DOI:10.19304/j.cnki.issn1000-7180.2015.09.029

低碳供应链环境下物联网 RFID 可信度研究

杨传明
(苏州科技大学 商学院,江苏 苏州 215009)

摘 要: 针对低碳供应链环境下物联网可信度的相关要求,提出一种基于供应链的 RFID 改进随机 Hash 锁协议. 结合随机预言模型安全理论(ROM),运用数据进行实验. 结果表明,该协议实现了访问认证、匿名安全、防重传性、防追踪性、数据问责、缩时增效和成本优势,可有效提升低碳供应链环境下物联网可信度.

关键词: 可信度;RFID;物联网;低碳供应链
中图分类号: TP393.04 **文献标识码**: A **文章编号**: 1000-7180(2015)09-0144-04

Study on the Credibility of Internet of Things RFID Under Low-Carbon Supply Chains Enviroment

YANG Chuan-ming
(Business School, Suzhou University of Science and Technology, Suzhou 215009, China)

Abstract: Based on a detailed analysis of the requirements of the internet of things reliability under low-carbon supply chains environment, this paper proposes an improved random Hash lock protocol of RFID to suit supply chains. Proved by the experiment based on the ROM security theory, the protocol can solve the security problems of access certification, anonymous security, anti retransmission, anti-tracking, data accountability, efficiency and cost, and improve the credibility of internet of things under low-carbon supply chains environment effectively.

Key words: credibility; RFID; internet of things; low-carbon supply chains

1 引言

伴随着工业化城镇化的加速,能源耗费及碳排放量迅猛上升,面对着日益严峻的国内外节能减排压力,建设有效的低碳供应链成为实现可持续发展、增强综合竞争力的必然选择. 而物联网技术则是利用无线射频识别(RFID)、传感器等信息设备,将供应链涉及的所有物品信息通过互联网相连,实现物体的智能全方位定位跟踪和监控管理. 其通过数字化物质知识有效降低供应链信息传输耗费,借助泛在化远程控制提升效率并节省成本,利用智能化管理决策节约资源能耗,从而成为推动低碳供应链健康发展的强力支撑.

2010 年,IBM、Intel 和微软引领 300 余家公司成立了国际可信度组织. 从技术角度而言,可信度目的是保护设计者和所有者的信息不被非法用户窃取或使用. 随着物联网在低碳供应链的广泛应用,由于存在众多终端、高智能程度、有限能量处理和人工监控困难等原因,其可信度也越来越受到重视. 按照国际物联网协会的划分,物联网依照技术构架可分为感知层、网络层和应用层. 感知层主要通过无线射频识别系统(RFID)采集物品信息构成;网络层主要涉及通信及互联融合网络;应用层主要融合物联网与行业专业技术. 三层中最为关键的是感知层,因此,低碳供应链环境下物联网可信度的核心在于提升感知层中 RFID 系统的可信度.

收稿日期: 2014-11-21; 修回日期: 2014-01-15
基金项目: 国家自然科学基金资助项目 (71071141);教育部人文社科基金资助项目 (13YJC630199);江苏省高校哲学社科基金资助项目 (2012SJB630059);江苏省高校研究生科研创新计划资助项目 (CXZZ13_0847)

本文从物理机制和协议机制剖析现有 RFID 安全机制存在的问题，设计一种基于供应链的 RFID 改进随机 Hash 锁协议，以求更好地提升供应链环境下物联网的可信度.

2　供应链环境下 RFID 系统可信度要求

RFID 系统主要是由标签、天线、读卡器及后端数据库组成. 标签由耦合线圈与逻辑门电路组成用于存储数据，可分为主动式标签、被动式标签和半被动式标签. 读卡器主要用于读写标签，其到标签之间分为前向及后向信道. 供应链环境下物联网的每个节点企业均配有自身的 RFID 系统，运用读卡器读取上下游企业物品标签，结合后端数据库获得物品详细信息，而由于 RFID 系统信道通信均采用非接触暴露式无线信道，极易从以下几个方面威胁物联网的可信度.

第一、干扰拒绝. 现行 RFID 主要采用低频信号(13.56 MHz 和 125 MHz)及高频信号(433.56 MHz、915 MHz、2.45 GHz 和 5.8 GHz)[1]，而相邻频带之间会产生较强的干扰，从而导致标签混淆应答、写入休眠、识别错误等拒绝服务通信故障.

第二、窃取信息. RFID 标签中存储了大量物品信息，非法用户可通过设置关联物品清单，借助大能量读卡器及大尺寸天线远距离窃取清单物品标签信息，获得物品价格种类数量等商业信息.

第三、重传伪装. 非法用户通过窃取标签响应，利用设备改写可重写标签基本信息，并将其伪装为合法标签，响应合法读卡器询问，从而篡改物品基本数据；或通过人为信号干扰修改标签安全码，使得标签拒绝合法读卡器，干扰供应链物联网服务.

第四、位置跟踪. 非法用户可借助非授权读卡器多次询问标签，获得标签动态数据，分析标签响应，在非许可情况下追踪物品及商家行动路径.

第五、数据追踪. 非法用户窃取了供应链某一环节标签信息后，运用数据演绎追踪推测供应链其他标签信息，获取供应链物联网 RFID 系统数据.

为了更好地应对以上问题，要求低碳供应链环境下 RFID 系统满足健壮可靠性、读写认证性、所有权转移、匿名安全性、回溯安全性等要求. 其中健壮可靠性为保证通信协议失效或者频带受到干扰情况时，系统可以自行恢复信息流；读写认证性要求只有合法授权用户才能访问标签数据；作为典型分布松散结构，供应链节点企业即合作又竞争，为了保护商业机密避免利益冲突，节点企业在处理完 RFID 标签后，应实现所有权转移；匿名安全性通过加密系统 ID 防止窃取信息及重写伪装；回溯安全性可切断供应链前后向关联度以防止位置及数据追踪.

3　RFID 系统安全机制

由于成本因素，商业 RFID 系统必须精炼物理电路配备，在满足基础操作后，仅有少量电路为安全等用途服务；且极小体积和弱微电源均限制了复杂加密方法的运用. 针对 RFID 系统特点，现有研究主要从物理和协议机制两方面入手.

3.1　物理机制

物理机制主要使用法拉利屏蔽、主动干扰、Kill 标签命令等物理方法[2]. 法拉利屏蔽通过为每个物品套上金属制网罩阻断前后向通信以屏蔽标签，但该方法显然无法针对供应链海量物品实施. 主动干扰指用户使用信号设备干扰读取受保护标签，但此方法在增加成本的同时，可能会干扰合法 RFID 系统运行. Kill 标签命令在标签信息被读取后，通过物理方法牺牲标签，但低碳供应链环境下标签的回溯性及低成本要求使得该方法无法广泛采用.

3.2　协议机制

相对物理安全机制，软件协议机制更适合低碳供应链环境下物联网要求，其主要利用密码方案和机制设计创建符合可信度的协议. 主要协议分析如下所示.

(1)ISO15693/IEC15693 的两种标准安全协议模式[3]. 模式一设置非冲突避免 64 字节 ID，利用伪随机码生成器为每个标签配置带有独特随机码的 32 个字节反馈. 但非法用户可利用 32 字节线形反馈移位器或 Massey 等特定解密算法，破解随机码追溯用户标签 ID. 模式二采用插槽模式或非插槽模式为标签配备排他性 64 字节的微小流量调节(MFR)标签 ID，根据物品目录命令要求对 MFR 标签 ID 采取无存取控制式反馈，而非法用户可利用无控制缺陷获得物品标签信息. 其中两种模式的基本原理均为读卡器发射可变长度屏蔽信息，使对应标签产生响应，同时静默非对应标签. 而非法用户可通过对单字节的双次屏蔽查询发现响应标签，借助 64 次单字节增加查询，窃取标签冲突避免 ID，进而掌控 MFR 标签 ID.

(2)Hash 协议. 主要分为 Hash 链、Hash 锁及随机 Hash 锁三种协议[4]. Hash 链协议通过创建一定数量的杂凑函数，对标签和读卡器提出请求认证，

ID 可运用不同应答实现自主更新. 但该协议仅能实现标签的单向身份认证,一旦 ID 被截获,极易受到重传伪装攻击;且每次标签认证均需多次杂凑运算,大大增加了计算负荷及时间成本. Hash 锁利用单向 Hash 函数产生 metaID 保护标签 ID,但其 metaID 及 ID 不能动态刷新且明文传送信息,易受到追踪和重写伪装攻击. 随机 Hash 锁协议采用随机数的挑战响应机制,但标签与读卡器间信道存在大量明文形式的数据通信,一方面易受到数据伪装及追踪式攻击,另一方面无法适用于供应链海量物品标签情形.

(3)其他协议. 杂凑 ID 变化协议通过随机数动态更新标签信息抗拒重传式攻击[5]. 但标签与后端数据库信息更新不同步,若非法用户攻击更新的后端数据库,即可阻断标签的后向认证. YA-TRAP 协议通过单调递增时间戳抵抗追踪[6],但易受到干扰拒绝攻击. 改进 YA-TRAP 协议及 LPN 协议通过共享密钥方式识别标签,供应链节点特殊利益关系下无法保证密钥共享性[7].

综上所述,物理机制、协议机制虽然均能在一定程度上保障安全,但各自均存在问题. 因此,研究一种 RFID 系统的安全协议成为保障低碳供应链环境下物联网可信度的当务之急.

4 基于供应链的 RFID 可信度协议

在分析供应链物联网特点及现有 RFID 安全机制的基础上,借助改进随机 Hash 锁协议,设计基于供应链的 RFID 可信度协议,并结合随机预言模型安全理论进行数据实验证明协议可信度.

4.1 基于供应链的 RFID 可信度模型

设供应链每个节点企业拥有自己的 RFID 读卡器及后端数据库,供应链物流中包含 n 个 RFID 标签. 由于 RFID 可信度问题主要产生于标签和读卡器间的前向通信信道,而企业读卡器与后端数据库因通讯距离短而相对安全,在一定程度上可认作同一通信实体. 模型首先假设非法用户可控制所有实体通信,能通过发起实体间对话,实施干扰拒绝、窃取信息、重传伪装、位置跟踪和数据追踪等行为.

现有 Hash 函数均利用分组密码散列算法进行构造,非法用户亦可通过密码攻击破坏 Hash 函数以窃取信息;现有研究表明可采用 MD5、SHA 等方法保证 Hash 函数自身安全,但均存在散列扩散过度等种种缺陷[8]. 为此,本文基于已有研究成果,采用 AES 非线性映射方法建立 Hash 函数保障算法安全,依照随机预言模型安全理论设置实验数据重点关注信道传输安全.

4.2 协议描述

(1)系统设置

默认供应链节点企业初始接收标签(T_i,$1 \leqslant i \leqslant n$)时,标签处于安全模式状态,且仅有该节点企业有权限修改标签状态. T_i 包含初始随机化标识符 r_i 及标签序列号 ID_i,后端数据库 TS 每一条记录对应着各标签的随机化标识符,并包含标签初始位长、指示器和标志位等数据信息.

(2) 协议流程

第 t 次读卡器访问标签流程如图 1 所示.

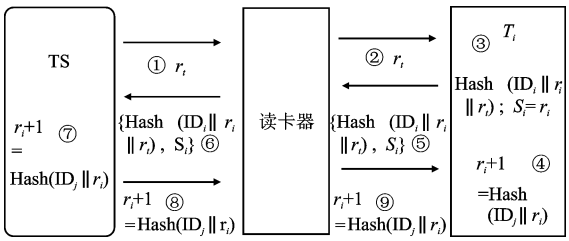

图 1 协议流程图

Step1:受到读卡器请求,TS 随机生成密码 r_t,传输给读卡器.

Step2:读卡器传送 r_t 至 T_i 并将其激活.

Step3:T_i 利用自身状态设置的 TS 及 ID_i,结合 r_i,计算 $Hash(ID_i \| r_i \| r_t)$.

Step4:T_i 生成 $s_i = r_i$,将标识符更新为 $r_i + 1 = Hash(ID_i \| r_i)$.

Step5:T_i 将 $Hash(ID_i \| r_i \| r_t)$ 及 s_i 返还读卡器.

Step6:读卡器将 $Hash(ID_i \| r_i \| r_t)$ 及 s_i 返还给 TS.

Step7:根据 s_i,TS 在数据表中检测是否存在 ID_j,使得 $Hash(ID_j \| s_i \| r_t) = Hash(ID_i \| r_i \| r_t)$,存在则认证成功,否则失败.

Step8:TS 重置随机标识符 $r_i + 1 = Hash(ID_j \| r_i)$,并新建记录 RD_j 与之对应. 再发送 $r_i + 1$ 给读卡器并转发至 T_i.

Step9:T_i 验证是否存在 $Hash(ID_j \| r_i) = Hash(ID_i \| r_i)$,存在则认证成功,否则用 s_i 替换 $r_i + 1$,并将 r_i 恢复至初始化状态.

4.3 实验数据处理

项目组在 SQL SERVER 2012 中模拟存储了 900 个标签数据,标签 T_i 在后端数据库 TS 存储格式为($ID = a$,$r_i = b$,$K = c$),其中 a、b 为初始赋值

（随机赋值为 8、9）；K 为位置索引，未被阅读时 $c=0$，阅读完成后 c 为新位置值. 模拟过程 TS 产生随机数 $r_t=d$（随机赋值为 36）激发访问第 900 个标签 T_{900}，T_{900} 先计算 Hash(8 ‖ 9 ‖ 36)、$s_{900}=r_{900}=8$、$r_{901}=$ Hash(8 ‖ 9)；再发送(Hash(8 ‖ 9 ‖ 36)，9) 至 TS，TS 根据 $s_{900}=9$ 查找是否存在记录 RD_{900}：(8，9，0)，若存在则计算 Hash(ID ‖ r_{900} ‖ r_t) = Hash(8 ‖ 9 ‖ 36)，并与接收到的 Hash 值对比，相等则验证通过. TS 计算 $r_{901}=H(8 \| 9)$ 并新建 RD_{901}：(ID = 8，r_{901} = Hash(8 ‖ 9)，$K=901$)，再修改 RD_{901}：(ID = 8，$r_{900}=9$，$K=901$). 若此次通信结束，TS 再与 T_{900} 通信时，会根据 $s_{901}=r_{901}$ 查询到 RD_{901}，此时该记录的 $K=900$，再用 RD_{901} 覆盖 RD_{900}. 若此次通信未获通过，则 T_{900} 初始化标识符 r_{900} 不更新，TS 再次与 T_{900} 通信时，仍寻找到 RD_{900}，并根据 $K=901$ 修改 RD_{901}.

4.4　可信度分析

（1）访问认证

访问认证. T_i 初始状态默认为安全模式，仅授权供应链节点企业消息认证成功后才可访问，有效控制了初始伪装攻击. 当读卡器向 T_i 阅读请求时，假设非法用户已经窃取了 r_t，但此时 ID_i 和 r_i 尚未经信道传送，其无法窃取 r_{i+1}；系统在借助位置索引 K 找到 TS 中对应记录后，才会改写标识符 r_{i+1}，此时非法用户攻击成功概率低于 $1/2^{|r_{i+1}|}$，有效保证了初始数据查询安全.

（2）匿名安全

在 $\mathrm{Hash}(x)=h$ 中，因为 Hash 函数单向性特性，不可能借助 h 反推 x. 因此若 Hash(ID_i ‖ r_i)、Hash(ID_j ‖ r_i ‖ r_t) 等值被窃取，非法用户也无法反推标签 ID 和某一随机数.

（3）防重传性

协议通过实时动态刷新标签 ID，更新每次 ID 交换信息，即使非法用户记录了上一次传递的 ID，也无法通过重放该 ID 通过验证.

（4）防追踪性

由于 T_i 在发出 Hash(ID_i ‖ r_i ‖ r_t) 之前已经更新，可有效防止非法用户持续追踪某一 ID 获取物品定位. 由于基于 AES 的 Hash 函数可有效屏蔽 r_i 和 r_{i+1} 间关联信息，即使非法用户利用中间攻击 T_i 并破译了 r_{i+1}，也无法进一步获得 r_i 的历史数据，保障了 T_i 的前向不可追踪性.

（5）数据问责

理想环境下，后端数据库 TS 掌握所有 T_i 的信息，当标签 T_i 与供应链节点企业关联异步时，可借助 K 值和 s 值恢复 T_i，有效保障了 TS 与 T_i 数据的一致性.

（6）缩时增效

本协议中 TS 根据 r_i 来解码 ID，无需穷举 ID 进行 Hash 函数运算. 在供应链节点企业 TS 中存储 n 个 T_i 时，利用本协议，每次查询 TS 会产生 1 个随机数，实施 n 次搜索和 2 次 Hash 函数运算，而相对最有效率的 Hash 链协议则需实施 $2n$ 次 Hash 函数运算、$2n$ 次搜索和比较. 因此本协议有效缩短了搜索时间、减少了运算负载、提升了比较效率，且随着供应链物品 T_i 数目的递增，协议搜索计算所需时间增加缓慢，非常适合低碳供应链环境下物联网海量商品要求.

（7）成本优势

麻省理工大学 Auto-ID 实验室数据显示，实施单个 Hash 函数运算约需 0.02 ～ 0.04 kb 门电路，现有商用 RFID 安全用途的门电路为 2.5 ～ 5 kb. 本协议仅需要 0.04 ～ 0.10 kb 门电路，可轻松适应现有硬件条件；且把产生随机数等相对复杂计算流程转换到 TS，有效降低了 T_i 的复杂性，使得标签具有良好的制造使用成本优势.

5　结束语

本文根据低碳供应链环境物联网特点，在分析已有 RFID 系统物理及协议安全机制的基础上，设计了一种低碳供应链环境下改进的 RFID 协议，根据基于 ROM 模型的模拟数据实验证明，该安全协议可有效提升低碳供应链环境下物联网的可信度. 下一步研究主要是结合低碳供应链要求，设计一个通用组合的物联网安全模型，进一步改进 Hash 函数的自身安全性，提升可信度.

参考文献：

[1] 刘培学，高颖，陈玉杰. 分组自适应多叉树 RFID 防碰撞算法研究[J]. 微电子学与计算机，2014，31(10)：156-159.

[2] Masoumeh Safkhani. Cryptanalysis of the protocol：A hash-based RFID tag mutual authentication protocol [J]. Journal of Computational and Applied Mathematics，2014，259 (15)：571-577.

[3] Jin Sha Yuan，Yue Hu. Implementation of RFIDmiddleware based on hash chain[J]. Applied Mechanics and Materials，2013，41(12)：12-15.

（下转第 152 页）

很好的普适性.但对于收敛到全局最小值附近的平坦区域,由于网络输出误差小,学习速率低,使 CBP 算法收敛速度缓慢,降低学习效率,这是本文下一步研究的方向.

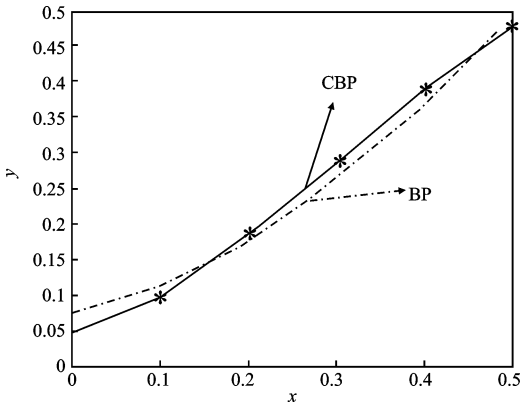

图 3 函数逼近效果图

参考文献:

[1] BISHOP C M. Neural networks for pattern recognition[M]. NewYork: Oxford University Press, 1995.

[2] 朱大奇,史慧. 人工神经网络原理及应用[M]. 北京:科学出版社, 2006.

[3] 王玲芝,王忠民. 动态调整学习速率的 BP 改进算法[J]. 计算机应用, 2009, 29(7): 1894-1896.

[4] 张雨浓,曲璐,陈俊维. 多输入 Sigmoid 激励函数神经网络权值与结构确定法[J]. 计算机应用研究, 2012, 29(11): 4113-4151.

[5] Azamat Amirov, Olga Gerget, Dmitry Devjatyh. Medical data processing system based on neural network and genetic algorithm[J]. Procedia -Social and Behavioral Sciences, 2014(131): 149-155.

[6] Chao Ren, Ning An, Jianzhou Wang. Optimal parameters selection for BP neural network based on particle swarm optimization: A case study of wind speed forecasting[J]. Knowledge-Based Systems, 2014(56): 226-239.

[7] Huang Han-Xion, Li Jiong-Cheng, Xiao Cheng-Long. A proposed iteration optimization approach integrating backpropagation neural network with genetic algorithm[J]. 2015, 42(1): 146 - 155.

[8] Ng S C, Leung S H, Luck A. The generalized backpropagation algorithm with convergence analysis[C]// Proc of the 1999 IEEE International Symposium or Lando,FL:IEEE,1999: 612-615.

[9] 张国翊,胡铮. 改进 BP 神经网络模型及其稳定性分析[J]. 中南大学学报:自然科学版, 2011, 42(1): 115-124.

[10] Vogl T P, Mangis J K, Rigler A K, Accelerating the convergence of the back-propagation method[J]. Biological Cybernetics, 1988, 59(4): 257-263.

[11] WANG Ching-hwang, KAO Chih-han, LEE Wei-hsien. A new interactive model for improving the learning performance of back propagation neural network[J]. Automation in Construction, 2007, 16(6): 745-758.

[12] 程玥,刘琼荪. 一种放大误差信号的 BP 算法[J]. 计算机应用研究, 2011, 28(2): 529-531.

作者简介:

裴松年 男,(1990-),硕士研究生.研究方向为机器学习.
E-mial:peisongnian@gmail.com.

杨秋翔 男,(1969-),教授,硕士生导师.研究方向为网络安全,模式识别.

刘忠宝 男,(1981-),博士,CCF 高级会员(E200015757S).研究方向为机器学习.

(上接第 147 页)

[4] Masoud Hadian Dehkordi. Improvement of the hash-based RFID mutual authentication protocol[J]. Wireless Personal Communications, 2013,25(8):152-159.

[5] M Sandhya, T R Rangaswamy. Zero knowledge and hash-based secure access control scheme for mobile RFID systems[J]. Arabian Journal for Science and Engineering, 2013,16(9):77-84.

[6] M Moessner, Gul N Khan, T R Rangaswamy. Secure authentication scheme for passive C1G2 RFID tags [J]. Computer Networks, 2012,56(1):273-286.

[7] 周永,杨云志,李元忠,等. 利用 RFID 和 VFID 技术实现卡车和集装箱自动识别管理系统[J]. 电讯技术, 2014,54(4):379-384.

[8] Kimmo Halunen. Multicollisions and graph-based hash functions[J]. Trusted Systems, 2012, 9(3):156-167.

作者简介:

杨传明 男,(1979-),博士,副教授.研究方向为科技管理.
E-amil:cmlucky@163.com.