基于伪ID的RFID认证协议及串空间证明

徐 扬 苑津莎 高会生 胡晓宇 赵振兵
(华北电力大学电气与电子工程学院 保定 071003)

摘 要 安全有效的认证协议是对RFID系统安全的有力保障,适宜的形式化分析方法能为RFID认证协议提供有效的证明。设计了基于伪ID的RFID认证协议,伪ID由标签ID、标签认证数值和随机数产生。标签ID不出现在协议执行过程中,减少了系统遭受攻击的可能性。协议通过标签ID、标签认证值和随机数的Hash运算实现认证。利用串空间模型对协议进行形式化分析,建立认证协议的串空间模型丛图,证明了协议的保密性和匿名性。通过分析常规的基于Hash函数的认证协议的性能可知,该协议在使用较低运算成本的情况下可以抵抗多种攻击,并能够完成标签和读写器之间的双向认证。

关键词 认证协议,RFID,Hash,串空间
中图法分类号 TN918.91 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.10.027

RFID Authentication Protocol Based on Pseudo ID and Certification by Strand Space Model

XU Yang YUAN Jin-sha GAO Hui-sheng HU Xiao-yu ZHAO Zhen-bing
(School of Electrical and Electronic Engineering, North China Electric Power University, Baoding 071003, China)

Abstract Secure and effective authentication protocol is a powerful guarantee for the security of RFID system, and the appropriate formal analysis method can provide a valid proof for the RFID authentication protocol. In this paper, the RFID authentication protocol based on pseudo ID was designed, and the pseudo ID was generated by the tag's ID, the authentication value of the tag and the random number. Tag's ID does not appear in the process of protocol implementation, which reduces the possibility of system attacks. The protocol uses hash algorithm of the tag's ID, authentication value of the tag and the random number to achieve certification. Based on the formal analysis of the protocol by the strand space model, the cluster map of the strand space model of the authentication protocol was established. The per-for-mance of security and authentication of the protocol were proved. By comparing the common protocol based on hash, the proposed method can resist attacks with low computation cost and realize mutual authentication between the tag and reader.

Keywords Authentication protocol, RFID, Hash, Strand space

随着物联网在社会生活各个领域的广泛应用,越来越多的用户会通过物联网进行数据传播和交流,海量的个人隐私数据和信息将存储在政府机关、第三方机构以及商业智能设备中,这将很大程度地提高个人隐私数据被非法传播、篡改或者盗用的可能性[1-3]。RFID标签、阅读器和应用服务器等都属于物联网中的感知设备[4]。物联网应用的一般情况是:由阅读器的持有者通过阅读器读取标签的ID,再由标签的ID通过应用服务器到数据库查询对应的信息,最终将查询结果信息返回给阅读器的持有者。

设计一个正确的没有安全缺陷的认证协议是一项十分复杂的工作[5]。安全协议形式化分析方法就是一种证明协议是否安全可行的理论,以BAN逻辑为代表的模态逻辑是应用最为广泛的形式化分析方法[6-7]。但是模态逻辑过于抽象,难以完全映射协议运行的全貌。串空间(Strand Space)模型理论将安全协议的形式化分析技术提升到一个新的高度[8],通过建立协议主体间交换信息的代数结构以及推理规则来证明协议的安全性。

1 相关工作

Hash函数是一种能把任意长度的输入通过散列运算转换成固定长度输出的算法。这种压缩运算被广泛用在RFID的认证协议中。基于Hash函数的RFID认证协议[9-15]主要包括Hash-lock协议、Random hash-lock协议、Hash-chain协议、基于ID变化的协议(Hash-based variation)、图书馆RFID协议、基于挑战-响应的RFID认证协议和LACP协议等。文献[9]提出的Hash-lock协议用metaID来代替标签ID,避免

到稿日期:2016-09-07 返修日期:2017-01-03 本文受国家自然科学基金(61401154)资助。
徐 扬(1979-),女,博士生,主要研究方向为物联网信息安全,E-mail:xuyang@ncepu.edu.cn;苑津莎(1957-),男,教授,博士生导师,主要研究方向为通信与信息系统、物联网信息安全;高会生(1963-),男,教授,主要研究方向为通信网管理与安全风险评估;胡晓宇(1989-),男,硕士生,主要研究方向为物联网协议安全;赵振兵(1979-),男,副教授,主要研究方向为物联网技术、图像处理技术及其在智能电网中的应用。

了信息泄漏,但不能抵抗重传和位置跟踪攻击。Random hash-lock 协议[10]是 Hash-lock 协议的升级版,用随机数 R 取代密钥 Key,但是系统易受到假冒攻击。Hash-chain 协议[11]使用不同的 Hash 函数来进行计算和更新,避免了标签被跟踪和信息泄露,但 Hash 函数的运算量大,不适合在大量标签的情况下使用。Hash-based variation[12]使用随机数 R 和标签 ID 的 Hash 函数来更新标签细信息,可有效抵抗重放攻击。文献[13]基于共享密钥的伪随机数实现认证,伪随机数和安全伪随机数发生器需要存储空间,对标签的要求较高,系统实现成本大。基于挑战-响应的安全协议[14]适用于分布式环境,协议执行过程的计算量大,同样也不适合低成本的 RFID 系统使用。基于挑战-相应的协议[15]每次认证后会更新标签 ID,使应答信息不同,可以避免标签被跟踪,但标签更新信息与后端数据库更新 ID 时间存在不同步的问题。文献[16-18]提出了基于 Hash 函数的 RFID 双向认证协议。文献[16]将协议分为标签更新和读写器更新两种方式,其满足前向安全的要求,但是系统使用非对称密钥方式实现认证,运算量大。HSAP 协议[17]中标签需要执行 2 次 Hash 函数来完成认证,不满足前向安全性。基于伪随机数发生器和通用 Hash 的 PFP 协议[19]满足前向隐私安全,适合在低成本 RFID 系统中应用,但不能抵挡 Dos 攻击。

本文提出基于伪 ID 的 RFID 认证协议,旨在在利用单向 Hash 函数所具有的良好的认证性能的基础上,采用标签伪 ID 的方法来防止标签的真实 ID 被更新后无法实现产品回溯的情况发生,并克服标签 ID 更新过程中的数据不同步问题。

2　提出的协议

在物联网中,数据库服务器和应用服务器之间的信息传输被认为是安全的。可以由应用服务器上的应用软件保护其安全,使其不被其他用户访问。标签和阅读器之间是无线连接且不安全的通道,数据库非公开,用户访问数据库时必须经过应用服务器。应用服务器验证标签是否是其所属范围内的合法标签;验证阅读器是否合法,同时通过阅读器记录标签的路径信息。协议中的主要设备有阅读器、标签、应用服务器和数据库。

协议中使用的各种符号的定义如下。

DB:数据库服务器;AS:应用服务器;R:阅读器;T:标签;T_{num}:标签认证数字值;R_{num}:阅读器认证数字值;r_i:随机数;$H(\cdot)$:哈希函数;TID:标签 ID 值;RID:阅读器 ID 值;$TPID$:标签的伪 ID 值;M:标签物品的信息;$\|$:字符串连接、异或运算。

安全认证之前标签应存储的信息:TID,$TPID$,T_{num}。

安全认证之前数据库应存储的信息:TID,RID,$TPID$,T_{num},M。

协议的认证过程如图 1 所示。

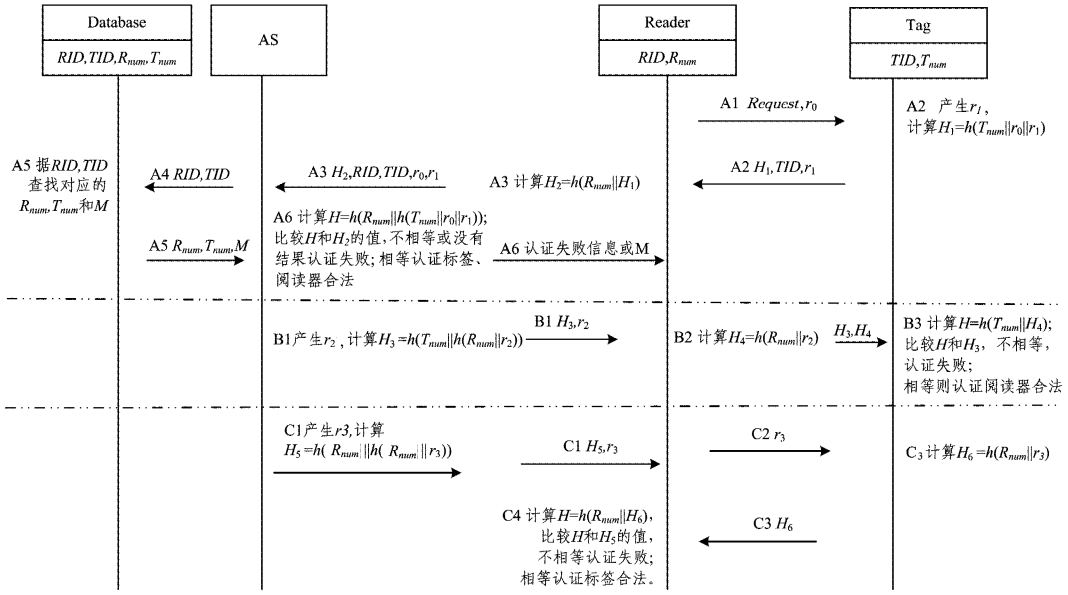

图 1　协议认证过程图

协议详细认证步骤如下:

A:应用服务器认证阅读器和标签

A1:阅读器向标签发送 $Request$ 请求,产生随机数 r_0;

A2:标签根据阅读器命令产生随机数 r_1,将 T_{num} 和随机数 r_0 与 r_1 进行 Hash 运算 $H_1=h(T_{num}\|r_0\|r_1)$,并将计算结果 H_1、随机数 r_1 和标签 TID 发送给阅读器;

A3:阅读器根据标签发送的 H_1 和阅读器的 R_{num} 进行哈希运算 $H_2=h(R_{num}\|H_1)$,并将计算结果 H_2,RID,TID 和随机数 r_0 与 r_1 发送给应用服务器;

A4:应用服务器将 RID 和 TID 发送给数据库服务器进行检索;

A5:数据库服务器根据 TID 和 RID 的数值在数据库中检索到与之相对应的 T_{num},M 和 R_{num} 并返回给应用服务器;

A6:应用服务器计算 $H=h(R_{num}\|h(T_{num}\|r_0\|r_1))$,比较 H 值和阅读器 A3 步骤中发送过的 H_2 值是否相等,若相等,则认证标签和阅读器合法,根据需要将 M 传送给阅读器,认证结束;若不相等或者数据库未检索出结果,则认证失败,返回阅读器认证失败信息。

B:标签认证阅读器和应用服务器(接续 A1)

B1:应用服务器产生随机数 r_2,并计算 $H_3=h(T_{num}\|h$

($R_{num} \| r_2$))，将 r_2 和 H_3 发送给阅读器；

B2：阅读器计算 $H_4=h(R_{num} \| r_2)$，将 H_3 和 H_4 发送给标签；

B3：标签根据发送过来的数据信息计算 $H=h(T_{num} \| H_4)$，并比较 H 和 H_3，如果 $H \neq H_3$，则通知阅读器认证失败；若 $H=H_3$，则认证阅读器合法。

C：阅读器验证标签(接续 A1)

C1：应用服务器产生随机数 r_3，计算 $H_5=h(R_{num} \| h(T_{num} \| r_3))$，并将 H_5 和 r_3 发送给阅读器；

C2：阅读器将 r_3 发送给标签；

C3：标签计算 $H_6=h(T_{num} \| r_3)$，并将 H_6 发送给阅读器；

C4：阅读器计算 $H=h(R_{num} \| H_6)$，并比较 H 与 H_5 是否相等，若相等则验证标签合法，若不相等则验证失败，过程结束。

3 串空间模型

在串空间模型中，每个串代表协议中某一主体行为事件的一个消息序列，“串空间”就是协议运行中所有可能出现的串的集合。用 L 表示协议中主体所交换的信息的集合，该集合中的元素称为项，并用“$\sqsubset$”表示子项关系。协议的主体可以接收(“－”接收项)或发送(“＋”发送项)。$(\pm L)^*$ 表示有符号项的有限序列的集合。串空间中迹是一个有符号项的有限序列，通常用 Σ 表示一个串空间。如果存在 L 上的一个串空间的集合 Σ，那么就存在一个迹的映射 $\mathrm{tr}:\Sigma(\pm L)^*$。

3.1 串空间的基本性质

串空间常用的基本性质有以下 5 条：

(1)$\langle s,i\rangle$ 表示结点，其中 $s \in \Sigma$，i 是 $[1,length(\mathrm{tr}(s))]$ 区间的一个整数，结点 $\langle s,i\rangle$ 属于串 S。每一个结点都属于唯一的一个串，结点的集合用 N 表示。

(2)若 $n=\langle s,i\rangle \in N$，用 $index(n)$ 表示 n 在 S 的迹上的索引，$index(n)=i$。定义 $term(n)$ 代表串 S 的迹中第 i 个有符号项，用项(n)表示 S 的迹上第 i 个有符号项的非符号部分。

(3)对于 $n_1,n_2 \in N$，$n_1 \rightarrow n_2$ 表示项$(n_1)=+a$，项$(n_2)=-a$。它表示结点 n_1 发送消息 a，该消息被结点 n_2 接收，从而便在它们所属的串空间上建立了因果联系。

(4)如果 $n_1,n_2 \in N$，$n_1 \Rightarrow n_2$ 表示 n_1,n_2 出现在同一个串上，且 $index(n_1)=index(n_2)-1$，表示 n_1 在这个串上是 n_2 的因果前驱。

(5)无符号项 t 出现在 $n(n \in N)$ 上，当且仅当 $t \in term(n)$。若项 t 在一个特定的串空间唯一生成，则它可以作为一个新的随机数或会话密钥。

3.2 束及束高度

设 S 是串空间中部分边的集合，N_C 是与 S 中任意边相关联的结点集合，C 是 S 和 N_C 的并集。C 是一个束，如果满足：

1)C 是有限的无环图；

2)若 $n_1 \in N_c$，并且 $term(n_1)$ 为负，那么存在唯一的结点 n_2，使得 $n_2 \rightarrow n_1 \in C$；

3)若 $n_1 \in N_c$ 且 $n_2 \Rightarrow n_1$，则 $n_2 \Rightarrow n_1 \in C$。

束高度是指束 C 中使节点 $\langle s,i\rangle \in C$ 最大的 i 值，称为串 S 的束高度。若串 S 的迹为 $\mathrm{tr}(S)=\langle \mathrm{tr}(S)(1),\cdots,\mathrm{tr}(S)(m)\rangle$，则 $m=C-height(S)$，即 m 就是串 S 的束高度。

3.3 结点关系

设 S 是串空间中一个边的集合，且 $S \subseteq (\rightarrow \cup \Rightarrow)$，$N_S$ 是附属于各边的结点集。对于 $\forall n_1,n_2 \in N_S$，定义结点之间的关系“$\prec_S$”和“$\preceq_S$”。

$n_1 \prec_S n_2$：表示在边集 S 中存在一条从结点 n_1 到结点 n_2 的由“$\rightarrow$”和“$\Rightarrow$”类型的边组成的路径，边的数目必须大于零。

$n_1 \preceq_S n_2$：表示在边集 S 中存在一条从结点 n_1 到结点 n_2 的由“$\rightarrow$”和“$\Rightarrow$”类型的边组成的路径，边的数目必须大于或等于零。

关系“$\preceq_S$”具有自反、反对称以及可传递 3 条性质，满足偏序关系。偏序关系具有以下 3 条重要性质：

(1)设 C 是一个束，因为二元关系 $\preceq_S$ 是偏序的，所以 C 的任意非空结点都存在 $\preceq_S$ 最小元；

(2)设 C 是一个束，N 是 C 中满足 $uns\_term(m)=uns\_term(m')$ 的结点集，如果 n 是 N 中第一个 $\preceq_S$ 最小元，则 n 的符号为正；

(3)设 C 是一个束，$t \in A$，且 $n \in C$ 是结点集 $\{m \in c: t \sqsubseteq uns\_term(m)\}$ 的 $\preceq_S$ 最小元，则消息项 t 起源于结点 n。

3.4 攻击者模型

定义二元组 $(\Sigma,\mathscr{P})$ 表示含有攻击者串的渗透串空间模型，其中 Σ 是一个协议的串空间模型，$\mathscr{P}$ 中的串为攻击者串，任意的 $p \in \mathscr{P}$。

4 协议安全性的串空间分析

在本协议中 A 代表阅读器，B 代表标签，AS 代表应用服务器，DB 代表数据库。限于篇幅，仅以协议第一个步骤即运用服务器对标签的认证和标签对阅读器的认证为例来证明其安全性。协议描述为：

(1)Message1：$A \rightarrow B: r_0$；

(2)Message2：$B \rightarrow A: r_1, TID, H_1$；

(3)Message3：$A \rightarrow AS: r_0, r_1, TID, RID, H_2$；

(4)Message4：$AS \rightarrow DB: RID, TID$；

(5)Message5：$DB \rightarrow AS: R_{num}, T_{num}$；

(6)Message6：$AS \rightarrow A: H_3, r_2$；

(7)Message7：$A \rightarrow B: H_3, H_4$。

首先定义协议的串空间：设 $(\Sigma,\mathscr{P})$ 是一个渗透串空间，它由以下 5 种串组成，称为 PID 串空间。T 代表原子信息。

(1)攻击者串 $s \in \mathscr{P}$。

(2)发起者串 $s \in Init[A,B,AS,TID,RID,r_0,r_1,r_2]$，$s$ 的迹(tr)：$\langle +r_0, -r_1 TIDH_1, +r_0 r_1 TIDRIDH_2, -H_3 r_2, +H_3 H_4\rangle$。其中，$A,B,AS \in Tname, r_i, RID, TID \in \mathscr{T}$，但是 $r_i RID \notin Tname$。串 $s \in Init[A,B,AS,TID,RID,r_0,r_1,r_2]$ 相关联的主体为 A。

(3)响应者串 $s \in Resp[A,B,TID,r_0,r_1,r_2]$，迹(tr)：$\langle -r_0, +r_1 TIDH_1, -H_3 H_4\rangle$。其中，$A,B \in Tname, r_i, TID \in \mathscr{T}$，但是 $TID \notin Tname$。串 $s \in Resp[A,B,TID,r_0,r_1,r_2]$ 相关联的主体为 B。

(4)应用服务器串 $s \in Serv[A,S,TID,RID,r_0,r_1,r_2]$，迹(tr)：$\langle -r_0 r_1 TIDRIDH_2, +RIDTID, -T_{num} R_{num}, +$

$H_3 r_2\rangle$。其中,$A, AS \in Tname, r_i, RID, TID \in \mathcal{T}, r_i \notin Tname$。串 $s \in Serv[A, S, TID, RID, r_0, r_1, r_2]$ 相关联的主体为 S。

(5)数据库串 $s \in Data[DB, AS, RID, TID]$,迹(tr):$\langle -RIDTID, +R_{num} T_{num}\rangle$。其中,$DB, AS \in Tname, RID, TID \in \mathcal{T}$。串 $s \in Data[DB, AS, RID, TID]$ 相关联的主体为 DB。$s \in Init[A, B, AS, TID, RID, r_0, r_1, r_2]$ 或 $s \in Resp[A, B, TID, r_0, r_1, r_2]$ 是一个常规串,A 和 B 为常规串 s 的发起者和响应者,r_i 是随机值,具有新鲜性。

4.1　保密性

(1)R_{num} 的保密性

命题 1　设 C 是 PID 串空间 Σ 中的一个束,$A, B \in Tname, RID \neq TID \neq r_0 \neq r_1$,$R_{num}$ 唯一起源于串空间 Σ,$s \in Init[A, B, AS, TID, RID, r_0, r_1, r_2]$,且 s 的束高度为 5,则 R_{num} 唯一起源于节点 $\langle s, 3\rangle$。

证明:设 n_3 代表节点 $\langle s, 3\rangle$,v_3 代表节点 $\langle s, 3\rangle$ 的消息,使用 n_2, n_4 分别代表节点 $\langle s, 2\rangle$ 和 $\langle s, 4\rangle$,它们满足关系:$n_2 \prec n_3 \prec n_4$。根据命题可知:$R_{num} \in H_2 \sqsubset v_3$,$sign(n_3) = +$,因此只需验证关系 $H_2 \not\sqsubset uns\_term(n_2)$ 是否成立。

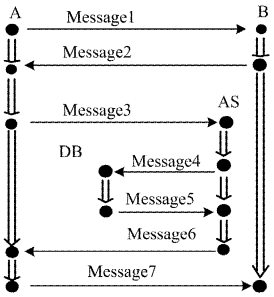

图 2　PID 串空间模型丛图

从图 2 可以看出,$uns\_term(n_2) = \{r_0, TID, H_1\}$。因为 $RID \neq TID \neq r_0 \neq r_1$,$H_2 = hash(Rnum \| H_1)$,在这种情况下,可以将 H_2 看作将 H_1 通过自身存储的 R_{num} 加密而成的消息项,故 $H_2 \neq H_1$。通过自有假设中的连接加密互斥性质:令 $m_1 = r_0, m_2 = TID, m_3 = R_{num}, H_1 = K$,并通过关系式 $m_1, m_2, m_3 \in A, K \in \boldsymbol{K}$,有 $m_1 m_2 \neq \{m_3\}_K$,可得 $H_2 \not\sqsubset uns\_term(n_2)$。

命题 2　在命题 1 的基础上,设集合 $\boldsymbol{N} = \{n \in C: H_2 \sqsubset uns\_term(n) \wedge v_3 \not\sqsubset uns\_term(n)\}$ 有最小元 n_0,则 n_0 是常规者结点且 $sign(n_0) = +$。

证明:$n_4 \in \boldsymbol{N}$,因此集合 $\boldsymbol{N}$ 非空,故集合 $\boldsymbol{N}$ 至少有一个 $\preceq_C$ 最小元,设该最小元为 n_0;又根据 $\preceq_C$ 的性质可知 $sign(n_0) = +$。因此只需证明 n_0 是非攻击者节点即可(见图 3)。

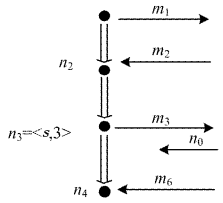

图 3　结点 n_3

下面考察所有攻击者串中发送消息的节点类型(参考攻击者模型,对各个类型的攻击者串进行分析)。

M 正文消息:$\langle +t\rangle$,$t \in T$,在 PID 串空间中 $t = H_2$,则 H_2 起源此串,这与 H_2 唯一起源于 n_3 矛盾;

F 窃听(接收消息):$\langle -g\rangle$ 没有发送消息的节点;

T 接收转发:$\langle -g, +g, +g\rangle$ 攻击者截获一条信息后又转发出去,发送消息的节点不可能是最小元节点;

C 联结:$\langle -g, -h, +gh\rangle$ 攻击者将截获到的两个消息发送出去,发送消息的节点不可能是最小元节点;

S 拆分:$\langle -gh, +g, +h\rangle$ 攻击者将截获的消息拆分后发送出去,因为 H_2 是一个 Hash 函数输出的散列值,无法拆分,所以排除此串,因此集合 $\boldsymbol{N}$ 中不存在攻击者结点,n_0 只能是常规节点。

(2)T_{num} 的保密性

证明的命题和过程与 R_{num} 的保密性的相似。

4.2　认证性

开始证明之前,引入两条本协议串空间 Σ 认证性的引理。

引理 1　C 是 PID 串空间 Σ 中的一个束,T_{num} 和 R_{num} 唯一起源于 Σ,则不存在消息项起源于 C 中一个侵入者结点,且形如 $hash(T_{num})$ 或 $hash(R_{num})$。

引理 2　若 s 是协议串空间 Σ 中一个常规串,且 $A \neq B$:

(1)若 $\{h(R_{num} \| r_2), M\}$ 起源于 s,则对 $r_2 \in \mathcal{T}/Tname, s \in Init[A, B, AS, TID, RID, r_1, r_2]$,该消息项起源于节点 $\langle s, 5\rangle$;

(2)若 $\{h(T_{num} \| h(R_{num} \| r_2), M)\}$ 起源于 s,则对 $R_2 \in r_2 \in \mathcal{T}/Tname, s \in Serv[A, AS, TID, RID, r_1, r_2]$,该消息项起源于节点 $\langle s, 4\rangle$;

(3)若 $\{h(T_{num} \| r_1), M\}$ 起源于 s,则对 $TID \in \mathcal{T}/Tname$,$s \in Resp[A, B, TID, r_1, r_2]$,该消息项起源于节点 $\langle s, 2\rangle$;

(4)若 $\{RID, M\}$ 起源于 s,则对 $RID \in \mathcal{T}/Tname, s \in Init[A, B, AS, TID, RID, r_1, r_2]$,该消息项起源于节点 $\langle s, 3\rangle$。

1)B 认证 A

命题 3　设 C 是 PID 串空间 Σ 中的一个束,$A \neq B$;在 C 中 TID 是唯一起源的。若 $s \in Resp[A, B, TID, r_1, r_2]$ 且 $C-height(s) = 3$,则 C 中必然存在常规串 $s_{Init} \in Init[A, B, AS, TID, RID, r_1, r_2]$,且 $C-height(s_{Init}) = 5$。

证明:假设 s 在 C 中的迹至少包括 $\langle -r_1, +TIDH_1, -H_3 H_4 r_2\rangle$,其中 $H_4 = h(R_{num} \| r_2)$。根据引理 1 可得 $\{H_3, H_4, r_2\}$ 起源于 C 中的常规节点。又因为 $H_4 = h(R_{num} \| r_2)$,令 $M = H_3, r_2 \in \mathcal{T}/Tname$,则根据引理 2(1)可知,该常规节点属于串 $s_{Init}, s_{Init} \in Init[A, B, AS, TID, RID, r_1, r_2]$,由于该节点为 $\langle s_{Init}, 5\rangle$ 且 $\langle s_{Init}, 5\rangle \in C$,因此 $C-height(s_{Init}) = 5$。

2)AS 认证 A

命题 4　设 C 是 PID 串空间 Σ 中的一个束,$A \neq B$;若 $s \in Serv[A, S, TID, RID, r_1, r_2]$,且 $C-height(s) = 4$,则必然存在常规串 $s_{Init} \in Init[A, B, AS, TID, RID, r_1, r_2]$ 且 $C-height(s_{Init})$ 至少为 4。

证明:假设 s 在 C 中的迹至少包括 $\langle -r_1 TIDRIDH_2, +RIDTID, -T_{num} R_{num}, +H_3 H_5 r_2\rangle$,其中 RID 唯一起源于 A,且必然起源于常规节点。因此若 $M = H_2, RID \in \mathcal{T}/Tname$,根据引理 2(4)可知,该常规节点属于串 $s_{Init}, s_{Init} \in Init[A, B, AS, TID, RID, r_1, r_2]$,由于该节点为 $\langle s_{Init}, 3\rangle$ 且 $\langle s_{Init}, 3\rangle \in C$,因此 $C-height(s_{Init})$ 至少为 3。

但是根据 PID 协议串空间可知，只要 A 接到 C 的消息，其高度 $C-height(s_{Init})$ 必大于 3。因此可得 $C-height(s_{Init})$ 至少为 4。

3)A 认证 B 和 AS

命题 5 假设 C 是 PID 串空间 Σ 中的一个束，$A\neq B$；RID 是唯一起源的，若 $s\in Init[A,B,AS,TID,RID,r_1,r_2]$，且 $C-height(s)=5$，则 C 中必然存在常规串。

① $s_{Resp}\in Resp[A,B,TID,r_1,r_2]$，且 $C-height(s_{Resp})=3$；

② $s_{Serv}\in Serv[A,S,TID,RID,r_1,r_2]$，且 $C-height(s_{Serv})=4$。

证明：假设 s 在 C 上的迹至少包括 $\langle +r_1,-TIDH_1,+r_1TIDRIDH_2,H_3H_5r_2,+H_3H_4r_2\rangle$，其中 $H_3=h(T_{num}\parallel h(R_{num}\parallel r_2))$。据引理 1 可知，$\{H_3,H_4,r_2\}$ 起源于 C 中的常规节点，令 $M=H_5$，$r_2\in\mathcal{T}/Tname$，则根据引理 2(3)可得，该常规节点属于串 s_{Serv}，$s_{Serv}\in Serv[A,S,TID,RID,r_1,r_2]$，由于该节点为 $\langle s_{Serv},4\rangle$，且 $\langle s_{Serv},4\rangle\in C$，因此 $C-height(s_{Serv})=4$。

同理可知，$C-height(s_{Resp})$ 至少为 2，但根据 PID 协议串空间可知，只要 B 收到 A 的消息，其高度 $C-height(s_{Resp})$ 必大于 2，故 $C-height(s_{Resp})$ 至少为 3；由图 3 可知 $C-height(s_{Resp})$ 的最大值仅为 3；故 $C-height(s_{Resp})=3$。

5 协议性能分析

将本文提出的协议与常规的基于 Hash 函数的 RFID 认证协议的安全性能和标签的计算性能进行分析。

5.1 标签匿名性

标签伪 ID 是由标签 ID 和随机数 r_i 通过 Hash 函数运算得出的，系统中传输的是标签的伪造 ID(PID)，不是标签的真实 ID 值。

5.2 抵抗位置跟踪攻击

位置攻击是指攻击者假冒一个合法读写器并向标签发送查询命令，通过标签的回复信息来跟踪标签。提出的协议中标签和读写器之间的认证是通过标签 PID 与随机数的 Hash 运算值实现的，每次的随机数都不同，攻击者即使获得了 Hash 值，也不能从中计算出标签的 PID 或 ID，同样也不能获得标签的位置信息。

5.3 前向安全

标签和读写器(读写器和应用服务器)之间通过 Hash 函数或者通过标签认证值和随机数的 Hash 函数值来进行认证。由于每次的随机数都不同，因此每次的 Hash 函数值亦不相同。由于 Hash 函数是不可逆的，因此攻击者不能通过标签的 ID 逆向推导出标签的伪 ID 和随机数。

5.4 双向认证

应用服务器通过计算 $H_1=h(T_{num}\parallel r_1)$ 并比较 H_1 和阅读器发送过来的 H 值来认证标签是否合法；通过计算 $H_2=h(R_{num}\parallel H_1)$ 并比较 H_2 和 $H=h(R_{num}\parallel h(T_{num}\parallel r_1))$ 是否相等来认证读写器是否合法；标签通过计算 $H=h(T_{num}\parallel H_4))$ 和 $H_3=h(T_{num}\parallel h(R_{num}\parallel r_2))$ 是否相等来认证读写器是否合法；读写器通过计算并比较 $H=h(R_{num}\parallel H_6)$ 和 $H_5=h(R_{num}\parallel h(T_{num}\parallel r_3))$ 是否相等来认证标签是否合法。只有合法的标签、读写器才能通过认证，从而实现了双向认证。

表 1 列出了 4 种常用的基于 Hash 函数的 RFID 认证协议与本文提出的协议在安全性能和计算性能上的对比。

表 1 协议安全性能和计算性能比较

	随机化 Hash lock 协议	Hash 链协议	ID 变化的协议	基于挑战-响应的协议	本文提出的协议
前向安全	√	√	√	√	√
抵抗窃听攻击	√	√	√	√	√
抵抗重传攻击	×	√	√	√	√
抵抗假冒攻击	×	×	√	√	√
标签 ID 能力	×	√	√	√	√
保留合法 ID	√	×	×	×	√
标签计算次数	1*hash*	2*hash*	2*hash*	2*hash*	1*hash*

结束语 协议采用了伪 ID 的安全认证方法，伪 ID 由合法 ID、标签认证数字和随机数派生，保留了合法的 ID。标签认证数字保证了其隐秘性，随机数保证了其不可跟踪，跟踪者即使知道 ID 也无法通过推理或运算得到新的伪 ID。利用串空间理论证明了协议的认证性，包括标签对读写器的认证、应用服务器对阅读器的认证以及阅读器对标签和应用服务器的认证。本方案适合应用于供应链的生产企业内部系统，数据库非公开，由应用服务器保护其安全，使其不被其他用户访问；阅读器和标签的认证可在应用服务器的协助下完成，而且只需哈希函数即可完成；阅读器和标签可以更新；应用服务器记录标签经过的路径和阅读器的位置。

参 考 文 献

[1] SARMA S E, WEISS A, ENGELS D W. RFID systems and security & privacy implications[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer-Verlag, 2002: 454-469.

[2] RIEBACK M R, CRISPO B, TANENBAUM A S. The evolution of RFID security[J]. IEEE Pervasive Computing, 2006, 5(1): 62-69.

[3] PATERIYA R K, SHARMA S. The evolution of RFID security and privacy: a research survey[C]// 2011 International Conference on Communication Systems and Network Technologies (CSNT). IEEE, 2011: 115-119.

[4] HENRICI D. RFID Security and Privacy: Concepts, Protocols, and Architectures[M]. Berlin: Spring, 2008.

[5] YANG X, LING J. Low-cost ultralightweight RFID mutualauthentication protocol[J]. Computer Science, 2016, 43(4): 160-162, 172. (in Chinese)
杨昕，凌捷. 一种低成本超轻量级 RFID 双向认证协议[J]. 计算机科学，2016，43(4)：160-162，172.

[6] DOLEV D, YAO A C. On the security of public key protocols [J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[7] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication[J]. ACM Transactions on Computer Systems, 1990, 8(1): 18-36.

[8] BREGA F J T. Strand spaces: proving security protocols correct [J]. Journal of Computer Security, 1999, 7(2-3): 191-230.

[9] LIU D W, LING J, YANG X. Improved RFID authentication

(下转第 176 页)

the scalar field mapping technique[C]// Proceedings of the 2013 39th Annual Conference of the IEEE Industrial Electronics Society. New York: IEEE Press, 2013: 2455-2459.

[9] ACHAKEEV D, SEEGER B, WIDMAYER P. Sortbased Query-adaptive Loading of R-trees[C]// Proceedings of 2012 the 21st ACM International Conference on Information and Knowledge Management. New York: ACM, 2012: 2080-2084.

[10] ZHANG J, PAN H, YUAN Z M. A Novel Spatial Index for Case based Geographic Retrieval[C]// Proceedings of 2009 International Conference on Interaction Sciences. New York: ACM, 2009: 342-347.

[11] PATEL P, GARG D. Perfect Hashing Base R-tree for Multiple Queries[C]// Proceedings of 2014 IEEE International Advance Computing Conference. New York: IEEE Press, 2014: 636-640.

[12] GONG J, ZHANG H W. A Method for LOD Generation of 3D City Model Based on Extended 3D RTree Index[C]// Proceedings of 2011 Eighth International Conference on Fuzzy Systems and Knowledge Discovery. New York: IEEE Press, 2011: 2004-2008.

[13] LI J, JING N, SUN M Y. A Mechanism of Implementing Visualization with Level of Detail at Multiscale[J]. Journal of Software, 2002, 13(10): 2037-2043. (in Chinese)
李军, 景宁, 孙茂印. 多比例尺下细节层次可视化的实现机制[J]. 软件学报, 2002, 13(10): 2037-2043.

[14] DENG H Y, WU F, ZHAI R J, et al. R-Tree Index Structure for Multi-Scale Representation of Spatial Data[J]. Chinese Journal of Computers, 2009, 32(1): 177-184. (in Chinese)
邓红艳, 武芳, 翟仁健, 等. 一种用于空间数据多尺度表达的 R 树索引结构[J]. 计算机学报, 2009, 32(1): 177-184.

[15] ACHAKEEV D, SEIDEMANN M, SCHMIDT M, et al. Sort-based Parallel Loading of R-trees[C]// Proceedings of the 1st ACM SIGSPATIAL International Workshop on Analytics for Big Geospatial Data. New York: ACM, 2012: 62-70.

[16] YOU S M, ZHANG J T, GRUENWALD L. Parallel Spatial Query Processing on GPUs Using R-Trees [C]// Proceedings of the 2nd ACM Sigspatial International Workshop on Analytics for Big Geospatial Data. New York: ACM, 2013: 23-31.

[17] TAO Y F, YANG Y, HU X C, et al. Instance level worst-case query bounds on R-trees[J]. The VLDB Journal, 2014, 23(4): 591-607.

[18] YIN K X, HUANG H, ZHANG H, et al. Morfit: Interactive Surface Reconstruction from Incomplete Point Clouds with Curve-Driven Topology and Geometry Control[J]. ACM Transactions on Graphics, 2014, 33(6): 1-12.

[19] SONG J, LI T T, ZHU Z L. Research on I/O Cost of MapReduce Join[J]. Journal of Software, 2015, 26(6): 1438-1456. (in Chinese)
宋杰, 李甜甜, 朱志良. MapReduce 连接查询的 I/O 代价研究[J]. 软件学报, 2015, 26(6): 1438-1456.

[20] WANG C K, MENG X F. Relational Query Techniques for Distributed Data Stream: A Survey[J]. Chinese Journal of Computers, 2016, 39(1): 80-96. (in Chinese)
王春凯, 孟小峰. 分布式数据流关系查询技术研究[J]. 计算机学报, 2016, 39(1): 80-96.

(上接第 146 页)

protocol with backward privacy[J]. Computer Science, 2016, 43(8): 128-130, 158. (in Chinese)
刘道微, 凌捷, 杨昕. 一种改进的满足后向隐私的 RFID 认证协议[J]. 计算机科学, 2016, 43(8): 128-130, 158.

[10] WEIS S A, SARMA S E, RIVEST R L, et al. Security and privacy aspects of low-cost radio frequency identification systems[M]// Security in Pervasive Computing. Springer Berlin Heidelberg, 2004.

[11] OHKUBO M, SUZUKI K, KINOSHITA. K Hash-Chain based forward secure privacy protection scheme for lowcCost RFID [C]// Proceedings of the 2004 Symposium on Crypto-graphy and Information Security(SCIS 2004). 2004: 719-724.

[12] COHEN M, DAM M. A completeness result for BAN logic[EB/OL]. [2011-06-22]. http://www.access.ee.kth.se/reports/2007/13.pdf.

[13] MOLNAR D, WAGNER D. Privacy and security in library RFID: issues, practices, and architectures[C]// Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS' 04). Washington, DC, USA, 2004: 210-219.

[14] RHEE K, KWAK J, KIM S, et al. Challenge-response based RFID authentication protocol for distributed database environment[C]// Proceedings of the 2nd International Conference on Security in Pervasive Computing (SPC 2005). Berlin: Springer-Verlag, 2005: 70-84.

[15] SHEN J, TAN H, ZHENG Y, et al. An enhanced ID-updating Hash-based RFID authentication protocol with strong privacy protection[J]. Frontiers in Artificial Intelligence & Applications, 2016, 274: 2070-2079.

[16] YUAN J S, XU Y, QI Y C, et al. Mutual authentication protocol for RFID based on asymmetric keys and hash function[J]. Journal of Cryptologic Reseatch, 2014, 1(5): 456-464. (in Chinese)
苑津莎, 徐扬, 戚银城, 等. 基于非对称密钥和 Hash 函数的 RFID 双向认证协议[J]. 密码学报, 2014, 1(5): 456-464.

[17] DING Z H, LI J T, FENG B. Research on Hash-based RFID security authentication protocol[J]. Journal of Computer Research and Development, 2009, 46(4): 583-592. (in Chinese)
丁振华, 李锦涛, 冯波. 基于 Hash 函数的 RFID 安全协议研究[J]. 计算机研究与发展, 2009, 46(4): 583－592.

[18] SAFKHANI M, PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, et al. Protocol: a hash-based RFID tag mutual authentication protocol[J]. Journal of Computational & Applied Mathematics, 2014, 259(6): 571-577.

[19] JIN Y M, WU Q Y, SHI Z Q, et al. RFID lightweight authentication protocol based on PRF[J]. Journal of Computer Research and Development, 2014, 51(7): 1506-1514. (in Chinese)
金永明, 吴棋滢, 石志强, 等. 基于 PRF 的 RFID 轻量级认证协议研究[J]. 计算机研究与发展, 2014, 51(7): 1506-1514.