·安全技术· 文章编号:1000-3428(2017)10-0126-08 文献标志码:A 中图分类号:TP309

一种安全的 RFID 委托认证方案

周由胜,李 缘

(重庆邮电大学 计算机科学与技术学院,重庆 400065)

摘 要: 针对智能家居中的事务委托场景,提出一种安全的委托认证方案,基于切比雪夫混沌映射分别构造适用于通用场景及委托场景的认证协议。考虑到切比雪夫映射的半群特性,所有标签与门禁阅读器共享唯一的认证服务器公钥,即可实现各实体之间的相互认证,解决了公钥密码认证方案中密钥管理繁琐的难题。利用 BAN 逻辑对所提方案正确性进行验证,并分析方案的安全性,结果表明,该方案安全可行,可以抗重放攻击和假冒攻击。

关键词: 射频识别;混沌映射;认证;委托;BAN 逻辑

中文引用格式: 周由胜,李 缘. 一种安全的 RFID 委托认证方案[J]. 计算机工程,2017,43(10):126-133.

英文引用格式: ZHOU Yousheng, LI Yuan. A Secure RFID Delegation Authentication Scheme [J]. Computer Engineering,2017,43(10):126-133.

A Secure RFID Delegation Authentication Scheme

ZHOU Yousheng, LI Yuan

(College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

【Abstract】 Aiming at the situation of delegation in smart home, a secure authentication scheme is proposed, which constructs authentication protocols for general scene and delegation scene based on Chebeshev chaotic mapping. Since the Chebeshev chaotic mapping owns the semi-group property, only one public key of the trusted server is shared with all tags and readers to achieve mutual authentication between the entities, and the heavy key management is avoided which lies in the traditional public key based authentication. The correctness of the proposed scheme is verified by using the BAN logic, and the security is analyzed as well. Analysis results show that the proposed scheme is correct and secure, it can resist relay attacks and impersonation attacks.

【Key words】 Radio Frequency Identification(RFID); chaotic mapping; authentication; delegation; BAN logic

DOI: 10.3969/j.issn.1000-3428.2017.10.022

0 概述

随着科技技术的不断发展以及人们生活水平的不断提高,智能家居[1-3]受到人们越来越多的追捧。智能家居的应用越来越多样化,其采用的技术也是各种各样的,包括 Zigbee[4],PLC[5],RFID[6]等,其中以 RFID 最为普遍。例如,文献[7]提出一种利用 RFID 技术对老年人在家中的位置进行追踪,然后分析老人的健康状况的方法。当判断出老人的健康可能出现问题时,会及时通知其家人和医疗人员。文献[8]提出一种利用 RFID 技术对水压变化进行监控,然后分析是否有漏水情况产生的方法,当分析到家里可能出现漏水情况时发出警告以节约水资源。文献[9]提出一种基于 RFID 技术的手势识别[10]。文献[11]提出一种基于 RFID 技术的智能冰箱的概念,它用于帮助人们管理冰箱中的食物和准确地定位食物在冰箱中的位置。文献[12]提出一种利用 RFID 技术的提醒系统,当系统检测到用户出门的时候忘记带了某种物品,该系统就会提醒用户。文献[13]提出一种利用 RFID 技术的智能冰箱的概念,该冰箱能识别内部的食物,并从营养学的角度对下一餐该食用哪种食物提出建议。当冰箱空时,会打印一个益于用户健康的食物清单。文献[14]提出一种利用传感器系统和 RFID 技术对房间空气进行监控和调整的方法。

将 RFID 技术用于门禁系统[15-16],不仅可以使用户省去传统钥匙开锁中的使用繁琐以及维护不便,而且可以解决传统机械门锁所不能解决的问题。例如,当某个用户(A)在外出差或者旅游期间因无法按期返回,需要委托他人(B)进入其家中完成某些任务,如喂

基金项目: 国家社会科学基金(14CTQ026);重庆市自然科学基金(2014jcyjA-40028)。

作者简介: 周由胜(1979—),男,副教授、博士,主研方向为网络与信息安全;李 缘,硕士研究生。

收稿日期: 2016-08-05 **修回日期:** 2016-10-19 **E-mail:** youshengzhou@foxmail.com

养宠物等。由于事发突然,A 并未事先将钥匙交于 B,因此 B 除破门而入外无其他更便利的方法进入 A 的家中并完成委托事务。所以,传统的基于机械锁门显然无法满足该需求,但采用 RFID 技术的门禁系统可以解决该问题。一种可能的方法是通知控制中心(如物业管理中心)为 B 开门,但这种委托方式风险较大,一方面是控制中心并非完全可信,事先设定其具有开门权限具有一定的安全隐患;另一方面,一旦控制中心遭受黑客恶意攻击,那么所有居民财产安全将受到严重威胁,所以这种方式并不可取。因此,本文提出一种用户自主授权的安全委托方式,具体如下:在没有任何委托事务产生之前,用户 A,B 只能通过持自己的标签 Tag-A,Tag-B 才能打开各自的家门。当用户 A 需要远程委托用户 B 进入其家中完成某项事务时,A,B 之间必须首先执行如下委托认证过程,然后 B 才能凭借 Tag-B 进入 A 的家中:1) A 需要向 B 获取其标签 Tag-B 的信息;2)B 把 Tag-B 身份信息告知 A;3)A 向智能家居服务商(可信第三方)发送对 B 的委托信息,服务商收到该消息之后,先验证其有效性,如果验证成功,将存储委托信息;4)B 通过 Tag-B 向 A 的门禁 Reader-A 发起访问;5)Reader-A发送信息给可信第三方以进行对 Tag-B 的验证;6)可信第三方将验证结果返回给 A 的门禁 Reader-A,若验证通过,则 A 的门禁放行 B。

本文介绍混沌映射的基础知识及方案的具体构造过程,并对方案的安全性进行分析。

1　基础知识

由于本文所提认证的方案是基于切比雪夫混沌映射构造,为便于理解,首先介绍切比雪夫混沌映射[17-20]的定义及相关知识。

定义 1　T_n(切比雪夫多项式)是一个循环定义:$T_n(x)=2xT_{n-1}(x)-T_{n-2}(x)$,$n\geqslant 2$,$n\in\mathbb{N}$,$x\in\mathbb{R}$,其中,$T_0(x)=1$;$T_1(x)=x$。

定义 2　T_n(扩展的切比雪夫多项式)仍然是一个循环的定义,与定义 1 稍有不同,它的定义如下:$T_n(x)=2xT_{n-1}(x)-T_{n-2}(x)(\mathrm{mod}\ p)$,$n\geqslant 2$,$n\in\mathbb{N}$,$x\in\mathbb{R}$,其中,$T_0(x)=1$;$T_1(x)=x$。

定义 3(半群性质[18])　切比雪夫多项式 T_n 有如下半群性质:$T_a(T_b(x))=T_b(T_a(x))=T_{ab}(x)\ \mathrm{mod}\ p$,$a\in\mathbb{N}$,$b\in\mathbb{N}$,$p\in\mathbb{N}^*$。

定义 4(DLP 问题[19])　DLP 问题是对于给定的 x 和 y,不可能找到一个整数 a,使得等式 $T_a(x)=y$ 成立。

定义 5(DHP 问题[20])　对于已知的 $T_a(x)$ 和 $T_b(x)$,在不知道 a,b 的情况下是无法计算出 $T_{ab}(x)$ 的值的。

2　本文方案

如前所述,虽然目前已有一些基于 RFID 的门禁方案[15-16]以及基于混沌映射的 RFID 认证方案[17],但这些方案都无法满足事务委托认证场景,鉴于此,本文设计了一种非委托的 RFID 认证协议,用于智能家居中不需要委托的通用认证场景,称作普通认证;在此基础上,针对事务委托场景提出了一种委托认证协议。本文方案基于切比雪夫混沌映射设计,方案优势在于用户可以远程完成事务委托,而且由于混沌映射的半群特性,使得系统无需承载传统公钥密码认证的密钥管理任务,系统开销大大降低。

本文方案包括普通认证和委托认证 2 个过程,而委托认证过程包括委托阶段和委托之后的认证阶段,即如图 1 所示的步骤。

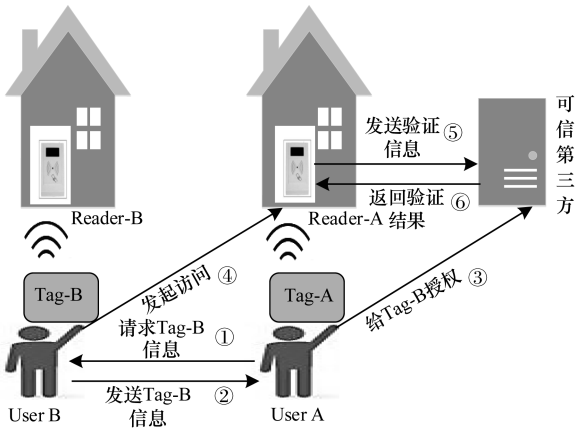

图 1　应用场景图

2.1　系统初始化

在初始化阶段,可信第三方选择 2 个随机数 r 和 s。然后可信第三方计算 $T_S=T_s(r)\ \mathrm{mod}\ p$。参数 (T_S,r,p) 和 s 将分别成为可信第三方的公钥和私钥。门禁阅读器和标签将会分别和可信第三方建立共享口令。标签、阅读器和可信第三方将会存储一些必要的信息。每个标签将会存储一个二元组 (ID_{Tg},PW_{Tg}),其中,ID_{Tg} 是标签自己的身份;PW_{Tg} 是它和可信第三方的共享口令。门禁阅读器会存储一个二元组 (ID_{Rd},PW_{Rd}),其中,ID_{Rd} 是它自己的身份;PW_{Rd} 是它和可信第三方的共享口令。对于可信第三方,它会为每个标签存储一个三元组 $(ID_{Tg},ID_{Rd},PW_{Tg})$,其中,$ID_{Tg}$ 是标签的身份;ID_{Rd} 是该标签对应的拥有者阅读器的身份;PW_{Tg} 是该标签和可信第三方的共享口令。除此之外,可信第三方还会为每一个阅读器存储一个二元组 (ID_{Rd},PW_{Rd}),其中,ID_{Rd} 为该阅读器的身份;PW_{Rd} 是阅读器和可信第三方之间的共享口令。

接下来将介绍普通认证和委托认证 2 个过程的具体步骤。这 2 个过程中的一些相关符号如表 1 所示。

表 1 符号定义

符号	含义
ID_{Tg_A}, ID_{Tg_B}	Tag-A 的身份和 Tag-B 的身份
PW_{Tg_A}, PW_{Tg_B}	Tag-A 和 Tag-B 分别与可信第三方的共享口令
ID_{Rd_A}, PW_{Rd_A}	Reader-A 的身份以及其可信第三方的共享口令
(T_S, r, p)	可信第三方公钥
s	可信第三方私钥
$h()$	单向哈希函数
Δt	一个特定的时间范围
$\oplus$	异或操作
$\|\|$	连接操作

2.2 普通认证

普通认证是指 Tag-A 与其拥有者阅读器 Reader-A、Tag-B 与 其拥有者阅读器 Reader-B 这类的认证。下面以 Tag-A 与 Reader-A 的认证为例进行说明。

第 1 步 Tag-A 首先生成一个随机数 x_{Tg}，然后计算 $T_{Tg} = T_{x_{Tg}}(r) \bmod p$，$K_{TS} = T_{x_{Tg}}(T_S) \bmod p$，$ID'_{Tg\_A} = ID_{Tg\_A} \oplus K_{TS}$，$h_{Tg} = h(ID_{Tg\_A} \| PW_{Tg\_A} \| t_{Tg} \| T_{Tg})$，其中 t_{Tg} 是标签的当前时间戳，接着标签发送 $M_{Tg} = \{h_{Tg}, t_{Tg}, T_{Tg}, ID'_{Tg\_A}\}$ 给阅读器。

第 2 步 收到 M_{Tg} 之后，阅读器 Reader-A 首先检验不等式 $(t_{Rd} - t_{Tg}) \leqslant \Delta t$ 是否成立（t_{Rd} 为阅读器的当前时间戳），如果成立，阅读器将生成一个随机数 x_{Rd}，然后计算 $T_{Rd} = T_{x_{Rd}}(r) \bmod p$，$K_{RS} = T_{x_{Rd}}(T_S) \bmod p$，$ID'_{Rd\_A} = ID_{Rd\_A} \oplus K_{RS}$，$h_{Rd} = h(ID_{Rd\_A} \| PW_{Rd\_A} \| t_{Rd} \| T_{Rd})$，接着阅读器发送 $M_{Rd} = \{h_{Rd}, t_{Rd}, T_{Rd}, ID'_{RD\_A}\}$，$M_{Tg}$ 给可信第三方。

第 3 步 当收到 M_{Rd}，M_{Tg} 之后，可信第三方首先检验不等式 $(t_S - t_{Tg}) \leqslant \Delta t$，$(t_S - t_{Rd}) \leqslant \Delta t$ 是否成立。如果不等式成立，那么可信第三方计算 $K'_{TS} = T_s(T_{Tg}) \bmod p$，$K'_{RS} = T_s(T_{Rd}) \bmod p$，$ID''_{Tg\_A} = ID'_{Tg\_A} \oplus K'_{TS}$，$ID''_{Rd\_A} = ID'_{Rd\_A} \oplus K'_{RS}$。然后根据 ID''_{Tg_A} 到它的存储单元里找到对应的 PW_{Tg_A}，并计算 $h'_{Tg} = h(ID''_{Tg\_A} \| PW_{Tg\_A} \| t_{Tg} \| T_{Tg})$。接着比较 h'_{Tg}，h_{Tg}，如果它们相同，那么标签的身份就被可信第三方认证通过。同理验证阅读器的身份。如果两者的身份都被验证通过，可信第三方根据 ID''_{Tg_A} 在存储的元组 $(ID_{Tg}, ID_{Rd}, PW_{Tg})$ 中找到对应的 ID_{Rd}，将其与 ID''_{Rd_A} 比较。如果相等，那么可信第三方就知道该阅读器是该标签的拥有者。在这里，显然相等，于是可信第三方知道该标签是对应于该阅读器的标签。然后可信第三方计算：

$$h_{Ts_1} = h(K'_{RS} \| T_{Tg} \| Own)$$
$$h_{Ts_2} = h(K'_{TS} \| T_{Rd} \| Own)$$
$$M_{Ts1} = \{h_{Ts_1}, T_{Tg}, Own\}$$
$$M_{Ts2} = \{h_{Ts_2}, T_{Rd}, Own\}$$

其中，Own 表示该阅读器是标签的拥有者。可信第三方发送 M_{Ts1}，M_{Ts2} 给阅读器。

第 4 步 收到 M_{Ts1}，M_{Ts2} 之后，阅读器 Reader-A 计算 $h'_{Ts_1} = h(K_{RS} \| T_{Tg} \| Own)$，将其与 h_{Ts_1} 比较。如果相等，阅读器知道标签被可信第三方认证成功。接着它把 M_{Ts2} 发送给标签。阅读器计算 $K = T_{x_{Rd}}(T_{Tg})$ 作为和标签的会话密钥。

第 5 步 标签收到 M_{Ts2} 之后，首先计算 $h'_{Ts_2} = h(K_{TS} \| T_{Rd} \| Own)$，将其与 h_{Ts_2} 比较。如果两者相等，那么标签就知道被可信第三方认证成功，接着标签计算 $K' = T_{x_{Tg}}(T_{Rd})$ 作为和阅读器的会话密钥。这个操作完成之后，标签和阅读器的相互认证就完成了。

2.3 委托认证

委托认证由 2 个阶段组成，即委托阶段与认证阶段，具体如下所示。

1）委托阶段

委托阶段如图 2 所示，在该阶段进行之前默认图 1 的第 1 步操作和第 2 步操作已经完成，即 A 已经取得 Tag-B 的身份信息。

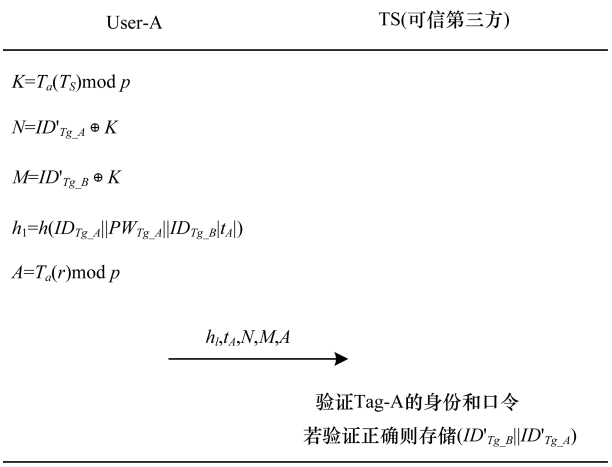

图 2 用户 A 对 Tag-B 的委托阶段

委托阶段具体步骤如下：

第 1 步 A 选取随机数 a，计算 $K = T_a(T_S) \bmod p$，然后计算 $N = ID_{Tg\_A} \oplus K$，$M = ID_{Tg\_B} \oplus K$，$h_1 = h(ID_{Tg\_A} \| PW_{Tg\_A} \| ID_{Tg\_B} \| t_A)$，$A = T_a(r) \bmod p$，其中 ID_{Tg_A}，PW_{Tg_A} 是 Tag-A 的身份和口令，t_A 为时间戳。ID_{Tg_B} 为 Tag-B 的身份。然后发送 h_1，t_A，N，M，A 给可信第三方。

第 2 步 可信第三方收到信息之后，计算 $K' = T_s(A) \bmod p$，$ID'_{Tg\_A} = N \oplus K'$，$ID'_{Tg\_B} = M \oplus K'$，然后根据 ID'_{Tg_A} 到数据库中找到对应的 PW_{Tg_A}，然后计算 $h_1' = h(ID'_{Tg\_A} \| PW_{Tg\_A} \| ID'_{Tg\_B} \| t_A)$，如果 h_1' 与 h_1 相等，那么可信第三方将 $(ID'_{Tg\_B} \| ID'_{Tg\_A})$ 存储在数据库中。

2）认证阶段

委托之后的认证如图 3 所示。

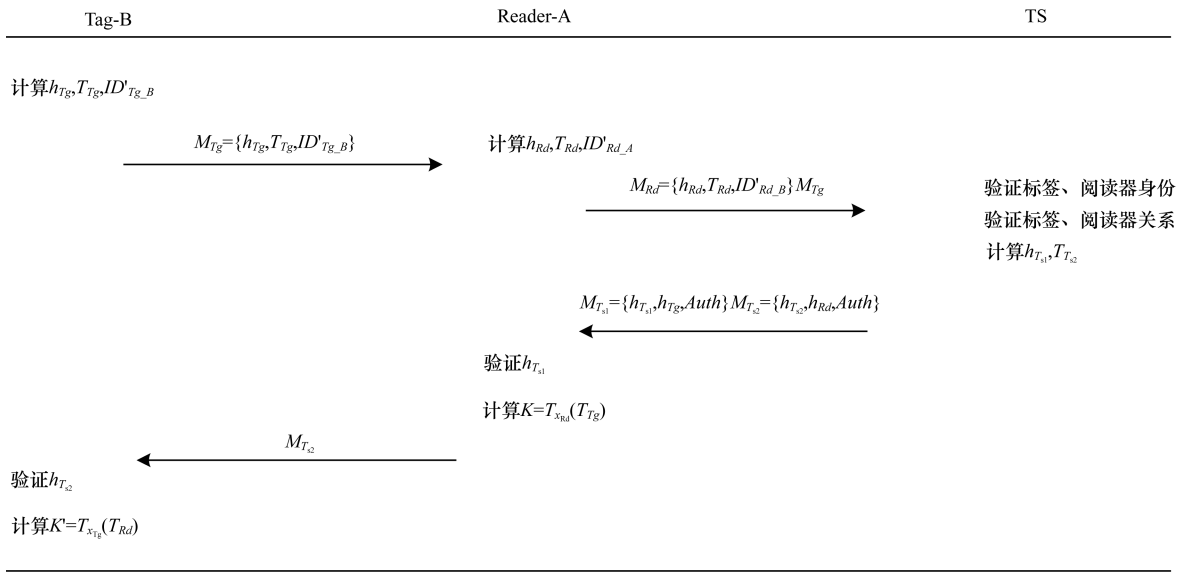

图 3　委托后认证阶段

认证阶段具体步骤如下:

第 1 步　Tag-B 生成一个随机数 x_{Tg},然后计算 $T_{Tg}=T_{x_{Tg}}(r) \bmod p$, $K_{TS}=T_{x_{Tg}}(T_S) \bmod p$, $ID'_{Tg\_B}=ID_{Tg\_B}\oplus K_{TS}$, $h_{Tg}=h(ID_{Tg\_B}\|PW_{Tg\_B}\|t_{Tg}\|T_{Tg})$,其中 t_{Tg} 是标签的当前时间戳,接着标签发送 $M_{Tg}=\{h_{Tg},t_{Tg},T_{Tg},ID'_{Tg\_B}\}$ 给阅读器 Reader-A。

第 2 步　收到 M_{Tg} 之后,Reader-A 首先检验不等式 $(t_{Rd}-t_{Tg})\leqslant\Delta t$ 是否成立(t_{Rd} 为阅读器的当前时间戳),如果成立,则阅读器将生成一个随机数 x_{Rd} 然后计算 $T_{Rd}=T_{x_{Rd}}(r) \bmod p$, $K_{RS}=T_{x_{Rd}}(T_S) \bmod p$, $ID'_{Rd\_A}=ID_{Rd\_A}\oplus K_{RS}$。然后计算 $h_{Rd}=h(ID_{Rd\_A}\|PW_{Rd\_A}\|t_{Rd}\|T_{Rd})$。接着阅读器发送 $M_{Rd}=\{h_{Rd},t_{Rd},T_{Rd},ID'_{Rd\_A}\}$, M_{Tg} 给可信第三方。

第 3 步　当收到 M_{Rd}, M_{Tg} 之后,可信第三方首先检验不等式 $(t_S-t_{Tg})\leqslant\Delta t$, $(t_S-t_{Rd})\leqslant\Delta t$ 是否成立。如果不等式成立,那么可信第三方计算 $K'_{TS}=T_s(T_{Tg}) \bmod p$, $K'_{RS}=T_s(T_{Rd}) \bmod p$, $ID''_{Tg\_B}=ID'_{Tg\_B}\oplus K'_{TS}$, $ID''_{Rd\_A}=ID'_{Rd\_A}\oplus K'_{RS}$。然后根据 ID''_{Tg_B} 到它的存储单元里找到对应的 PW_{Tg_B} 并计算 $h'_{Tg}=h(ID''_{Tg\_B}\|PW_{Tg\_B}\|t_{Tg}\|T_{Tg})$。接着比较 h'_{Tg}, h_{Tg},如果它们相同,那么标签的身份就被可信第三方认证通过。同理验证阅读器的身份。如果两者的身份都被验证通过,那么可信第三方根据 ID''_{Tg_B} 在存储的元组 $(ID_{Tg},ID_{Rd},PW_{Tg})$ 中找到对应的 ID_{Rd},将其与 ID''_{Rd_A} 比较。如果相等,那么可信第三方就知道该阅读器是该标签的拥有者。在这里,显然不相等。然后可信第三方找到委托阶段存储的身份对,就知道 ID''_{Tg_B} 是 ID''_{Tg_A} 委托的,然后根据 ID''_{Tg_A} 到对应的三元组 $(ID_{Tg},ID_{Rd},PW_{Tg})$ 找到其对应的 ID_{Rd} 就是 ID''_{Rd_A},于是可信第三方相信该标签可以通过该阅读器的认证。最后可信第三方计算 $h_{Ts_1}=h(K'_{RS}\|T_{Tg}\|Auth)$, $h_{Ts_2}=h(K'_{TS}\|T_{Rd}\|Auth)$, $M_{Ts1}=\{h_{Ts_1},T_{Tg},Auth\}$, $M_{Ts2}=\{h_{Ts_2},T_{Rd},Auth\}$ ($Auth$ 表示该标签是被委托的)。可信第三方发送 M_{Ts1}, M_{Ts2} 给阅读器 Reader-A。

第 4 步　收到 M_{Ts1}, M_{Ts2} 后,Reader-A 计算 $h'_{Ts_1}=h(K_{RS}\|T_{Tg}\|Auth)$,将其与 h_{Ts_1} 比较。如果相等,阅读器知道标签被可信第三方认证成功。接着把 M_{Ts2} 发送给标签。阅读器计算 $K=T_{x_{Rd}}(T_{Tg})$ 作为和标签的会话密钥。

第 5 步　标签收到 M_{Ts2} 之后,首先计算 $h'_{Ts_2}=h(K_{TS}\|T_{Rd}\|Own)$,将其与 h_{Ts_2} 比较,如果两者相等,那么标签就知道被可信第三方认证成功,接着标签计算 $K'=T_{x_{Tg}}(T_{Rd})$ 作为和阅读器的会话密钥。这个操作完成之后,标签和阅读器的相互认证即完成。

3　安全性分析

3.1　正确性

对于正确性采用 BAN 逻辑进行形式化的证明,首先给出 BAN 逻辑符号定义和用到的推理规则。

3.1.1　BAN 逻辑的基本符号

BAN 逻辑的基本符号表示如下:

A, B 表示通信的主体;

K_{ab}, K_{as}, K_{bs} 表示具体的通信主体的秘钥;

N_a, N_b 表示具体的通信主体的观点;

K_a, K_b 表示具体的通信主体的公开密钥;

$K-1_a$, $K-1_b$ 表示具体的通信主体的公开密钥;

X, Y 表示一般意义上的语句;

K 表示一般意义上的加密密钥;

(X,Y) 表示 X 和 Y 的连接;

$P|\equiv X$ 表示 P 相信 X, P 认为 X 为真;

$P\lhd X$ 表示 P 看到过 X, P 曾收到包含 X 的消

息,P 能读出并重复 X;

$P|\sim X$ 表示 P 在某一时刻发送过 X;

$P|\Rightarrow X$ 表示 P 对 X 有控制权;

$\overset{K}{\mapsto}P$:K 是 P 的公钥;

$\#X$ 表示 X 是新鲜的;

$P\overset{K}{\leftrightarrow}Q$:$P$ 和 Q 可使用共享密钥 K 通信,而且 K 是好的密钥,即只有 P,Q 或可信的第三方知道 K;

$\{X\}_K$ 表示用密钥 K 加密 X 的结果;

$\langle X\rangle_Y$ 表示 X 和 Y 的组合,Y 是一个秘密,它的出现证明使用 $\langle X\rangle_Y$ 的主体的身份。

3.1.2 BAN 逻辑的推理规则

BAN 逻辑的推理规则如下:

1)消息含义规则

(1)对于共享密钥:$\dfrac{P|\equiv P\overset{K}{\leftrightarrow}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$ 表示如果 P 相信 K 为 P 和 Q 之间的共享密钥,且 P 接收到用 K 加密 X 的消息 $\{X\}_K$,则 P 相信 Q 发送过消息 X。

(2)对于公开密钥:$\dfrac{P|\equiv\overset{K}{\mapsto}Q,P\triangleleft\{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$ 表示 P 相信 K 是 Q 的公钥,而 K^{-1} 是 Q 的私钥,当 P 看到用 Q 的私钥加密的消息,就能断定该消息是 Q 发送的。

2)管辖权规则

$$\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$$

如果 P 相信 Q 对 X 有控制权,且 P 相信 Q 也相信 X,则 P 相信 X。

3)临时值校验规则

$$\frac{P|\equiv\#X,P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

如果 P 相信 X 是新的,且 P 相信 Q 发送过 X,则 P 相信 Q 也相信 X。

4)接收消息规则

$$\frac{P\triangleleft(X,Y)}{P\triangleleft X},\frac{P\triangleleft\langle X\rangle_Y}{P\triangleleft X}$$

$$\frac{P|\equiv P\overset{K}{\leftrightarrow}Q,P\triangleleft\{X\}_K}{P\triangleleft X},\frac{P|\equiv\overset{K}{\mapsto}Q,P\triangleleft\{X\}_{K^{-1}}}{P\triangleleft X}$$

5)新鲜性规则

$$\frac{P|\equiv\#X}{P|\equiv\#(X,Y)},\frac{P|\equiv\#X}{P|\equiv\#(\alpha^X)}$$

6)信念规则

$$\frac{P|\equiv X,P|\equiv Y}{P|\equiv(X,Y)},\frac{P|\equiv(X,Y)}{P|\equiv X}$$

$$\frac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X},\frac{P|\equiv Q|\sim(X,Y)}{P|\equiv Q|\sim X}$$

7)密钥与秘密规则

$$\frac{P|\equiv R\overset{K}{\leftrightarrow}R'}{P|\equiv R'\overset{K}{\leftrightarrow}R},\frac{P|\equiv Q|\equiv R\overset{K}{\leftrightarrow}R'}{P|\equiv Q|\equiv R'\overset{K}{\leftrightarrow}R}$$

8)会话密钥规则

$$\frac{A|\equiv\#(K),A|\equiv B|\equiv X}{A|\equiv A\overset{K}{\leftrightarrow}B}$$

其中,X 是密钥 K 的必要的元素。

3.1.3 基于 BAN 逻辑的协议验证

协议的正确性由定理 1 给出。

定理 1 本文提出的认证协议(普通/委托)是正确可行的。

证明:本文的目标是利用 BAN 逻辑逐条验证认证协议执行过程,将结合协议过程和上述 8 条推理规则,推导出认证双方 A,B 最终都彼此信任并协商出有效密钥。

由于委托认证协议和普通认证协议的认证过程的区别只是在于标签和阅读器的对应关系的差别,而这种对应关系都是由可信第三方进行验证,并且这 2 种对应关系都是存储在可信第三方里面的,所以这并不会导致这 2 种协议的正确性证明过程产生差别,因此,只需要给出委托协议的正确性证明过程即可,该过程如下所示。

目标:

1) $Tag\text{-}B|\equiv Tag\text{-}B\overset{K}{\leftrightarrow}Reader\text{-}A$

2) $Reader\text{-}A|\equiv Tag\text{-}B\overset{K}{\leftrightarrow}Reader\text{-}A$

3) $TS|\equiv ID_{Tg\_B}$

4) $TS|\equiv ID_{Rd\_A}$

假设:

1) $Tag\text{-}B|\equiv Tag\text{-}B\overset{PW_{Tg\_B}}{\longleftrightarrow}TS$

2) $Reader\text{-}A|\equiv Reader\text{-}A\overset{PW_{Rd\_A}}{\longleftrightarrow}TS$

3) $TS|\equiv Tag\text{-}B\overset{PW_{Tg\_B}}{\longleftrightarrow}TS$

4) $TS|\equiv Reader\text{-}A\overset{PW_{Rd\_A}}{\longleftrightarrow}TS$

5) $Tag\text{-}B|\equiv x_{Tg}$

6) $Reader\text{-}A|\equiv x_{Rd}$

7) $TS|\equiv\#t_{Tg}$

8) $TS|\equiv\#t_{Rd}$

9) $TS|\equiv Tag\text{-}B|\Rightarrow\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle$

10) $Reader\text{-}A|\equiv Reader\text{-}A\overset{K_{RS}}{\longleftrightarrow}TS$

11) $Reader\text{-}A|\equiv\#K_{RS}$

12) $Reader\text{-}A|\equiv TS|\Rightarrow\langle T_{Tg},Auth\rangle$

13) $Tag\text{-}B|\equiv Tag\text{-}B\overset{K_{TS}}{\longleftrightarrow}TS$

14) $Tag\text{-}B|\equiv\#K_{TS}$

15) $Tag\text{-}B|\equiv TS|\Rightarrow\langle T_{Rd},Auth\rangle$

16) $TS|\equiv Reader\text{-}A\overset{K_{RS}}{\longleftrightarrow}TS$

17) $TS|\equiv Reader\text{-}A|\Rightarrow\{ID_{Rd\_A}\|PW_{Rd\_A}\|t_{Rd}\}$

18) $Reader\text{-}A|\equiv\#T_{Tg}$

协议描述:

1) $Tag\text{-}B\rightarrow Reader\text{-}A$:$M_{Tg}=\{h_{Tg},t_{Tg},T_{Tg},ID'_{Tg\_B}\}$

2) $Reader\text{-}A\rightarrow TS$:$M_{Rd}=\{h_{Rd},t_{Rd},T_{Rd},ID'_{Rd\_A}\}$,$M_{Tg}$

3) $TS\rightarrow Reader\text{-}A:M_{Ts1}=\{h_{Ts_1},T_{Tg},Auth\},M_{Ts2}=\{h_{Ts_2},T_{Rd},Auth\}$

4) $Reader\text{-}A\rightarrow Tag\text{-}B:M_{Ts2}=\{h_{Ts_2},T_{Rd},Auth\}$

协议理想化:

1') $Tag\text{-}B\rightarrow Reader\text{-}A:\{\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle_{PW_{Tg\_B}},t_{Tg},T_{Tg},ID'_{Tg\_B}\}$

2') $Reader\text{-}A\rightarrow TS:\{\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle_{PW_{Rd\_A}},t_{Rd},T_{Rd},ID'_{Rd\_A}\},\{\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle_{PW_{Tg\_B}},t_{Tg},T_{Tg},ID'_{Tg\_B}\}$

3') $TS\rightarrow Reader\text{-}A:\{\langle T_{Tg},Auth\rangle_{K_{RS}},T_{Tg},Auth\},\{\langle T_{Rd},Auth\rangle_{K_{TS}},T_{Rd},Auth\}$

4') $Reader\text{-}A\rightarrow Tag\text{-}B:\{\langle T_{Rd},Auth\rangle_{K_{TS}},T_{Rd},Auth\}$

逻辑推理:

由 2')得:

$V1.\ TS\lhd\{\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle_{PW_{Rd\_A}},t_{Rd},T_{Rd},ID'_{Rd\_A}\},\{\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle_{PW_{Tg\_B}},t_{Tg},T_{Tg},ID'_{Tg\_B}\}$

$V2.\ \dfrac{V1}{TS\lhd\{\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle_{PW_{Tg\_B}},t_{Tg},T_{Tg},ID'_{Tg\_B}\}}$

$V3.\ \dfrac{TS\mid\equiv TS\overset{PW_{Tg\_B}}{\longleftrightarrow}Tag\text{-}B,TS\lhd\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle_{PW_{Tg\_B}}}{TS\mid\equiv Tag\text{-}B\mid\sim\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle}$

$V4.\ \dfrac{TS\mid\equiv\#(t_{Tg})}{TS\mid\equiv\#\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle}$

$V5.\ \dfrac{TS\mid\equiv\#\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle,TS\mid\equiv Tag\text{-}B\mid\sim\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle}{TS\mid\equiv Tag\text{-}B\mid\equiv\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle}$

$V6.\ \dfrac{TS\mid\equiv Tag\text{-}B\mid\Rightarrow\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle,TS\mid\equiv Tag\mid\equiv\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle}{TS\mid\equiv\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle}$

$V7.\ \dfrac{TS\mid\equiv\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle}{TS\mid\equiv ID_{Tg\_B}}\ Goal\,3$

$V8.\ \dfrac{TS\lhd\{\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle_{PW_{Rd\_A}},t_{Rd},T_{Rd},ID'_{Rd\_A}\},\{\langle ID_{Tg\_B},t_{Tg},T_{Tg}\rangle_{PW_{Tg\_B}},t_{Tg},T_{Tg},ID'_{Tg\_B}\}}{TS\lhd\{\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle_{PW_{Rd\_A}},t_{Rd},T_{Rd},ID'_{Rd\_A}\}}$

$V9.\ \dfrac{TS\lhd\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle_{PW_{Rd\_A}},TS\mid\equiv Reader\text{-}A\overset{PW_{Rd\_A}}{\longleftrightarrow}TS}{TS\mid\equiv Reader\text{-}A\mid\sim\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle}$

$V10.\ \dfrac{TS\mid\equiv\#t_{Rd}}{TS\mid\equiv\#\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle}$

$V11.\ \dfrac{TS\mid\equiv\#\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle,TS\mid\equiv Reader\mid\sim\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle}{TS\mid\equiv Reader\mid\equiv\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle}$

$V12.\ \dfrac{TS\mid\equiv Reader\mid\equiv\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle,TS\mid\equiv Reader\mid\Rightarrow\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle}{TS\mid\equiv\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle}$

$V13.\ \dfrac{TS\mid\equiv\langle ID_{Rd\_A}\parallel t_{Rd}\parallel T_{Rd}\rangle}{TS\mid\equiv ID_{Rd\_A}}\ (Goal\,4)$

由 3')得:

$V14.\ Reader\text{-}A\lhd\{\langle T_{Tg},Auth\rangle_{K_{RS}},T_{Tg},Auth\},\{\langle T_{Rd},Auth\rangle_{K_{TS}},T_{Rd},Auth\}$

$V15.\ \dfrac{Reader\text{-}A\lhd\{\langle T_{Tg},Auth\rangle_{K_{RS}},T_{Tg},Auth\},\{\langle T_{Rd},Auth\rangle_{K_{TS}},T_{Rd},Auth\}}{Reader\text{-}A\lhd\{\langle T_{Tg},Auth\rangle_{K_{RS}}\}}$

$V16.\ \dfrac{Reader\text{-}A\lhd\langle T_{Tg},Auth\rangle_{K_{RS}},Reader\text{-}A\mid\equiv Reader\text{-}A\overset{K_{RS}}{\longleftrightarrow}TS}{Reader\text{-}A\mid\equiv TS\mid\sim\langle T_{Tg},Auth\rangle}$

$V17.\ \dfrac{Reader\text{-}A\mid\equiv\#K_{RS}}{Reader\text{-}A\mid\equiv\#\langle T_{Tg},Auth\rangle_{K_{RS}}}$

$V18.\ \dfrac{Reader\text{-}A\mid\equiv\#\langle T_{Tg},Auth\rangle_{K_{RS}}}{Reader\text{-}A\mid\equiv\#\langle T_{Tg},Auth\rangle}$

$V19.\ \dfrac{Reader\text{-}A\mid\equiv TS\mid\sim\langle T_{Tg},Auth\rangle,Reader\mid\equiv\#\langle T_{Tg},Auth\rangle}{Reader\text{-}A\mid\equiv TS\mid\equiv\langle T_{Tg},Auth\rangle}$

$V20.\ \dfrac{Reader\text{-}A\mid\equiv TS\mid\equiv\langle T_{Tg},Auth\rangle,Reader\text{-}A\mid\equiv TS\mid\Rightarrow\langle T_{Tg},Auth\rangle}{Reader\text{-}A\mid\equiv\langle T_{Tg},Auth\rangle}$

$$V21.\ \frac{Reader\text{-}A\mid\equiv\langle T_{Tg},Auth\rangle}{Reader\text{-}A\mid\equiv T_{Tg}}$$

$$V22.\ \frac{Reader\text{-}A\mid\equiv T_{Tg},Reader\text{-}A\mid\equiv x_{Rd}}{Reader\text{-}A\mid\equiv Reader\text{-}A\overset{K=T_{x_{Rd}}(T_{Tg})\bmod p}{\longleftrightarrow}Tag\text{-}B}\ (Goal\,2)$$

由 4’)得:

$$V23.\ Tag\text{-}B\lhd\{\langle T_{Rd},Auth\rangle_{K_{TS}},T_{Rd},Auth\}$$

$$V24.\ \frac{Tag\text{-}B\lhd\{\langle T_{Rd},Auth\rangle_{K_{TS}},T_{Rd},Auth\}}{Tag\text{-}B\lhd\{\langle T_{Rd},Auth\rangle_{K_{TS}}}$$

$$V25.\ \frac{Tag\text{-}B\mid\equiv Tag\text{-}B\overset{K_{TS}}{\longleftrightarrow}TS,Tag\text{-}B\lhd\{\langle T_{Rd},Auth\rangle_{K_{TS}}}{Tag\text{-}B\mid\equiv TS\mid\sim\langle T_{Rd},Auth\rangle}$$

$$V26.\ \frac{Tag\text{-}B\mid\equiv\#K_{TS}}{Tag\text{-}B\mid\equiv\#\langle T_{Rd},Auth\rangle_{K_{TS}}}$$

$$V27.\ \frac{Tag\text{-}B\mid\equiv\#\langle T_{Rd},Auth\rangle_{K_{TS}}}{Tag\text{-}B\mid\equiv\#\langle T_{Rd},Auth\rangle}$$

$$V28.\ \frac{Tag\text{-}B\mid\equiv TS\mid\sim\langle T_{Rd},Auth\rangle,Tag\text{-}B\mid\equiv\#\langle T_{Rd},Auth\rangle}{Tag\text{-}B\mid\equiv TS\mid\equiv\langle T_{Rd},Auth\rangle}$$

$$V29.\ \frac{Tag\text{-}B\mid\equiv TS\mid\equiv\langle T_{Rd},Auth\rangle,Tag\text{-}B\mid\equiv TS\mid\Rightarrow\langle T_{Rd},Auth\rangle}{Tag\text{-}B\mid\equiv\langle T_{Rd},Auth\rangle}$$

$$V30.\ \frac{Tag\text{-}B\mid\equiv\langle T_{Rd},Auth\rangle}{Tag\text{-}B\mid\equiv T_{Rd}}$$

$$V31.\ \frac{Tag\text{-}B\mid\equiv T_{Rd},Tag\text{-}B\mid\equiv x_{Tg}}{Tag\text{-}B\mid\equiv Tag\text{-}B\overset{K=T_{x_{Tg}}(T_{Rd})\bmod p}{\longleftrightarrow}Reader\text{-}A}\ (Goal\,1)$$

3.2 安全性

安全性分析包括以下部分:

1)可认证性

标签 Tag-B 发送 $h_{Tg}=h(ID_{Tg\_B}\|PW_{Tg\_B}\|t_{Tg}\|T_{Tg})$,$t_{Tg}$,$T_{Tg}$,$ID'_{Tg_B}=ID_{Tg_B}\oplus K_{TS}$给阅读器,然后阅读器转发给可信第三方,根据混沌映射的半群性质可信第三方计算出$K'_{TS}=T_s(T_{Tg})\bmod p$,然后计算出$ID''_{Tg_B}=ID'_{Tg_B}\oplus K'_{TS}$,再根据$ID''_{Tg_B}$到数据库中查找它对应的$PW_{Tg_B}$,再计算$h'_{Tg}=h(ID''_{Tg_B}\|PW_{Tg_B}\|t_{Tg}\|T_{Tg})$与$h_{Tg}$比较。由于只有 Tag-B 知道它对应的$PW_{Tg_B}$,因此当$h'_{Tg}$与$h_{Tg}$相等时,可信第三方即可验证 Tag-B 的身份的合法性。同理验证阅读器的身份合法性。然后可信第三方再根据数据库存储的每个标签对应的三元组(ID_{Tg},ID_{Rd},PW_{Tg})或授权阶段存储的($ID''_{Tg\_B}\|ID''_{Tg\_A}$)判断该标签是否能通过阅读器的认证。如果该标签能够通过该阅读器的认证,可信第三方发送$M_{Ts1}=\{h_{Ts_1}=h(K'_{RS}\|T_{Tg}\|Auth),T_{Tg},Auth\}$给阅读器。阅读器收到$M_{Ts1}=\{h_{Ts_1},T_{Tg},Auth\}$之后,计算$h'_{Ts_1}=h(K_{RS}\|T_{Tg}\|Auth)$与$h_{Ts_1}$比较,如果相等,阅读器知道标签被认证通过,因为根据混沌映射的半群性质以及 DLP,DHP 问题,除了阅读器自身之外,只有可信第三方能计算出h_{Ts_1}。同理,标签可以知道自己被认证通过。

2)防重放攻击

由于在$h_{Tg}=h(ID_{Tg_B}\|PW_{Tg_B}\|t_{Tg}\|T_{Tg})$中添加了时间戳$t_{Tg}$,因此$M_{Tg}$中时间戳$t_{Tg}$的更改操作将使得其无法被可信第三方认证通过。而如果攻击者在不更改M_{Tg}中的时间戳t_{Tg}的情况下,试图对之前的消息重放的时候,可信第三方会首先根据不等式$(t_S-t_{Tg})\leqslant\Delta t$是否成立来对$M_{Tg}$中的时间戳$t_{Tg}$进行检验。显然,此时不等式$(t_S-t_{Tg})\leqslant\Delta t$是不成立的,那么可信第三方就会检验出该时间戳是过期的,然后终止操作。所以,该协议是抗重放攻击的。

3)匿名性

协议中身份都是由$ID'_{Tg_B}=ID_{Tg_B}\oplus K_{TS}$保护的,其中,$K_{TS}=T_{x_{Tg}}(T_S)\bmod p$,$x_{Tg}$是由标签选取的随机数。由于混沌映射的半群性质,可信第三方在收到$T_{Tg}=T_{x_{Tg}}(r)\bmod p$之后,再根据其私钥$s$可以计算出$K'_{TS}=T_s(T_{Tg})\bmod p$,然后计算$ID''_{Tg_B}=ID_{Tg_B}\oplus K'_{TS}$以得到标签的身份。而由于混沌映射的 DLP,DHP 问题,使得除了标签自身和可信第三方可以计算出K_{TS}之外,其他人都计算不出来。所以,也就无法获得标签的真实身份,标签的匿名性得到了保证。

4)防假冒标签攻击

为了假冒标签,攻击者必须知道标签的身份ID_{Tg}和口令PW_{Tg},但是口令都是作为参数嵌在哈希函数$h_{Tg}=h(ID_{Tg}\|PW_{Tg}\|t_{Tg}\|T_{Tg})$里面的,由于哈希函数的单向不可逆性,攻击者无法根据哈希值h_{Tg}获得身份ID_{Tg}和口令PW_{Tg},因此攻击者将无法假冒标签进行攻击。

5)防口令 PW_{Tg} 猜测攻击

该部分包括防在线口令猜测攻击和防线下口令猜测攻击 2 个部分。

(1)在线口令猜测指的是攻击者通过在线的形式猜出用户的口令 PW_{Tg}。对于在线口令猜测,攻击者在不知道标签身份 ID_{Tg} 和口令 PW_{Tg} 的情况下,计算出来的消息 $h_{Tg}=h(ID_{Tg}\|PW_{Tg}\|t_{Tg}\|T_{Tg})$ 将不会通过可信第三方的验证,并且在多次不能通过验证的情况下(比如说三次),可信第三方会拒绝再进行验证,故该协议可以防止在线口令猜测攻击。

(2)线下口令猜测指的是攻击者通过窃取合法用户和可信第三方之间的消息,从而试图猜测出用户的口令 PW_{Tg}。对于线下口令猜测,由于标签的匿名性,攻击者无法获得标签的身份 ID_{Tg},在只知道 (t_{Tg},T_{Tg}),$h_{Tg}=h(ID_{Tg}\|PW_{Tg}\|t_{Tg}\|T_{Tg})$ 的情况下,攻击者无法通过穷举得出正确的口令 PW_{Tg},故该协议可以防止线下口令猜测攻击。

4　结束语

智能家居作为物联网的典型应用具有广阔的市场前景,但其安全问题是决定其能否被深入推广的主要问题。本文针对事务委托场景的安全需求,提出一种委托认证方案,通过将混沌映射引入委托认证,大幅降低了密钥管理难度,提升系统运行效率。下一步将考虑引入基于生物信息的认证,实现多因子认证技术,进一步提高智能家居系统的安全性。

参考文献

[1] 何东之,于敬芝,王书锋,等. 基于环绕智能的智能家居控制系统研究[J]. 计算机工程,2007,33(10):261-262.

[2] JIANG L,LIU D Y,YANG B. Smart Home Research[C]//Proceedings of International Conference on Machine Learning and Cybernetics. Shanghai,China:[s. n.],2004:125-136.

[3] RICQUEBOURG V,MENGA D,DURAND D,et al. The Smart Home Concept:Our Immediate Future[C]//Proceedings of IEEE International Conference on E-learning in In dustrial Electronics. Hammamet,Tunisie:IEEE Press,2006:23-28.

[4] 宋　冬,廖　杰,陈　星,等. 基于 ZigBee 和 GPRS 的智能家居系统设计[J]. 计算机工程,2012,38(23):243-246.

[5] 严　义,胡峰令. 面向嵌入式 PLC 的调度算法[J]. 计算机工程,2009,35(19):257-259.

[6] 俱　莹,刘开华,史伟光,等. 基于 RFID 的边界虚拟参考标签定位算法[J]. 计算机工程,2011,37(6):274-276.

[7] KIM S C,JEONG Y S,PARK S O. RFID-based Indoor Location Tracking to Ensure the Safety of the Elderly in Smart Home Environments[J]. Personal & Ubiquitous Computing,2013,17(8):1699-1707.

[8] NASIR A,HUSSAIN S I,SOONG B H,et al. Energy Efficient Cooperation in Underlay RFID Cognitive Networks for a Water Smart Home[J]. Sensors,2014,14(10):18353-18369.

[9] BOUCHARD K,BOUZOUANE A,BOUCHARD B. Gesture Recognition in Smart Home Using Passive RFID Technology[C]//Proceedings of ACM International Conference on Pervasive Technologies Related To Assistive Environments. New York,USA:ACM Press,2014:569-575.

[10] MITRACHARYA S,ACHARYA T. Gesture Recognition:A Survey[J]. IEEE Transactions on Systems Man & Cybernetics Part C Applications & Reviews,2007,37(3):311-324.

[11] XIE L,YIN Y,LU X,et al. iFridge:An Intelligent Fridge for Food Management Based on RFID Technology[C]//Proceedings of ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication. Zurich,Switzerland:ACM Press,2013:214-226.

[12] HSU H H,LEE C N,CHEN Y F. An RFID-based Reminder System for Smart Home[C]//Proceedings of IEEE International Conference on Advanced Information Networking and Applications. Sinapore:IEEE Press,2011:365-375.

[13] GU H,WANG D. A Content-aware Fridge Based on RFID in Smart Home for Home-healthcare[C]//Proceedings of International Conference on Advanced Communication Technology. Phoenix,USA:IEEE Press,2009:169-176.

[14] XU W,LI D. Design and Implementation of Smart Home System Based on RFID Technology[J]. Advanced Materials Research,2014(1):1057-1060.

[15] VERMA G K,TRIPATHI P. A Digital Security System with Door Lock System Using RFID Technology[J]. International Journal of Computer Applications,2010,5(11):6-8.

[16] CHEN K M. An Evaluation Of RFID Door Security System at Taipei Arena Ice Land Based On Technology Acceptance Model[J]. International Journal of Management & Information Systems,2013,17(2):117-130.

[17] ZHANG Z,WANG H,GAO Y. C2MP:Chebyshev Chaotic Map-based Authentication Protocol for RFID Applications[J]. Personal & Ubiquitous Computing,2015,19(7):1053-1061.

[18] XIE Q,HU B,WU T. Improvement of a Chaotic Maps-based Three-party Password-authenticated Key Exchange Protocol Without Using Server's Public Key and Smart Card[J]. Nonlinear Dynamics,2014,79(4):2345-2358.

[19] LEE C C,LI C T,CHIU S T,et al. A New Three-party-authenticated Key Agreement Scheme Based on Chaotic Maps Without Password Table[J]. Nonlinear Dynamics,2014,79(4):2485-2495.

[20] YAU W C,PHAN C W. Cryptanalysis of a Chaotic Map-based Password-authenticated Key Agreement Protocol Using Smart Cards[J]. Nonlinear Dynamics,2015,79(2):809-821.

编辑　索书志