码 M 和标签密钥 K,DB → R → T。

数据库确认标签 T_1 的合法性后生成 k 位随机数 r_{d1}(假设 GID 除去末 n 位用于区分组中标签和工作模式后还剩余 k 位),计算 $GID_{new} = GID \oplus r_{d1}$,再计算 $M_{new} = M \oplus r_{d1}$,最终得 $RGID_{new} = GID_{new} \wedge M_{new}$。由于

M_{new} 和 GID_{new} 长度不同,在“与”的过程中,M_{new} 低位置 1,使其长度与 GID_{new} 长度相同。

数据库更新存储的标签密钥,计算 $K_{1new} = K_1 \oplus M_{new}$,然后计算更新消息 m_1,$m_1 = M_{new} \oplus r_1 \oplus M$($M$ 来自于 $(ID_1, K_1, GID, M, RGID)_{old}$),将 m_1 经阅读器发送至标签 T_1。

标签 T_1 收到 m_1 后,计算 $M'_{new} = m_1 \oplus M \oplus r_1$,再计算新的密钥值 $K'_{1new} = K_1 \oplus M'_{new}$。

步骤 5:标签发送更新完成确认消息,$T_i \rightarrow R \rightarrow DB$。

标签 T_1 完成信息更新后生成确认消息 ACK_1,将 ACK_1 经阅读器发送至数据库。

数据库收到 ACK_1 后,在 buffer 中保存“Y”,删除对应的 $(ID_1, K_1, GID, M, RGID)_{old}$,若在阈值 T_{max} 内没收到标签发送的 ACK,数据库在对应标签的 buffer 中保存“N”。

步骤 6:到达时间阈值 T_{max} 后,数据库开始认证下一个标签,对标签 T_i 重复步骤 2 至 5,由于同一组标签使用相同的 GID、M 和 RGID,所以一次协议过程中数据库内部的 GID、M 和 RGID 只更新一次。

组中所有标签完成响应后,数据库将 buffer 中的标签读写情况告知管理员。

(2)单标签模式相互认证过程。

单标签模式与组标签模式的不同之处在于该模式 1 次仅唤醒 1 个标签,组中其他成员都处于静默状态。为了使经过单标签模式认证的标签不会从原标签组中丢失,该工作模式不进行 GID、M 和 RGID 更新,认证结束后只更新标签密钥 K。

步骤 1:与组标签模式相同,标签先判断是否为应唤醒的标签组中成员,再根据 GID 的末 $n-1$ 位确定组中第 i 个标签 T_i 被唤醒,此时 GID 末位的工作模式标志位为 0。

步骤 2 ~ 3 与组标签模式相同。

步骤 4:数据库确认标签的合法性后更新标签密钥 K,计算 $K_{inew} = K_i \oplus r_i$。

步骤 5:标签确认数据库的合法性后,计算 $K_{inew} = K_i \oplus r_i$,然后生成确认消息 ACK_i,将 ACK_i 经阅读器发送至数据库。

数据库收到 ACK_i 后,在 buffer 中保存“Y”,删除对应的 $(ID_i, K_i, GID, M, RGID)_{old}$,若在阈值 T_{max} 内没收到标签发送的 ACK,在对应标签的 buffer 中保存“N”。

3 MATG 协议安全性及性能分析

3.1 安全性分析

MATG 协议与其他协议安全性比较如表 2 所示。

表 2 五种认证协议安全性比较

协议	重放攻击	跟踪攻击	去同步攻击	认证方式	密钥更新
YP[2]	no	no	yes	单向	有
Hash-Lock	no	no	no	单向	无
Hash Chain[11]	no	yes	no	单向	无
LMAP++[12]	yes	no	no	双向	有
MATG	yes	yes	yes	双向	有

注:“yes”表示可以抵御攻击,“no”表示无法抵御。

本节主要对 MATG 协议抵御重放攻击、跟踪攻击、去同步攻击的安全性进行分析。

(1)重放攻击(reply attack)。

为了抵御重放攻击,MATG 协议在组标签模式更新 GID,两种工作模式的步骤 2、3 利用数据库生成随机数 r_d 区分不同认证回合,标签 T_i 生成随机数 r_i 区分组中的不同标签。组标签模式步骤 4 中更新密钥 K_{new} 由更新后的掩码 M_{new} 生成,单标签模式中 K_{new} 的生成利用了标签随机数 r_i。因为每一回合协议都更新标签密钥 K_i 以及掩码 M,所以即使本回合的标签密钥 K_i 以及掩码 M 被攻击者获知,攻击者也无法在下一回合协议过程中伪装成合法标签。不同标签在不同回合使用的更新完成确认消息 ACK 值也不相同,ACK 的独立性可以有效抵御重放攻击。

(2)跟踪攻击(tracking attack)。

跟踪攻击是指攻击者伪装成合法阅读器不断向标签发送认证请求,根据不同标签响应的独特性确定目的标签的运动轨迹。MATG 协议中标签的响应信息不包含自身 ID 信息,组标签模式下标签合法性认证从 $T_1 \sim T_n$ 自动运行(在一个标签认证时间到达阈值 T_{max} 后,数据库自动开始下一个标签的认证)。由于攻击者无法确定这些响应来自某一个确定标签,因此无法对标签实施跟踪。

(3)去同步攻击(de-synchronization attack)。

去同步攻击是指由于攻击者截断数据库与标签之间的更新信息,造成数据库中存储的标签信息和标签实际存储的信息不一致,在下一轮认证过程中合法标签无法被读取[11]。去同步攻击主要发生在步骤 4、5,若攻击者截断步骤 4,造成数据库中信息更新,而实际上标签信息未更新;若攻击者截断步骤 5,当等待 ACK 时长超过阈值 T_{max} 时数据库认为标签认证失败,而实际上标签已完成了信息更新。管理员可以根据数据库 buffer 中保存的标签认证情况进行标签和数据库的再同步。在单标签模式下管理员分别用 $(ID_i, K_i, GID, M, RGID)_{old}$ 和 $(ID_i, K_i, GID, M, RGID)_{new}$ 扫描认证失败的标签 T_i,若标签响应 GID_{old} 表明上一轮标签信息

更新失败,管理员在单标签模式认证成功后将 $(\mathrm{ID}_i, K_i, GID, M, \mathrm{RGID})_{\mathrm{new}}$ 中的 M_{new} 和 K_{new} 写入标签。若标签响应 $\mathrm{GID}_{\mathrm{new}}$ 表明上一轮信息更新成功,管理员删除后端数据库中对应标签的 $(\mathrm{ID}_i, K_i, \mathrm{GID}, M, \mathrm{RGID})_{\mathrm{old}}$[12-13]。

3.2 性能分析

下面从计算开销、存储开销和通信开销三个方面对 MATG 协议的性能进行分析,并与 YP 协议比较。

1)计算开销。

MATG 协议中使用了 Hash 函数、异或(⊕)、与(∧)等运算,一次协议过程中标签需要进行 1 次"与"操作,2 次 Hash 运算,4 次"异或"。协议将计算量较大的 Hash 运算用于标签和数据库的相互认证,而计算量较小的"与"和"异或"用于标签的唤醒和密钥、掩码的更新。YP 协议中,一对标签一次协议过程中需要进行 6 次 Hash 运算,2 次加法运算。MATG 协议与 YP 协议相比,减少了 4 次复杂的 Hash 运算,节省了计算开销[14]。

2)存储开销。

为了防止去同步攻击,在数据库中保留认证失败标签所对应的 $(\mathrm{ID}_i, K_i, \mathrm{GID}, M, \mathrm{RGID})_{\mathrm{old}}$,用于管理员对标签的再同步。标签认证成功后,数据库删除对应的 $(\mathrm{ID}_i, K_i, \mathrm{GID}, M, \mathrm{RGID})_{\mathrm{old}}$,节省存储开销。

3)通信开销。

MATG 协议执行过程中共需要传递 5 次信息,其中 1 次用于唤醒标签,2 次用于标签和阅读器的相互认证,1 次用于密钥和掩码的更新,1 次用于标签信息更新确认。假设一个标签组具有 n 个标签,MATG 协议一次就可唤醒组所有标签,而 YP 协议完成一对标签认证的通信次数为 6,若要唤醒 n 个标签,阅读器和标签需要通信 n 次。

4)特性。

MATG 协议在性能方面具有下述优越性。

(1)自动性:对一类商品进行识别时只需启动一次协议,不需要人工逐个唤醒每个标签,大大减少了使用者的工作量。标签组在完成一次认证后,可以将组中所有错误标签的信息同时通知管理员,与单标签认证相比,MATG 协议减少了管理员的工作量。

(2)防碰撞性:组编号的设计使唤醒标签阶段只有组中成员才响应,降低了无关标签的干扰,广播组编号 GID 长度远远小于标签 ID 长度,不同标签组之间的碰撞概率较低。

(3)可扩展性:MATG 协议中阅读器没有计算量,因此可以在阅读器上增加算法和存储空间,实现阅读器和数据库的相互认证。在此基础上可将 MATG 扩展为移动的 RFID 相互认证协议。

4 MATG 协议安全性证明

为了证明后端数据库与标签能够相互信任对方传输的合法信息,本节运用 BAN 逻辑证明 MATG 协议的逻辑安全性[15]。因为在 MATG 协议中阅读器只起到传递信息的作用,所以对该协议的逻辑证明可以抽象为后端数据库与标签之间的逻辑证明。

4.1 建立 BAN 逻辑初始假设

(1)标签 T_i 成立的初始条件。

$T_i \mid \equiv \#\mathrm{ID}_i, T_i \mid \equiv \#r_i, T_i \mid \equiv \#M,$

$T_i \mid \equiv \overset{K_i}{\leftrightarrow} \mathrm{DB}, T_i \mid \equiv \overset{M}{\leftrightarrow} \mathrm{DB}$

(2)数据库 DB 成立的初始条件。

$\mathrm{DB} \mid \equiv \#r_{\mathrm{d}}, \mathrm{DB} \mid \equiv \mathrm{DB} \overset{K_i}{\leftrightarrow} T_i, \mathrm{DB} \mid \equiv \mathrm{DB} \overset{M}{\leftrightarrow} T_i$

4.2 建立理想化协议模型

明文传输的消息以及不涉及逻辑分析的语句对协议逻辑属性的分析不起作用,将安全协议模型简化,写成 BAN 逻辑语言:

$\mathrm{M}_1: T_i \lhd \mathrm{DB}: \{\mathrm{RGID}\}_M$

$\mathrm{M}_2: \mathrm{DB} \lhd T_i: \{r_{\mathrm{d}}, \mathrm{RGID}', \mathrm{ID}_i, K_i, r_i\}_K$

$\mathrm{M}_3: T_i \lhd \mathrm{DB}: \{M_{\mathrm{new}}, r_i\}_M$

4.3 预期目标

目标 1: $T_i \mid \equiv \mathrm{DB} \sim \#(\mathrm{RGID})$

目标 2: $\mathrm{DB} \mid \equiv T_i \sim \#(\mathrm{ID}_i)$

目标 3: $T_i \mid \equiv \mathrm{DB} \sim \#(M_{\mathrm{new}})$

4.4 协议证明

(1)证明 $T_i \mid \equiv \mathrm{DB} \sim \#(\mathrm{RGID})$。

由标签初始条件和 M_1 可知 $T_i \mid \equiv \overset{M}{\leftrightarrow} \mathrm{DB} \wedge T_i \lhd \{\mathrm{RGID}\}_M$

由消息含义规则可得:

$$\frac{T_i \mid \equiv T_i \overset{M}{\leftrightarrow} \mathrm{DB} \wedge T_i \lhd \{\mathrm{RGID}\}_M}{T_i \mid \equiv \mathrm{DB} \mid \sim \mathrm{RGID}}$$

所以有:

$$T_i \mid \equiv \mathrm{DB} \mid \sim \mathrm{RGID} \tag{1}$$

由标签初始条件可知: $T_i \mid \equiv \#M$,因此 $T_i \mid \equiv \#\{\mathrm{GID}\}_M$,即

$$T_i \mid \equiv \#\mathrm{RGID} \tag{2}$$

根据式(1)、(2)可得 $T_i \mid \equiv \mathrm{DB} \sim \#(\mathrm{RGID})$,目标 1 得证。

(2)证明 $\mathrm{DB} \mid \equiv T_i \sim \#(\mathrm{ID}_i)$。

由数据库初始条件可知: $\mathrm{DB} \mid \equiv \#r_{\mathrm{d}}$,根据新鲜性规则可得: $\dfrac{\mathrm{DB} \mid \equiv \#(r_{\mathrm{d}})}{\mathrm{DB} \mid \equiv \#(r_{\mathrm{d}}, \mathrm{ID}_i)}$,所以

$$\mathrm{DB} \mid \equiv \#(r_{\mathrm{d}}, \mathrm{ID}_i) \tag{3}$$

由数据库初始条件和 M_2 可知

$\mathrm{DB} \mid \equiv \mathrm{DB} \overset{K_i}{\leftrightarrow} T_i$

由消息含义规则可得

$$\frac{\mathrm{DB} \mid \equiv \mathrm{DB} \overset{K_i}{\leftrightarrow} T_i \ \wedge \ T_i \lhd \{r_\mathrm{d}, \mathrm{RGID}', \mathrm{ID}_i, r_i\}_{K_i}}{\mathrm{DB} \mid \equiv T_i \mid \sim (r_\mathrm{d}, \mathrm{RGID}', \mathrm{ID}_i, r_i)}$$

所以 $\mathrm{DB} \mid \equiv T_i \mid \sim (r_\mathrm{d}, \mathrm{RGID}', \mathrm{ID}_i, r_i)$。

由发送规则可得

$$\frac{\mathrm{DB} \mid \equiv T_i \mid \sim (r_\mathrm{d}, \mathrm{RGID}', \mathrm{ID}_i, r_i)}{\mathrm{DB} \mid \equiv T_i \mid \sim (\mathrm{ID}_i)}$$，所以

$$\mathrm{DB} \mid \equiv T_i \mid \sim (\mathrm{ID}_i) \tag{4}$$

根据式(3)、(4)可得 $\mathrm{DB} \mid \equiv T_i \sim \#(\mathrm{ID}_i)$，目标 2 得证。

(3)证明 $T_i \mid \equiv \mathrm{DB} \sim \#(M_\mathrm{new})$。

由标签初始条件和 M_3，根据消息含义规则可得

$$\frac{T_i \mid \equiv T_i \overset{M}{\leftrightarrow} \mathrm{DB} \wedge \ T_i < \{M_\mathrm{new}, r_i\}_M}{T_i \mid \equiv \mathrm{DB} \mid \sim (M_\mathrm{new}, r_i)}$$

根据发送规则可得：

$$T_i \mid \equiv \mathrm{DB} \sim M_\mathrm{new} \tag{5}$$

由标签初始条件可知 $T_i \mid \equiv \#r_i$，根据新鲜性规则可得

$$T_i \mid \equiv \#(M_\mathrm{new}, r_i) \tag{6}$$

根据式(5)、(6)可得 $T_i \mid \equiv \mathrm{DB} \sim \#(M_\mathrm{new})$，目标 3 得证。

由上述分析可见 MATG 协议达到了逻辑证明的目标，具有一定的安全性。

5 MATG 协议攻击仿真

本节利用 C 语言编程对 MATG 协议进行重放攻击仿真，并将仿真结果与现有安全协议比较，验证了 MATG 协议对重放攻击的抵御能力。

5.1 逐次重放攻击

由 MATG 协议流程可知，重放攻击主要发生在标签和数据库完成相互认证之前，此时标签和数据库均未产生随机数保证传输数据的安全性。攻击者可能截取上一轮协议过程中步骤 1 的数据，在本轮协议起始阶段进行重放攻击，达到唤醒合法标签的目的。文中对 MATG 协议的组标签模式和单标签模式步骤 1 进行重放攻击仿真，仿真流程如图 2 所示。

为了方便观察，重放攻击仿真时数值的输入输出均为十六进制。假设标签 ID 长度为 32 bit，前 24 bit 用于相互认证和信息更新，后 8 bit 代表标签在所属标签组中的编号，为了使标签不会从标签组中丢失，最后 8 bit 的值始终不变。

文中进行了 1 000 回合逐次重放攻击，每次重放攻击中攻击者获得上一轮协议密钥值，以此计算上一轮 m_d，而标签根据本地密钥值计算本轮协议 m_d'，标签将两个值相互比较，若相等则攻击成功。实际仿真时，在 1 000 回合逐次重放攻击中标签均能识别非法攻击。继续加大循环，逐次重放攻击的次数到 10^7 次，当攻击成功时跳出循环体，累计攻击总次数；当攻击总次数超过 10^7 次时，跳出循环体结束攻击。实验证明，在 10^7 次循环逐次重放攻击中，攻击成功次数为 0。说明 MATG 协议能够成功抵逐次重放攻击。

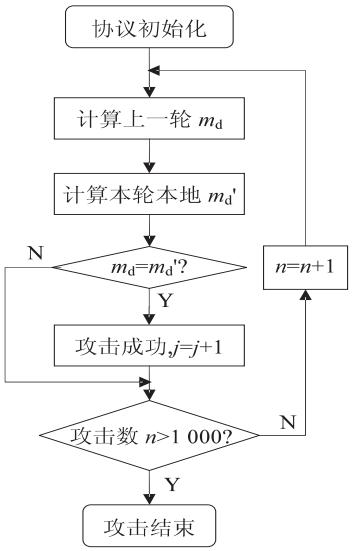

图 2 逐次重放攻击流程图

5.2 存储多值的重放攻击

攻击者有可能将多轮协议的数据窃听、存储，然后将存储的大量数据依次重放，因此需要探讨标签生成的本地值与之前多轮协议数据相等的可能性。文中在仿真时建立一个二维数组存储前 k 轮的 m_d 值。例如：第 2 轮标签生成的 m_d' 与第 1 轮的 m_d 比较，第 3 轮标签生成的 m_d' 分别与第 1 轮和第 2 轮的 m_d 比较，以此类推，第 k 轮标签生成的 m_d' 分别与前 n 轮的 m_d 比较(n = 1,2,…,k − 1)，仿真流程如图 3 所示。

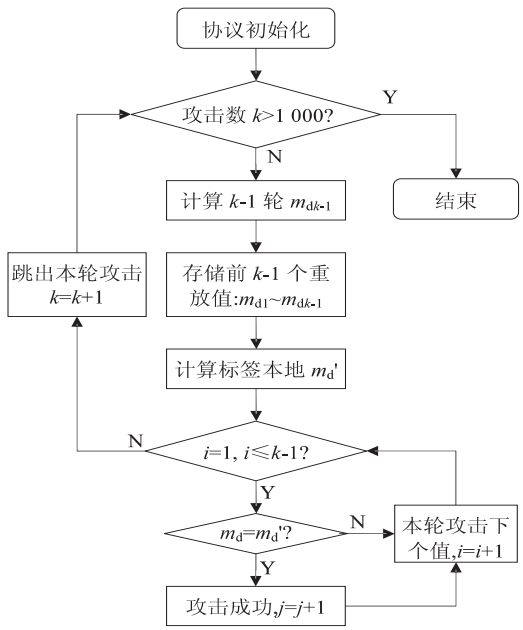

图 3 存储多值的重放攻击流程图

为了验证 MATG 协议在存储多值重放攻击中的安全性,文中增加数据存储量,存储前 1 000 轮 m_d 值进行重放攻击,攻击总次数达到 500 500 次,MATG 协议攻击成功率与文献[16]中相关安全协议攻击成功率的比较如表 3 所示。

表 3　不同安全协议的攻击成功率比较

协议名称	攻击数	攻击成功数	攻击成功率
Hash-Lock	28 659	11 575	0.403 887 086
随机 Hash-Lock	13 076	3 247	0.248 317 528
Hash Chain	21 337	2 630	0.123 260 065
LCAP	20 831	132	0.006 336 71
MATG	500 500	1 947	0.003 890 109

仿真结果表明,在逐次重放攻击中 MATG 协议具有很好的安全性,能够有效抵御 10^7 次逐次重放攻击,在存储多值的重放攻击中 MATG 协议与现有安全协议相比具有较低的攻击成功率。

6　结束语

文中在 YP 协议基础上提出了 MATG 协议,新协议提供了组标签和单标签两种认证模式。组标签模式适合对一类商品同时识别,而单标签模式可识别一个特定的标签,两种模式给使用者提供了更多的选择,同时也提高了系统的识别效率。文中对 MATG 协议进行理论分析和逻辑证明,并对 MATG 协议进行了重放攻击仿真,理论分析和仿真结果显示,新协议与现有安全协议相比安全性更高、性能更优越。

参考文献:

[1] Juels A. "yoking-proofs" for RFID tags[C]//Proc of second IEEE annual conference on pervasive computing and communication workshops. [s. l.]:IEEE,2004:138-143.

[2] Cho J S,Yeo S S,Hwang S,et al. Enhanced yoking proof protocols for RFID tags and tag groups[C]//Proc of 22nd international conference on advanced information networking and applications. Okinawa:IEEE,2008:1591-1596.

[3] Leng Xuefei, Lien Y H, Mayes K, et al. Select - response grouping proof for RFID tags[C]//Proc of first Asian conference on intelligent information and database systems. Dong hoi:IEEE Computer Society,2009:73-77.

[4] Piao Chunhui, Fan Zhenjiang, Yang Chunyan, et al. Research on RFID security protocol based on grouped tags and re-encryption scheme[C]//Proc of IEEE international conference on wireless communications, networking and information security. Beijing:IEEE,2010:568-572.

[5] 张学军,王绪海,蔡文琦. 基于分组码的改进型防碰撞算法研究[J]. 计算机应用研究,2012,29(11):4265-4268.

[6] Rahman M S, Soshi M, Miyaji A. A secure RFID authentication protocol with low communication cost[C]//Proc of IEEE international conference on complex, intelligent and software intensive systems. Fukuoka:IEEE,2009:559-564.

[7] Chien H Y. SASI:a new ultralight-weight RFID authentication protocol providing strong authentication and strong integrity [J]. IEEE Transactions on Dependable and Secure Computing,2007,4(4):337-340.

[8] 张学军,陈彦君,常　昆. 改进型 RFID 相互认证协议研究[J]. 计算机技术与发展,2013,23(8):129-132.

[9] 刘　一,卫宏儒,潘　伟. 低成本 RFID 双向认证协议[J]. 计算机应用,2013,33(A01):130-133.

[10] 张　顺,陈海进. 一种抗恶意攻击的 RFID 双向认证协议[J]. 计算机工程与应用,2012,48(25):112-117.

[11] 曹　峥,马建峰,杨　林,等. RFID 安全协议的数据去同步化攻击[J]. 华中科技大学学报:自然科学版,2013,41(4):65-69.

[12] Cho C H, Do K H, Kim J W, et al. Design of RFID mutual authentication protocol using time stamp [C]//Proc of 2009 fourth international conference on computer sciences and convergence information technology. [s. l.]:[s. n.],2009:1047-1051.

[13] Safkhani M, Bagheri N, Naderi M, et al. Security analysis of LMAP++, an RFID authentication protocol[C]//Proc of international conference on internet technology and secured transactions. Abu Dhabi:IEEE,2011:689-694.

[14] 张学军,王　玉,王锁萍,等. 基于循环移位的轻量型相互认证协议研究[J]. 电子学报,2012,40(11):2270-2275.

[15] 卿斯汉. 安全协议的设计与逻辑分析[J]. 软件学报,2003,14(7):1300-1309.

[16] 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.

基于标签编组的RFID相互认证协议

作者： 张学军， 常昆， 王玉， ZHANG Xue-jun， CHANG Kun， WANG Yu
作者单位： 南京邮电大学 电子科学与工程学院,江苏 南京,210003
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(4)