移动物联网的可定制 RFID 网络安全协议①

褚贵洋

(沈阳军区总医院 信息科, 沈阳 110015)

摘 要: 已有的 RFID 安全协议大多针对隐私性与匿名性而忽略了可扩展性与可定制性, 对此提出一种可扩展且可定制的 RFID 双向认证协议. 首先, 目标认证模块分别对标签与客户端阅读器进行认证, 其中分别使用基于线性搜索的标签分组以及一个映射表提高认证的效率; 然后, 通过简单的 ID 匹配机制检测恶意用户; 最终, 通过标签与服务器的交互认证实现双向认证过程, 进一步提高安全性. 分析结果表明, 本算法在具有可定制能力与可扩展能力的前提下, 且具有较好的计算效率与安全性.

关键词: 移动物联网; RFID 系统; 可定制能力; 可扩展能力; 双向认证; 安全协议

Customized Security Protocol of RFID Network in Mobile Internet of Things

CHU Gui-Yang

(Information Department, General Hospital of Shenyang Military Area Command, Shenyang 110015, China)

Abstract: Concerned the problem that the existing RFID security protocols focus on the privacy and anonymity of RFID system, but ignore the scalability and customizability, a scalable and customizable RFID bidirectional authentication protocol is proposed. Firstly, the tags and client readers are authenticated by target authentication module, the efficiency of the authentication is improved by using the tag grouping based on liner search method and a mapping table; secondly, the malicious users are detected by a simple ID matching detection; lastly, the mutual authentication between tags and servers is realized to enhance the security further more. The analysis results show that the proposed algorithm has a good computational efficiency and security, at the same time it realizes the customizability and scalability.

Key words: mobile internet of things; RFID system; customizability; scalability; both mutual authentication; security protocol

RFID 系统是物联网重要的一部分, 其安全性与性能直接影响物联网的整体性能, 随着物联网的多元化, 许多应用将阅读器植入移动设备之中(智能手机、平板电脑等), 因此 RFID 系统需要具有可扩展能力以及可根据不同应用场景所具备的可定制能力[1,2].

然而已有的RFID安全协议大多仅考虑了RFID的匿名性与隐私保护能力, 而忽略了目前移动物联网所需的可扩展能力与可定制能力[3,4]. 文献[5-7]对此提出了具有可扩展能力的 RFID 安全协议, 但是均具有一些不足之处, 这三种算法的计算复杂度均较高. 文献[8]针对应用于射频识别(RFID)系统中的 Hash 链协议在可扩展性和安全性方面存在的缺陷, 提出了一种高效可扩展的改进协议, 该方案供了标签与阅读器之间的双向认证, 通过利用标签 ID 的唯一性建立了数据索引, 但该方案中标签 ID 极为关键, 对克隆攻击的鲁棒性较弱. 文献[9]使用树结构管理标签实现隐私保护,将 RFID 系统搜索云数据库的时间复杂度由 O(N)减少到 O(lgN), 该方案基于数据库搜索与加密系统提高 RFID 网络的安全性, 但其通信成本与计算成本均远高于非数据库搜索的方案.

为了提高新型移动 RFID 系统的综合性能, 本文设计了新的具有可扩展且可定制的 RFID 安全协议, 本协议工作于 EPCglobal Architecture Framework[10]的 Application Level Event(ALE)层, 共包含四个模块: 客户端阅读器认证模块、标签认证模块、恶意入侵检测模块以及标签与服务器的双向认证模块. 前两个模块

① 收稿时间:2016-08-23;收到修改稿时间:2016-10-12 [doi:10.15888/j.cnki.csa.005769]

为初步筛选与过滤模块, 选择合法的客户端阅读器与标签; 第三个模块则检查系统的恶意入侵, 可抵御诸如 SQLIA、妥协攻击等恶意攻击; 第四个模块则深度检查标签的合法性. 本协议在具有可定制能力与可扩展能力的前提下, 且具有较好的计算效率与安全性, 满足新型移动物联网的安全性需求. 关键词库的结合大大提高了信息抽取算法的准确性和通用性, 基于 Web 信息抽取的混合交通出行方案生成与表示系统的成功实验也证明了本文提出的 Web 信息抽取算法的实用性.

1　移动RFID系统的架构

本系统总体分成三部分: 相关 Web 页面获取模块、Web 信息抽取模块、知识表示模块. 系统总体框图如图 1 所示.

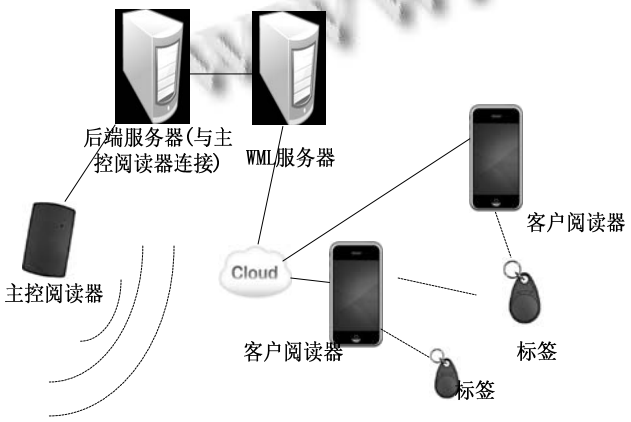

图 1　移动 RFID 系统的网络模型

参考众多的移动 RFID 系统实例[11,12], 考虑图 1 所示的移动 RFID 系统模型, 其中主要包含后端服务器、WML 服务器、客户端阅读器、主控阅读器、标签以及云, 各部分的作用如下描述:

后端服务器: 维护所有标签与阅读器的相关信息:

$$DB=<TID,OTID,SCH_b,SCH_t,P_{Sb},t_{re},t_{sy},RN_T,RC_{DB},W,RID,R_{status}> \quad (1)$$

表 1 描述了式(1)中的符号意义, 数据库直接与主控阅读器连接与交互.

表 1　后端服务器中维护的参数及其意义说明

参数	意义
TID	包含状态位的标签 ID
$OTID$	旧标签 ID
SCH_b	标签的清理状态位(1:ON, 0:OFF)
P_{Sb}	标签 ID 中清理状态比特的随机位置
P_{Sb+1}	标签的新 P_{Sb}
SCH_t	清理状态的时间戳比特
t_{re}	标签最后的阅读时间
t_{sy}	同步的系统时间
RN_T	该标签被阅读的次数
RC_T/RC_{DB}	标签清理会话中阅读标签的次数计数器
W	标签集的值
RID	阅读器的物理 ID
R_{status}	阅读器状态(ON/OFF)

WML 服务器: 为后端服务器与认证的用户分别提供无线连接与 Web 服务.

客户端阅读器: 位于远端的阅读器(移动或非移动状态, 可嵌入移动设备中), 可认证标签. 此类阅读器可通过云、服务器与主控阅读器通信, 后端服务器与认证的客户端阅读器均维护一个元组信息:

$$R_{DB}=<RID,R_{status}> \quad (2)$$

式中 RID 是认证的客户端阅读器 ID 列表, $R_{status}\in\{ON,OFF\}$ 是阅读器的状态信息.

主控阅读器: 管理所有的客户端阅读器并与后端服务器连接, 同时支持 EPCglobal 框架[8]. RFID 标签: 通过保存的 ID 识别目标标签.

本文协议共包含 4 个系统模块, 如图 2 所示. 模块 1 与 2 均使用搜索技术认证客户端阅读器与标签, 模块 3 通过恶意命令的匹配算法检测恶意入侵用户, 模块 4 实现了标签对服务器的双向交互认证.

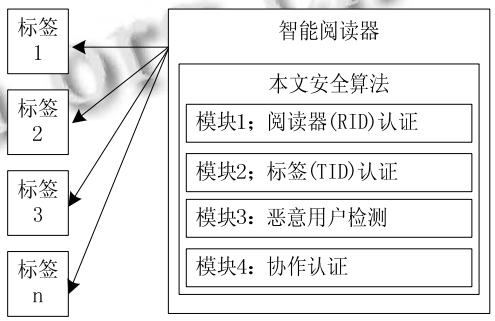

图 2　本文安全算法的架构(共包含四个模块)

图 3 所示是本文标签与阅读器通信的数据格式.

起始位(1比特)	数据域(96比特)	CRC-32(32比特)	结束位(1比特)

图 3　本文标签与阅读器通信的数据格式

2　本协议的主要模块

2.1 目标认证算法

目标认证技术包括模块 1 与模块 2, 分别处理标签

与阅读器的认证, 如图 4 所示是本文目标认证方法的处理流程.

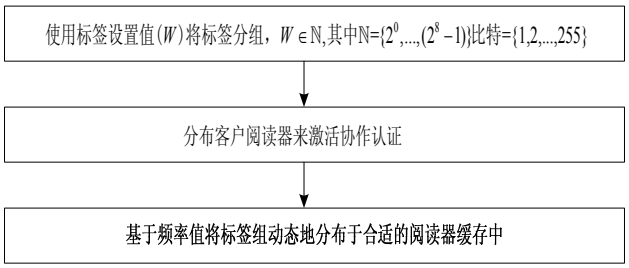

图 4 本文目标认证算法的流程

本文认证技术主要分为如下两步:

① 步骤 1(标签分组): 本文使用基于标签分组的线性搜索方法来缩短搜索的时间窗口. 将 255 个标签分为一组, 以 8 比特值表示, 分组方法如下式所示:

$$W=(bb_{MSB} \parallel bbbbbb_{LSB}) \tag{3}$$

式中 $W>0$, bb_{MSB} 是标签 ID 的两个 MSB(最高位), $bbbbbb_{LSB}$ 是后六个 LSB(最低位).

$$G(W)=<TG_{W_1},...,TG_{W_{\mathbb{N}max}}> \tag{4}$$

后端服务器按照式(4)获得分组的标签, 其中 $G(W)$ 是基于标签集合值 W 将标签分组的函数, W_1 表示 W=1, TG_{W_1} 表示集合值 W=1 的标签分组, $\mathbb{N}_{\max}$ 表示最大的标签集合值.

② 步骤 2(标签协同): 在该步骤中, 主阅读器与客户阅读器协作来获得 TG 动态且有效的分布. 主阅读器与客户端阅读器如下处理:

主控阅读器程序: 主阅读器将 $<TG_{W_1},...,TG_{W_{255}}>$ 分布并缓存于客户端阅读器中. 然后, 主阅读器使用(7)式建立一个映射表 $M(TG)$, 该表记录指定 TG 与当前主阅读器的映射, 客户端阅读器据此寻找当前的主控阅读器:

$$M(TG)=<TG_{W_1},RID_1>,...,<TG_{W_{255}},RID_{255}> \tag{5}$$

客户端阅读器程序: 标签协作方法旨在基于频率值将标签进一步地分组处理, 以确保阅读频率高的阅读器可快速地获得标签的认证信息. 客户端阅读器周期地计算 TG 的频率值, 计算方法如下:

$$T_T^R=\sum_1^n T_1+...+T_3+...+T_n \tag{6}$$

$$T_t^R=\sum_1^n t_1+...+t_3+...+t_n \tag{7}$$

$$F(R)=\frac{T_t^R}{T_T^R} \tag{8}$$

式中 $T_1,...,T_n$ 是标签集合, $t_1,..,t_n$ 是时间间隙(n 个标签阅读), R 是阅读器, T_T^R 是 $T(t)$时隙中 R 所阅读的标签总数量, $F(R)$是 $T(t)$时隙中阅读器 R 的频率.

客户端阅读器的 TG 频率值越低, 则将该 TG 移动到对应客户端阅读器的概率越高.

2.2 双向认证协议

图 5 所示是本文双向认证协议的具体算法与流程, 详细描述了四个模块的运行流程与具体实现. 阅读器通过 EPC 通信协议 LLRP 开始协议, 阅读器生成一个查询 q, 如下式所示:

$$q=h(RID_i \oplus r_1) \tag{9}$$

式中 r_1 是一个随机数, 通过轻量级伪随机数生成器(PRNG)与阅读器 ID(RID_i)进行异或运算生成. 然后对结果进行 hash 计算生成 q.

然后, 阅读器随机地生成 P_{Sb+1} 并发送 r_1、q、P_{Sb+1} 然至标签来初始化标签与阅读器之间的通信. 该初始化帧(协议的第一帧)的数据格式如图 6(a)所示. 标签对阅读器返回响应帧, 响应中包含 $r_2, \mathcal{W}', RC_T', r_3$, 响应帧格式如图 6(b)所示.

参数 r_2 是标签中使用 PRNG 生成的随机数, $\mathcal{W}'$ 是随机的标签值, 由 r_1 与 $\mathcal{W}$ 异或运算生成. 将标签的阅读次数值(RC_T)进行 hash 运算以生成 RC_T', 然后, 使用(10)(11)两式生成计算 r_3.

$$k'=rot(TID_i, P_{Sb+1}) \tag{10}$$

$$r_3 \leftarrow h(r_2 \oplus k' \oplus q) \tag{11}$$

式(10)中 rot 使用随机数 P_{Sb+1} 进行随机左循环移位(rot)运算, 式(11)中将 k'、r_2、q 三者进行异或运算, 并将结果进行 hash 运算获得最终的 r_3. 上述处理中通过 hash 函数、随机数与左循环移位操作来保证传输的数据无法被追踪以及安全性.

图 6(a)(b)所示是帧的成功传输实例, 阅读器使用主控阅读器中的 R_{DB} 来初始化 RID_i 的识别处理. 系统模块 1 对应于阅读器识别程序. 如果在 R_{DB} 中发现 RID_i, 则模块 1 调用模块 2 进行后续处理; 否则, 拒绝所有收到的数据.

图 5　本文双向认证的详细流程与步骤

Start	r_1	q	P_{Sb+1}	保留	CRC	End
1比特	8比特	8比特	8比特	72比特	32比特	1比特

(a) 第一个传输帧格式

Start	r_2	W'	RC'_T	r_3	CRC	End
1比特	8比特	8比特	8比特	72比特	32比特	1比特

(b) 第二个帧格式

Start	r_4	保留	r_5	CRC	End
1比特	8比特	16比特	72比特	32比特	1比特

(c) 第三个帧格式

图 6　双向认证协议的帧格式

如果在 DB(数据库)中找到 TID_i, 客户端阅读器识别出 TID_i 并使用标签的 SCH 比特(保存于 DB 中)来决定标签的 SCH 状态. 如果标签的 *SCH=ON*, 则忽略模块 3 与模块 4; 如果 *SCH=OFF*, 则运行模块 3 与模块 4 两个模块以提高安全级别.

TID 的计算方法如下所示:

$$TID_{i+1} = \left(k''_{MSB} \| b_T \oplus SCH_b \| k''_{LSB}\right) \tag{12}$$

式中 b_T 表示 P_{sb} 的比特, k''_{MSB} 表示 TID 中 b_T 之前的比特, k''_{LSB} 表示 TID 中 b_T 之后的比特.

如果标签是 OFF 状态, 系统则运行模块 3 与模块 4. 在模块 3 中, 恶意检测程序将确保标签数据不受恶意命令影响. 模块 3 的方法对文献[13]进行了修改: 如果发现了恶意 SQLIA 命令, 则系统调用模块 4 进行处理, 模块 4 是一个交互认证阶段, 该阶段的阅读器发送标签的 r_4 与 r_5 到标签, 如图 6(c)所示. 随机数 r_4 由 PRNG 计算获得, r_5 签则通过对 r_3、k''、q 进行异或运算, 并保存于后端的服务器中.

式(20)生成的标签使用与式(19)相似的处理, 将 r'_5 与式(21)中的 r_5 进行比较, 如果式(21)返回 TRUE, 则认为交互认证成功. 然后, 协议使用式(12)的 SCH 比特计算新的标签 ID(TID_{i+1}). 最终, 更新 TID 与 RCT 并结束整个协议. 如果式(21)返回 FALSE, 系统拒绝所有值钱的通信并结束后续的通信.

3 安全协议的性能分析

为了横向地评估本文可扩展、可定制 RFID 安全协议的综合性能, 将本协议与文献[5-7]进行了比较, 表 2 与表 3 所示是各性能指标的结果统计, 表 2 所示是各协议的扩展性与计算复杂度结果, 可看出本协议的扩展性优于其他三种协议, 同时由于本算法采用的动态标签分组技术, 使得本方法的计算复杂度低于文献[7]的方案(可扩展的认证方案).

表 2 四种安全协议的可扩展能力比较(n_T/n_{CR}: 客户端阅读器中缓存的标签数量, n_T/n_R: 阅读器中缓存的标签数量)

协议	可扩展的标签认证方法	计算复杂度
文献[5]	不满足	O(1)
文献[6]	不满足	O(1)
文献[7]	协作认证	O(n_T/n_R)
本协议	混合认证算法	O(n_T/n_{CR})

表 3 所示是四种安全协议的安全性性能的比较, 总体而言, 本方法比其他协议的 hash 运算少, 同时本方法包含多个控制参数(例如 SCH_t, t_{re}, RC_T, RN_t)以确保对不同的 RFID 分布系统进行最优化地定制. 阅读次数(RC_T)与阅读数(RN_t)参数的作用是控制系统期望阅读标签的次数, 状态时间戳比特 SCH_t 与标签的最终阅读时间 t_{re} 作用是控制标签的阅读时间. 此类控制参数增强了协议的自适应性, 并且可有效地抵御了恶意标签的入侵.

表 3 四种安全协议的自适应性与安全性比较

协议	自适应性	hash 运算的最大数量	hash 运算的最小数量	是否可抵御恶意攻击
文献[5]	部分满足	4	2	否
文献[6]	部分满足	5	3	否
文献[7]	部分满足	无	无	否
文献[14]	部分满足	无	无	是
本协议	完全满足	4	2	是

4 结语

针对新型移动 RFID 系统, 本文设计了新的具有可扩展且可定制的 RFID 安全协议, 共包含四个模块: 客户端阅读器认证模块、标签认证模块、恶意入侵检测模块以及标签与服务器的双向认证模块. 在目标认证模块中, 通过标签分组提高标签搜索的效率, 并使用标签协同方法基于阅读器频率值确保阅读频率高的阅读器快速获得标签的认证信息. 同时为算法引入了多个控制参数, 阅读次数(RC_T)与阅读数(RN_t)参数的作用是控制系统期望阅读标签的次数, 状态时间戳比特 SCH_t 与标签的最终阅读时间 t_{re} 作用是控制标签的阅读时间, 此类控制参数增强了协议的自适应性, 并且可有效地抵御恶意用户的入侵.

参考文献

1 孙其博,刘杰,黎彝,等.物联网:概念、架构与关键技术研究综述.北京邮电大学学报,2010,33(3):1–9.

2 杨光,耿贵宁,都婧,等.物联网安全威胁与措施.清华大学学报(自然科学版),2011,(10):1335–1340.

3 张捍东,丁磊,岑豫皖.基于 Hash 函数的 RFID 安全协议研究.计算机工程与设计,2013,34(11):3766–3769.

4 冯君,汪学明.基于超椭圆曲线密码体制的 RFID 安全协议.计算机工程与设计,2013,34(10):3427–3430.

5 Song B, Mitchell CJ. Scalable RFID security protocols supporting tag ownership transfer. Computer Communications, 2011, 34(4): 556–566.

6 Erguler I, Anarim E. Security flaws in a recent RFID delegation protocol. Personal & Ubiquitous Computing, 2012, 16(3): 337–349.

7 Trujillo-Rasua R, Solanas A, Pérez-Martínez PA, et al. Predictive protocol for the scalable identification of RFID tags through collaborative readers. Computers in Industry, 2012, 63(6): 557–573.

8 裴小强,卫宏儒.基于 Hash 链的 RFID 安全双向认证协议.计算机应用,2014,(S1):47–49.

9 温聪源,曾致远,徐守萍.使用云数据库作为服务器的 RFID 安全认证协议设计研究.科学技术与工程,2015,15(16): 84–90.

10 Fabian B, Nther O. Security challenges of the EPCglobal network. Communications of the ACM, 2009, 52(7): 121–125.

11 吕峻闽,缪春池,周启海,等.基于 RFID 和 SCOR 的物联网配送中心信息系统模型研究.计算机科学,2011,38(12): 128–130.

12 王新锋,刘建国,蒋旭,等.移动型 RFID 安全协议及其 GNY 逻辑分析.计算机应用,2008,28(9):2239–2241.

13 Ray B, Chowdhury MU, Pham T. Mutual authentication with malware protection for a RFID system. International Conference on Advances in Distributed and Parallel Computing Adpc. 2010. 24–29.

14 杨昕,凌捷.一种低成本超轻量级 RFID 双向认证协议.计算机科学,2016,43(4): 160–162.