一种轻量级 RFID 系统抵抗克隆攻击方法

赵伯侯　2021302181156　武汉大学

摘要：射频识别技术（Radio Frequency Identification, RFID）在物联网中有着不可或缺的地位，依靠其快速识别、强大的抗干扰能力和适应恶劣环境的特性，使其广泛应用于物流产品跟踪、居民二代身份证等领域。本文旨在介绍 RFID 系统的硬件组成和工作原理，并探讨其中应用的安全认证协议。传统 RFID 系统中的标签常受克隆攻击威胁，因此，本文提出了一种基于 hash 链的抵抗克隆攻击方法。尽管尚未进行实验验证，但对该方法的优缺点进行了简要分析和假设。

关键词：射频识别系统；轻量级安全协议；克隆攻击；hash 链

1. 引言

RFID 系统因为有着较低的成本和较强的抗干扰能力，目前被广泛应用于物联网的各个方面中，居民二代身份证、物流仓库中的产品跟踪定位、门禁系统中都能看到 RFID 技术的身影。

RFID 系统的安全性至关重要，尤其是在涉及到敏感信息或重要资产的场景中。传统 RFID 标签在设计上缺乏抵抗克隆攻击的能力，这为潜在的攻击者提供了入侵的机会，可能导致严重的安全问题。为了解决这一问题，本文提出了一种基于 hash 链的方法，旨在增强 RFID 标签的安全性，防范克隆攻击的威胁。

2. RFID 基础理论

2.1 硬件组成

完整的射频识别硬件系统由标签、阅读器、天线和应用程序组成。下面对这四个硬件进行分别的介绍：

2.1.1 标签

标签由芯片和耦合元件构成，标签内部的耦合元件可以接受阅读器发送的电磁波，从而在标签内部产生电流。由于标签的成本较低且使用寿命较长，使得其被广泛应用在活动识别、手势识别、室内定位等场景。[1]

2.1.2 阅读器

阅读器按照工作频率可以分类为低频、高频、超高频和微波四种，频率越高读取的距离也就越远。阅读器可以通过连接多个天线来获取来自不同通道的数据。

2.1.3 天线

天线以集成或者外接的形式与阅读器连接，主要作用是发送和接收无线信号，实现阅读器和标签之间的通信。[1]

2.1.4 应用程序

应用程序作为 RFID 的核心，控制着整个交互流程，在应用场景中，由于标签的存储能力和计算能力有限，所以需要应用程序来代替其完成相应的工作。[1]

2.2 工作流程

对于无源标签来说，当电子标签进入到天线的磁场中后，如果能够接受到阅读器发出的特殊的射频信号，就能凭借感应电流的能量发送出存储在芯片中的信息；对于有源标签来说则是主动发送某一频率的信号，阅读器读取到信息并完成解码之后交给应用程序进行处理

2.3 应用场景

RFID 系统在众多场景中都有使用，在仓库运输时可以给货物镶嵌 RFID 芯片使得在物流过程中系统随时掌握货物的相关信息；在门禁系统中可以提前使用录入身份的标签来验证使用者的身份信息；在车辆调度系统中也可以使用 RFID 来自动识别车辆号码进而省去大量人工统计时间并且可以提高精确度。

3.RFID 安全认证协议

3.1 RFID 安全认证协议攻击方式

RFID 常见的攻击方式有如下几种

（1） 拒绝服务攻击，也称淹没攻击，攻击者向服务器发送多个信号导致信号被淹没使系统丧失正确处理输入数据的能力。[2]

（2） 去同步攻击，破坏目标标签与应用程序之间的同步状态。[2]

（3） 泄露风险，破解 RFID 系统中的通信密钥。[2]

（4） 克隆攻击，攻击者获取标签内容后复制能够与阅读器交互的复制体。[2]

（5） 中间人攻击，攻击者截获标签与阅读器的交互信息并进行修改。[2]

（6） 重放攻击，攻击者捕获标签数据并将其重新发送给读取器,以与读取器通信并获取秘密信息。[2]

4.RFID 安全认证协议最新成果

查找最近文献可以找到多种对轻量级 RFID 安全认证协议的改进方法：

通过双向轻权认证协议来保护 RFID 系统的安全性和隐私，随机化标签的秘密信息再哈希的方法生成会话消息，标签与阅读器间采用二次相互认证的轻量级安全认证协议。使用 hash 运算确保认证过程中的保密性和完整性，通过对会话信息的随机化确保消息的新鲜行，通过对秘密信息的更新满足前向安全性。[3]

通过改进轻量级移动 RFID 双向认证协议，使用 hash 运算和异或运算，从而满足标签、阅读器和后台数据库之间的相互认证。[4]

通过将动态会话密钥长度进行压缩来降低标签的存储消耗，然后将处理后的输入进行异或和移位等逻辑运算，最后通过按位异或的逻辑操作缩短输出的数据长度来降低计算成本和复杂度来实现在轻量级 RFID 在存储能力有限的条件下防止隐私数据泄露的问题。[5]

5．解决方案

需要 RFID 安全认证协议能够抵抗克隆攻击也就是说我们需要防止标签中的内容被复制后能够直接被攻击者使用，所以想要在轻量级安全认证协议中引入 hash 链来阻止克隆攻击。

因为轻量级 RFID 的存储性能和运算性能有限，所以我们不能将整个标签中保存的用户认证 id 作为 hash 函数的种子，我们可以取用户认证 id 的一部分作为 hash 函数的种子，这里具体取用的位数需要根据实际 RFID 芯片的运算能力进行讨论。在标签中保存有最原始的用户认证 id（这里记作 seed），并且只允许标签内部读取 seed，不允许外界读取该部分的内容。

整个 RFID 系统的身份认证过程为首先阅读器的天线发射特定频率的信号被标签接收到，标签利用内部的线圈收集到天线释放的能量之后对 seed 进行 hash 运算，将 hash 运算 n 次的结果以及另外一部分的用户 id 值拼接之后向外发送，阅读器的天线接收到标签发来的信息之后首先通过未加密的用户 id 值确定用户的身份，然后读取数据库中该用户的 seed，将 seed 同样进行 n 次 hash 运算后与接收到的信息进行比对，若比对结果在误差范围内则用户身份认证成功。反之则视为非法访问。验证之后阅读器通过天线向标签发送验证成功信号，阅读器和标签内部的计数器由 n 变为 n-1。

因为外界能够读取到的标签的信号有两部分，并且由于使用了 hash 链技术，

使得攻击者读取标签时只能读取到本次认证的值，得益于 hash 函数的单向性，并不能计算出 seed 的值，由此实现防止攻击者对标签进行克隆攻击。

6. 结论

因为只能对提出的解决方案进行理论分析，没有进行实验验证的条件，所以下面对于该方案的分析部分均为猜测。

要完成这种解决方案，原始的标签中就需要加入能够进行数次的 hash 运算算模块以及对 seed 进行保存的不可读内存模块或者加密内存模块。这两个模块无疑会增加标签的成本，这样是否会与轻量级标签的规则相违背需要具体的实验进行验证。

因为轻量级 RFID 的运算能力有限，所以对标签进行初始化的时候不太可能将 n 的值设置为较大的值，因为这样会加重每次标签进行 hash 运算的负担，同时因为 hash 链的寿命问题，将 n 设置为较小的值后必须考虑标签每使用一定的次数就需要与服务器重新进行初始化的问题。所以 n 值具体设置怎样的值才会使得整个标签的利用效率最高需要具体的实验进行验证。

因为标签在接收到阅读器天线发出的成功认证信息后会将内部的计数器进行减 1，所以攻击者是不是可以通过仿造阅读器的成功认证信号将其多次发送给标签从而进行去同步攻击。通过破坏数据库与标签中的计数器同步状态来破坏整个 RFID 系统。

参考文献

[1] 殷宪祯. 基于 RFID 信号特征的安全认证技术研究与应用[D].南京邮电大学,2023.DOI:10.27251/d.cnki.gnjdc.2022.000034.

[2] 寇广岳, 魏国珩, 平源, 等. RFID 安全认证协议综述[J]. 计算机工程与科学, 2023, 45(01):77-84.

[3] 史志才.RFID 系统的安全性和隐私保护方法[J/OL].电子科技:1-6[2024-05-10].https://doi.org/10.16180/j.cnki.issn1007-7820.2025.02.010.

[4] 崔红达,徐森,杨硕.对轻量级移动 RFID 双向认证协议的分析与改进[J].物联网技术,2023,13(03):61-63+66.DOI:10.16667/j.issn.2095-1302.2023.03.019.

[5] 包红琦. 一种面向 RFID 的轻量级安全认证协议[D].哈尔滨师范大学,2024.DOI:10.27064/d.cnki.ghasu.2023.001972.