DOI：10.16667/j.issn.2095-1302.2023.03.019

对轻量级移动 RFID 双向认证协议的分析与改进

崔红达，徐　森，杨　硕
（沈阳化工大学 计算机科学与技术学院，辽宁 沈阳 110020）

摘　要：随着物联网技术的不断发展，RFID 系统中读写器与后台数据库直接相连的模式已经不再适合当下的需求。读写器与后台数据库之间通过无线方式进行通信成为当下的一种主流趋势。因此传统的 RFID 双向认证协议已经不能满足需求，而目前提出的移动 RFID 双向认证协议又都面临着诸多安全问题。在分析了前人协议的基础上，提出了一种改进的轻量级移动 RFID 双向认证协议。该协议能够满足标签、读写器和后台数据库之间实现相互认证。该协议通过 Hash 加密运算和异或运算实现，满足 RFID 系统中对标签轻量级的要求。最后采用 BAN 逻辑对协议的安全性进行了进一步的验证。

关键词：RFID；双向认证协议；Hash 运算；异或运算；BAN 逻辑；轻量级

中图分类号：TP391　　**文献标识码**：A　　**文章编号**：2095-1302（2023）03-0061-03

0　引　言

RFID 系统因成本低廉，能够适应多变复杂的外界环境，且占用空间小等多方面优点，目前被广泛应用于物联网的大环境之中。从居民二代身份证到物流仓库中的产品追踪定位，再到生产线上的流水管理等，RFID 系统都发挥着不可或缺的作用。

在传统的 RFID 系统中，读写器与后台数据库之间是通过有线方式进行通信的，对于读写器与后台数据库之间的通信，通常认为是安全的 [1]。因此在设计双向认证协议时，通常将读写器与后台数据库看作一个通信主体，不需要去考虑读写器与后台数据之间的验证过程。而在移动 RFID 系统中，读写器与后台数据库之间采用无线方式通信，所以读写器与后台数据库之间不再是传统的安全信道。因此，传统的 RFID 系统中使用的双向认证协议不能再用于移动 RFID 系统中去 [2]。当下很多学者对这一问题进行了深入的研究，并提出了诸多适用于移动 RFID 系统的双向认证协议，但都存在各种问题，使得 RFID 系统的安全性不能得到保障。

针对 RFID 系统存在的安全问题，国内外的学者提出了诸多解决方案，主要分为重量级协议、轻量级协议、超轻量级协议。重量级协议采用经典密码学算法，例如 RSA、椭圆曲线加密算法以及对称加密算法等。但是由于无源标签不支持如此大量的运算和存储，因此不能得到很好的推广使用。超轻量级协议采用异或、位运算等实现加密，虽然加密算法的实现过程简单，但是因为算法的单一性，很容易遭受攻击，安全性不能得到很好的保障。轻量级协议一般采用 Hash 函数去实现加密，既满足了 RFID 系统轻量级的要求，也保证了系统的安全性。

本文参考了诸多前人的认证协议 [3-10]。文献 [3] 提出了最初的 HashLock 协议。该协议采用基于 Hash 的随机应答机制。但是最后在服务器对标签进行应答时，会将标签 ID 进行明文发送，使得攻击者可以轻易地追踪标签，因此该协议不能有效地抵御跟踪攻击等，并且该协议不适用于新型移动 RFID 系统。文献 [4] 提出了一种新形式的移动 RFID 双向认证协议。该协议能够应用到移动 RFID 系统中去，并且在该协议中采用了椭圆曲线算法对信息进行加密，具有很好的安全性。但是因为加密算法中需要大量运算，现有的轻量级移动 RFID 系统中，计算量已经超出了标签的计算能力。文献 [5] 提出了一种基于动态 ID 的移动 RFID 认证协议，但是在该协议中最后阶段涉及到了 ID 的更新过程，容易因为物理干扰或者人为破坏，而导致 ID 更新不同步的情况，因此该协议不能有效地抵御去同步化攻击。文献 [6] 提出的协议满足了移动 RFID 系统的要求，在读写器与后台服务器之间加入了验证过程，但是忽略了标签与后台服务器之间的双向认证，因此该协议不能有效地抵御攻击者发起的假冒攻击。文献 [7] 中设计的协议满足了读写器、阅读器与标签三者之间的认证过程，但是其在信息更新时，一旦出现意外情况，就会导致后台服务器与标签之间的信息不同步。因此该协议不能很好地抵御异步攻击。

基于以往研究，本文提出了一种基于 Hash 运算的轻量级移动 RFID 双向认证协议。

收稿日期：2022-05-30　　**修回日期**：2022-06-28

1 改进的轻量级移动 RFID 双向认证协议

1.1 背景消除建模

在对当前存在的传统 RFID 双向认证协议和移动 RFID 双向认证协议进行分析研究后，在这些协议的基础上，提出了一个采用动态 ID 方式的移动 RFID 双向认证协议，并且该协议能够很好地满足 RFID 系统中对标签轻量级的要求，使用伪随机数产生器替代随机数产生器，降低标签的运算量。相比较于其他认证协议，该协议能够很好地抵御异步攻击、重放攻击等多种攻击。Hash 函数因其单向不可逆的特性，被认为它在协议中是绝对安全的。表 1 给出了改进后的移动 RFID 双向认证协议涉及到的符号。

表 1 移动 RFID 双向认证协议符号

符 号	含 义
TID	标签的 ID 值
RID	阅读器的 ID 值
Nr	读写器产生的伪随机数
Nt，Ntold	Nt 为标签产生的伪随机数； Ntold 为上一次的 Nt 值
P_L，P_R	$P=H_{kt}(Nt \oplus Nr \oplus TID)$， L 和 R 表示 P 的左右部分
Q_L，Q_R	$Q=H_{kr}(RID \oplus Nt \oplus Nr)$， L 和 R 表示 Q 的左右部分
kr，kt	分别对应服务器与阅读器和标签的共享密钥
preTID，preRID	分别对应上一轮认证的标签和阅读器的 ID 值
curTID，curRID	本次验证成功更新的标签 ID 和读写器 ID

1.2 协议的认证过程

本文提出的改进移动 RFID 双向认证协议如图 1 所示。

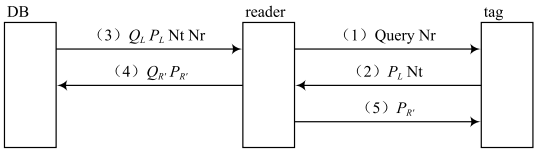

图 1 协议执行

（1）阅读器首先向标签发送质询请求并发送一个随机数 Nr。

（2）标签接到请求后，产生伪随机数 Nt，计算 $P=H_{kt}(Nt \oplus Nr \oplus TID)$，将计算结果分为左右两部分，将 P_L 以及 Nt 作为对读写器的应答，并保留 P_R 的值，便于接下来对于读写器身份的验证。

（3）阅读器接收到标签的应答后将自身保存的 Nt' 与 Nt 值进行比较，若相等则终止认证，否则计算 $Q=H_{kr}(RID \oplus Nt \oplus Nr)$，将计算结果分为左右部分，将 Q_L、Nr 以及标签传递过来的消息发送给服务器。

（4）服务器接收到消息后，先判断 Nr 的值是否与自身保存的 Nr' 相等，若相等，终止认证，否则验证读写器的身份。从数据库中得到 curRID 和 cur_kr 的值，计算 $Q_L'=H_{kr}'(RID' \oplus Nt \oplus Nr)L$ 是否与 Q_L 相等，若不相等，从数据库中取出上一轮的 preRID 和 pre_kr 再次计算 Q_L' 的值是否与 Q_L 相等，若不相等则终止认证，否则开始验证标签的身份。从数据库中得到 curTID 和 cur_kt 的值，计算 $P_L'=H_{kt}(Nt \oplus Nr \oplus TID)L$ 是否与 P_L 相等，若不相等，从数据库中取出上一轮的 preTID 和 pre_kt 再次计算 P_L' 的值是否与 P_L 相等，若不相等则终止认证，若相等则开始更新对应信息。更新 pre_kr=kr，pre_kt=kt，preRID=RID，preTID=TID，cur_kr=H_{kr}(kr $\oplus$ RID)，cur_kt=H_{kt}(kt $\oplus$ TID)，curRID=H_{kr}(Nr $\oplus$ RID)，curTID=H_{kt}(Nt $\oplus$ TID)，并将 P_R' 与 Q_R' 发送给阅读器作为答复。

（5）读写器将自身保存的 Q_R 与 Q_R' 进行比较，若不相等，则认证失败，否则读写器与后台服务器之间的双向认证完成，读写器开始更新对应的 kr 和 RID，并将 P_R' 发送给标签。

（6）标签接收到消息后，拿出自身保存的 P_R 与 P_R' 进行比较，若不相等，则认证失败，否则更新 TID 与 kt 的值。

2 协议安全性分析

本文改进的协议运用了 Hash 不可逆运算、异或运算，以及伪随机数产生器等多项安全技术，在每轮认证中，信息都是变化的，因此协议具有良好的安全性。

2.1 跟踪攻击

跟踪攻击主要是通过追踪标签时在每轮认证过程中发出的一致消息，但是该协议内消息二中的消息随机数 ID 和密钥在每轮消息认证过程中都是动态改变的，即使追踪者每次都能拿到对应的消息，但是因为 Hash 函数具有单向且不可逆的性质，因此攻击者不能追踪到标签的 ID 值。

2.2 异步攻击

异步攻击是目前大多数采用动态 ID 机制协议普遍面临的问题。异步攻击发生在服务器端和标签端及读写器端，进行信息更新时，通过外界干扰，使它们之间存储的信息不同步，进而导致下次认证失败。在每次的协议认证过程中，都会对上一次的 ID 值进行保存，当发现认证不通过时，不会马上终止协议的认证，而是通过对应的 ID 去寻找上一次认证过程中的 preID，看能否完成认证，从而有效地避免了异步攻击的问题。

2.3 重放攻击

重放攻击也是目前大多数协议中普遍存在的问题，攻击者通过截获上一轮认证的消息，在下一轮认证的过程中，冒

充通信参与的一方，将上轮解惑的消息无改动地发送，以达到欺骗的目的。该协议中引入动态 ID 以及密钥的机制，每轮的消息认证都会产生不同的结果；同时该协议还采用了过滤机制，因此攻击者不能在服务器、读写器和标签之间成功地进行重放攻击。

2.4 中间者攻击

在本协议中攻击者想要实施中间者攻击就必须要获得随机数 Nt 和双方共享的密钥 kt 或者 kr，通过重新构造 P_L 或 Q_L 的值替换原本的认证信息，去达到认证的目的。但是由于该协议中的 ID 值和密钥值每轮都是经过更新随机产生的，且 ID 和密钥并没有以明文的形式出现过。因此，该协议能够成功地抵御中间者攻击。

2.5 双向认证

本协议通过计算 $P=H_{kt}(\text{Nt} \oplus \text{Nr} \oplus \text{TID})$ 和 $Q=H_{kr}(\text{RID} \oplus \text{Nt} \oplus \text{Nr})$ 的对应左右部分，完成了双向认证的要求；并且为了提高效率，及时发现重放攻击，读写器和后台服务器中分别保存了标签以及读写器上一轮产生的随机数，能够很好地完成双向认证过程。表 2 为该协议与其他协议的比对结果。

表 2 移动 RFID 认证协议安全性对比

协 议	跟踪攻击	异步攻击	重放攻击	中间者攻击	轻量级
改进协议	√	√	√	√	√
文献 [3] 协议	×	√	√	×	√
文献 [4] 协议	√	√	√	√	×
文献 [5] 协议	√	×	×	√	√
文献 [6] 协议	√	×	√	√	√

3 改进协议的形式化分析与证明

BAN 逻辑是最早提出的验证协议安全性的一种形式化分析工具，过程大致分为以下几步：

第一步，将协议形式化描述；

第二步，初始化假设；

第三步，确立验证所需要达到的结果；

第四步，形式化分析与验证。

下面就本文改进的协议进行 BAN 逻辑分析验证。

下面的形式化描述中 D 代表后端服务器，T 代表标签，R 代表读写器，kt 和 kr 分别代表服务器与标签和读写器之间的共享密钥，Nt 和 Nr 表示标签和读写器产生的随机数，RID 和 TID 为读写器与标签的 ID 标识。

（1）协议的形式化描述

1) $R \to T$:#(Nr)

2) $T \to R$: #(Nt), (Nt, Nr, TID)L_{kt}

3) $R \to D$: #(Nr), #(Nt),(Nt, Nr, TID)L_{kt}, (Nt, Nr, RID)L_{kr}

4)$D \to R$: (Nt, Nr, TID)R_{kt}, (Nt, Nr, RID)R_{kr}

5)$R \to T$: (Nt, Nr, TID)R_{kt}

（2）初始化假设

1)$D \mid\equiv D \xleftrightarrow{kt} T$ 2)$D \mid\equiv D \xleftrightarrow{kr} R$

3)$T \mid\equiv D \xleftrightarrow{kt} T$ 4)$R \mid\equiv D \xleftrightarrow{kr} R$

5)$D \mid\equiv T \mid\Rightarrow$ TID 6)$T \mid\equiv D \mid\Rightarrow$ TID

7)$R \mid\equiv D \mid\Rightarrow$ RID 8)$D \mid\equiv R \mid\Rightarrow$ RID

9)$R \mid\equiv$ #(Nr) 10)$T \mid\equiv$ #(Nt)

（3）协议目标的形式化描述

1)$T \mid\equiv D \mid\equiv$ TID 2)$R \mid\equiv D \mid\equiv$ RID

3)$D \mid\equiv T \mid\equiv$ TID 4)$D \mid\equiv R \mid\equiv$ RID

3 逻辑推理及验证

3.1 验证目标 1：$T \mid\equiv D \mid\equiv$ TID

因为 TID=(Nt ⊕ TID)，由初始化假设 10 以及消息新鲜性规则 $\frac{p \mid\equiv \#(x)}{p \mid\equiv \#(x, y)}$ 可得 $T \mid\equiv \#(\text{TID})_{kt}$。由初始化假设 3 可知 $T \mid\equiv D \xleftrightarrow{kt} T$，联合上面得到的两个结果，由消息意义规则 $\frac{P \mid\equiv Q \xleftrightarrow{k} P \quad P \lhd (X)_k}{p \mid\equiv Q \mid\sim X}$，可得 $T \mid\equiv D \mid\sim$ TID。因为 $T \mid\equiv \#(\text{TID})$、$T \mid\equiv D \mid\sim$ TID，由随机数验证规则 $\frac{P \mid\equiv \#(X) \quad P \mid\equiv Q \mid\sim \text{X}}{p \mid\equiv Q \mid\equiv X}$ 得到 $T \mid\equiv D \mid\equiv$ TID。

3.2 验证目标 2：$R \mid\equiv D \mid\equiv$ RID

因为 RID=(Nr ⊕ RID)，由初始化假设 9 和消息新鲜性规则 $\frac{p \mid\equiv \#(x)}{p \mid\equiv \#(x, y)}$，能得到 $R \mid\equiv \#(\text{RID})$。由协议的形式化描述 4 得到 $R \lhd (\text{Nt, Nr, RID})_{kt}$。由消息接收规则 $\frac{P \lhd (x, y)}{p \lhd x}$，得到 $R \lhd (\text{RID})_{kr}$。由初始化假设 4 可知 $R \mid\equiv D \xleftrightarrow{kr} R$，联合上面得到的两个推论结果，再由消息意义规则 $\frac{P \mid\equiv Q \xleftrightarrow{k} P \quad P \lhd (X)_k}{p \mid\equiv Q \mid\sim X}$，可得 $R \mid\equiv D \mid\sim$ RID。因为 $R \mid\equiv \#(\text{RID})$、$R \mid\equiv D \mid\sim$ RID，由随机数验证规则 $\frac{P \mid\equiv \#(X) \quad P \mid\equiv Q \mid\sim X}{p \mid\equiv Q \mid\equiv X}$ 得到 $R \mid\equiv D \mid\equiv$ RID。

同理，结合初始化条件以及 BAN 逻辑的规则可以完成目标 3 和 4 的证明，并且证明方式与目标 1 和 2 相同。这里因为篇幅有限，不再进行证明。

4 结 语

本文在研究前人提出的 RFID 双向认证协议的基础上，

（下转第 66 页）

4 结 语

在物联网技术应用过程中，将物联网设备的数据直接暴露于网络中，将面临着巨大的安全风险。确保数据接入的安全性和可靠性是本文研究的重点问题。一方面，当前的物联网技术并没有提供数据接入的接口规范；另一方面，物联网设备也呈现出日新月异的变化。针对这种情况，设计一种合理的数据接入方法不仅能有效减少安全性问题，还能显著提高异构物联网设备的兼容问题。

在前人研究的基础上，优化了物联网应用项目的典型结构，在每个组成部分中增加设备注册和功能注册模块。设备注册模块用来验证设备接入对象的合法性，而功能注册模块用来验证功能接入对象的合法性。没有注册的设备和功能，无法访问数据中心对象对应的数据域。注册的设备和功能，通过加密算法封装数据包，确保数据接入的安全性和可靠性。实践结果表明，这种数据接入方法能够克服异构物联网设备的结构差异，安全可靠地将异构设备节点对象接入数据中心对象，并由服务终端对象可靠地访问。这种数据接入方法规范了设备节点对象、数据中心对象和服务终端对象之间的数据对接流程，可以防止非法入侵或避免意外的错误，从而减少不必要的经济损失和系统风险。

参 考 文 献

[1] 马亚蕾 . 物联网安全架构及关键技术研究 [J]. 电子制作，2017，24（11）：84-85.

[2] 方祥毅 . 大数据时代信息安全的隐患和建议 [J]. 信息与电脑（理论版），2014，8（1）：160-161.

[3] 李宗辉，许旭江 . 物联网信息安全与隐私保护研究 [J]. 无线互联科技，2021，18（20）：11-12.

[4] 任伟 . 物联网安全架构与技术路线研究 [J]. 信息网络安全，2012，12（5）：70-73.

[5] 黄军友 . 农场异构设备物联网数据接入控制机制研究 [J]. 五邑大学学报（自然科学版），2014，28（1）：28-35.

[6] 刘述波，仲春林，姜宇轩，等 . 综合能源物联网设备接入安全认证方法研究 [J]. 电力安全技术，2020，22（9）：4-7.

[7] 张喜平，赵维，王丽杰 . 新能源大数据平台物联网数据接入架构设计与实现 [J]. 分布式能源，2020，5（6）：33-38.

[8] 陈艳，宋英华 . 新型配电物联网后台系统架构设计与关键技术研究 [J]. 供用电，2020，37（2）：41-46.

[9] 甄凯成，黄河，宋良图 . 基于 Netty 和 Kafka 的物联网数据接入系统 [J]. 计算机工程与应用，2020，56（5）：135-140.

[10] 陈庆奎，吕晓明，郝聚涛，等 . 一个物联网异构数据接入系统 ChukwaX [J]. 计算机工程，2012，38（17）：12-15.

（上接第 63 页）

针对其中存在的安全问题以及系统成本双方面考虑，提出了改进的轻量级移动 RFID 双向认证协议。通过对协议的安全性分析以及形式化分析，结果显示该协议能够很好地抵御各种攻击，且满足 RFID 系统轻量级的要求。

参 考 文 献

[1] 占善华 . 基于交叉位运算的移动 RFID 双向认证协议 [J]. 计算机工程与应用，2019，55（7）：120-126.

[2] 梅松青，邓小茹 . 位替换运算的超轻量级移动 RFID 认证协议 [J]. 计算机工程与应用，2020，56（3）：100-105.

[3] LEE K. A two-step mutual authentication protocol based on randomized hash-lock for small RFID networks [C]// 2010 Fourth International Conference on Network and System Security. Melbourne，VIC，Australia：IEEE，2010：527-533.

[4] 杨玉龙，彭长根，周洲，等 . 基于 Edwards 曲线的移动 RFID 安全认证协议 [J]. 通信学报，2014，35（11）：132-138.

[5] 肖红光，陈蓉，巫小蓉，等 . 基于动态密钥的移动 RFID 安全认证协议 [J]. 计算机工程与应用，2016，52（22）：113-117.

[6] SUNDARESAN S，DOSS R，PIRAMUTHU S，et al. A secure search protocol for low cost passive RFID tags[J]. Computer networks，2017，122（20）：70-82.

[7] 霍成义 . 移动 RFID 双向认证协议设计与分析 [J]. 无线电工程，2014，44（8）：1-4.

[8] FELDHOFER M，RECHBERGER C. A case against currently used Hash functions in RFID protocols [C]// Proceedings of OTM Confederated International Conferences "On the Move to Meaningful Internet Systems". Berlin，Heidelberg：Springer，2006.

[9] CHIOU S Y，KO W T，LU E H. A secure ECC-based mobile RFID mutual authentication protocol and its application [J]. International journal of network security，2018，20（2）：396-402.

[10] ZHENG L，SONG C，CAO N，et al. A new mutual authentication protocol in mobile RFID for smart campus [J]. IEEE access，2018（6）：60996.

作者简介：崔红达（1998—），男，辽宁人，硕士，研究方向为射频识别认证协议分析。

徐 森（1975—），男，黑龙江人，博士，讲师，研究方向为信息安全、安全协议设计与分析。

杨 硕（1983—），男，吉林人，博士，讲师，研究方向为计算机视觉、目标跟踪和立体匹配。