



面向智慧园区的 RFID 系统信息安全认证方案

李荣荣¹, 寇建涛², 董刚³, 唐良瑞¹

(1. 华北电力大学新能源电力系统国家重点实验室, 北京 102206;

2. 国家电网公司客户服务中心, 天津 300012;

3. 北京国电通网络技术有限公司, 北京 100070)

摘要: RFID 系统本身在设备身份认证及信息传输过程中存在众多安全漏洞, 且现有的 RFID 安全认证大多为重量级认证, 必然会加重认证双方的信息处理负担, 导致出现有效信息率低的问题。为此, 对 ARAP 加以改进, 提出了一种可靠的轻量级 RFID 系统信息安全认证协议 (DARAP), 该协议可以有效抵抗重传、跟踪、欺骗、克隆和去同步等多种攻击手段, 具有较高的安全性和实用性。

关键词: RFID; 智慧园区; 轻量级; DARAP

中图分类号: TP393.08

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016067

A security authentication scheme in RFID system for smart park

LI Rongrong¹, KOU Jiantao², DONG Gang³, TANG Liangrui¹

1. State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources,
North China Electric Power University, Beijing 102206, China

2. State Grid Customer Services Center, Tianjin 300012, China

3. Beijing GuoDianTong Network Technology Co., Ltd., Beijing 100070, China

Abstract: There exist many security vulnerabilities in device's identity verification and the information transmission through RFID system, the computations and procedures in the classical RFID authentication protocols are so complex that will impose processing burdens on the data base or readers, leading to the problem of low effective information rate. To solve the problem, an improvement of ARAP protocol which called DARAP was proposed to realize authentication in RFID system for smart park. The new protocol could effectively resist attacks of re-transmission, tracking, deception, cloning and de-synchronization, and it had high security and practicability.

Key words: RFID, smart park, lightweight, DARAP

1 引言

射频识别 (radio frequency identification, RFID) 是 20 世纪 90 年代兴起并逐渐走向成熟的一种非接触式的自动识别技术, 它通过无线通信的方式自动识别和捕捉数

据, 以实现对象身份和信息的鉴定, 在识别、跟踪、定位等领域已得到广泛应用。在智慧园区中使用 RFID 技术, 可实现对园区人员的自动化管理识别、南北园区大量资产的有序便捷管理及维护, 提高园区信息自动化管理水平。然而, RFID 系统本身会存在一些隐私安全问题: 一方面, 由于

RFID 技术在标签与阅读器间采用无线传输方式,信道中传输的信息极易受到恶意攻击,从而造成标签敏感信息的泄露、篡改等问题,对园区信息安全造成巨大的威胁;另一方面,由于标签和阅读器的存储空间及计算能力有限,在进行认证协议设计时,必须考虑到计算复杂度及效率问题。此外,在智慧园区系统中,客服人员身份识别和设备维护权限识别等大多采用无源标签,其所处的硬件环境,如大门的数量和数据库内存的大小,一般是有严格限制的,对消息进行复杂的加密算法来保证信息安全的传统算法并不适用。为解决这些问题,亟需有效灵活的轻量级双向安全认证方案来保证智慧园区信息的隐私和安全,为实现园区信息管理的高度自动化提供保障。

目前,国内外关于轻量级认证协议的研究已有一些成果,但都存在一定的缺陷和漏洞。Peris 等人^[1]曾提出一种轻量级双向认证协议,但后续研究发现该协议无法抵御非同步攻击与信息泄露攻击^[2];参考文献[3]介绍了另外一种基于 SASI 的轻量级算法来提供顽健的身份验证,以保证信息的完整性,但也存在一些安全漏洞,如标签的可追溯性、非同步性和信息外泄等问题;参考文献[4-7]通过在特定场景下人为假设特定攻击,对 SASI 协议的相关漏洞进行了验证和说明;参考文献[8]在 SASI 算法的基础上,对其进行了改进,提出了一种 Gossamer 协议来弥补 SASI 算法的不足,但该算法仍然无法抵御参考文献[6]中提及的非同步攻击;参考文献[9]介绍了一种针对轻量级协议的新型攻击模式 Tango,在不需要获知双方密钥的情况下,通过巧妙地计算截获信息中“0”、“1”总数及比率,可以达到恢复原始信息的目的。此外,大多协议设计时都忽略了来自系统内部的合法阅读器之间的伪造和篡改问题。但是,在实际应用中,一旦攻击者通过物理手段截获合法阅读器,它就可以直接获取到后台数据库的全部信息,这必然对后台数据中心的信息安全造成无法挽回的巨大

损失。

基于以上分析,本文对 ARAP 进行了改进,提出了一种新型的 RFID 双向安全认证协议——DARAP,通过标签匿名来抵御标签的跟踪攻击,并采用随机数的方式保证信息的高度安全性与隐私性,具有很强的顽健性,可以抵御重传、跟踪、欺骗、克隆和去同步等多种攻击手段,可为 RFID 系统提供可靠的双向认证。

2 智慧园区中 RFID 系统漏洞分析

简单的 RFID 系统主要由阅读器、电子标签和后台数据库 3 部分组成^[10],RFID 系统的组成如图 1 所示。其中电子标签存储其持有者的相关数据信息,由射频芯片和天线构成,且具有全球唯一标识,即物理 ID;阅读器负责对标签进行读写,分为只读阅读器和读写器;后台数据库的主要作用是存储阅读器和标签的相关信息,并为标签和读写器之间的认证过程提供服务。阅读器与后台数据库间的通信一般认为是通过安全信道实现的,而标签与阅读器间的通信则是采用无线通信的方式,如射频识别技术等。



图 1 RFID 系统的组成

在分析智慧园区 RFID 系统安全漏洞时,本文首先建立了威胁模型^[11],并假设攻击者可以完全控制阅读器和标签之间的通信内容。攻击者既可以采用被动的攻击方式进行攻击,如窃听、截取、转发等;也可以采用主动的攻击方式进行攻击,如对读写器与标签之间的通信内容进行篡改等。威胁模型如图 2 所示,其中攻击者可以获取到标签是否通过认证的信息,如园区客服人员在刷

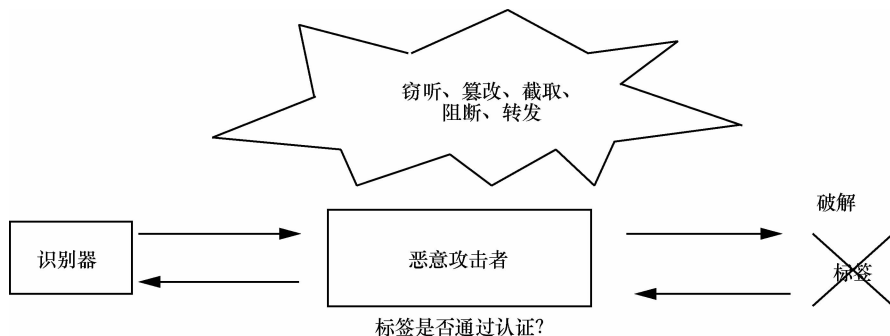


图 2 威胁模型



门禁卡时,往往可以通过门是否打开来判断标签认证是否成功;此外,部分标签的密钥可以通过物理破解的方式得到。

假设攻击者是一个恶意的实体,其目的是通过监听或者直接与标签通信的方式实施某些攻击。考虑到 RFID 系统在智慧园区中的具体应用,攻击的形式包括假冒合法持卡者身份、跟踪设备位置、窃取设备信息等,常见的攻击类型有以下几种^[12]。

(1) 窃听

窃听是指未经授权者的无线通信接收设备,对标签与阅读器之间传递的数据进行监视与记录。当数据未被加密时,窃听者可以很容易地截获传输过程中的数据,甚至还可以篡改数据。被加密的数据同样也存在被窃听的危险,但相对会困难些。

(2) 欺骗

欺骗是指攻击者采用一种特殊功能模拟合法的 RFID 标签或者阅读器发送数据,从而获取相关隐私数据以及向阅读器或标签发送虚假信息。要成功执行欺骗攻击,攻击者必须预先知道 RFID 系统使用的协议及认证密码。

(3) 拒绝服务

攻击者使用许多特殊设计的标签同时向阅读器发送大量会话请求,使阅读器超出其处理能力,从而导致阅读器崩溃,合法标签也不能被识别,从而阻断了标签与阅读器之间的正常通信。

(4) 跟踪

攻击者在某个区域伪装成多个阅读器,向标签发送相同的认证信息,如果标签响应的信息也相同,攻击者就可以通过判断标签出现的先后位置来跟踪标签的运动。采用假名替代真实的 ID,且每次认证后对假名进行更新,可以有效地抵御跟踪攻击。

(5) 克隆

尽管克隆和欺骗都是从一个合法标签复制数据,但欺骗是模拟标签数据的传输,而克隆则复制数据到攻击者自己的标签中,相当于产生了一个假冒的标签,该标签甚至可以侵入目的 RFID 系统,进行有计划地攻击。

(6) 非法访问

非法访问是指攻击者采用合法的读写器来获取该读写器非管辖范围内的标签上的信息,但一般不会对标签信息进行修改。如园区内某一部门的人员利用本部门的阅读器去获取非自己管辖范围内的设备信息。

(7) 重放

重传攻击主要包括 2 种:一种是攻击者伪装成标签,重传标签对阅读器的认证响应,从而获取标签的信任;另一种是攻击者伪装成阅读器,重传阅读器对标签的认证请求,使阅读器误以为其是合法的身份。常用的抵抗重传攻击的方法是时间戳和随机数。

(8) 去同步

在需要密钥更新的 RFID 系统中,标签端与读写器端、后台数据库端的密钥更新应是同步进行的,但如果攻击者通过一定的手段,使得标签与二者之间的密钥更新不同步,就会导致合法标签、读写器及后台数据库互相不识别。攻击者就可以利用该机会实施其他的攻击,从而破坏 RFID 系统的安全。

3 新型 RFID 安全认证协议 DARAP

3.1 协议模型

为了更好地理解协议的执行过程,对该协议中采用的一些符号进行了定义和说明,相关符号定义及说明见表 1。DARAP 涉及 3 个认证实体,即识别器、标签和后台数据库,且假设只有识别器可以与后台数据库进行通信。由于园区处于封闭状态,信息的传输是在楼内及近距离楼宇间进行的,因此可将阅读器(园区中应为识别器)与后台数据库间的信道视为安全信道,信息在本环节的传输被认为是安全的。但是识别器与标签之间采用的是无线信道,虽然在门禁类系统中,门禁卡的识别属于短距离非接触式识别,无线信道的安全性可以忽略不计,只需要考虑门禁卡身份冒充及欺骗的问题即可,但对于其他一些远程的信息识别及信息管理,必须重点考虑信息在无线信道中传输的安全性。

表 1 相关符号定义及说明

符号	说明
R	RFID 识别器
r_R	识别器 R 产生的随机数
T	RFID 标签
r_T	标签 T 产生的随机数
P	标签 T 的假名
S	假名 P 的覆盖值
x_R	识别器 R 的真实 ID
x_T	标签 T 的真实 ID
BS	后台数据库
$h()$	$h()$ 函数
$\oplus$	按位异或运算

在 DARAP 中,标签不采用自己真实的 ID,而是采用匿名的方式与识别器进行信息传输。但如果标签使用的假名固定不变,该假名本质上已经等同于标签的真实 ID,标签仍然无法抵御被动攻击,如果对标签设置动态的独立假名,则可以有效地解决该问题。假设智慧园区内所有标签共用一个假名库和散列函数,标签每次进行一个会话过程时,都会首先选取一个假名,同一个假名可以被不同的标签同时使用。设假名 P 的长度为 k bit,为保证园区内所有标签的可区分性,规定每个假名都具有覆盖值 $S, S=h(P\oplus x_T)$,其中 x_T 为标签的真实 ID 值, $h()$ 为单向的散列函数,该函数可以将任何长度的信息映射为 l bit。这样就可以保证同一个假名在不同标签的覆盖值 S 是不同的。由于散列函数为单向函数,攻击者通过捕获到的假名信息来获取标签真实 ID 几乎是不可能的。

此外,识别器需要与标签采用相同的散列函数,后台数据库也必须包含标签假名库、每个识别器的真实 ID 值、每个标签的真实 ID 值及相同的散列函数。其中, P 与 x_T 的长度都为 k bit, S 的长度为 l bit,随机数的长度也为 k bit。为了抵御重放攻击,每次会话任务时,标签端的随机数 r_T 和识别器端的 r_R 都要进行变化。

3.2 DARAP 的描述

DARAP 的认证过程如图 3 所示。

(1)初始化:在标签 T 的内存中存储本标签本次会话所需的假名 P 、真实 ID 标识 x_T 以及 $h()$ 函数,识别器内存

含有自身真实 ID 与同一个 $h()$ 函数,后台数据库中存储所有标签的真实 ID、所有识别器的真实 ID、假名数据库以及同一个 $h()$ 函数。

(2)当识别器 R 感知到周围存在标签 T 时,即刻发起认证,识别器 R 产生随机数 r_R ,并连同 request 一起发送给标签 T。

(3)标签 T 接收到来自识别器 R 的信息后,其随机数发生器产生随机数 r_T ,然后利用内存中本标签的 x_T 进行如下运算: $S=h(P\oplus x_T), M=h(r_T\oplus r_R\oplus P)\oplus S$,之后将 r_T, P, M 一并发送给识别器 R。

(4)识别器 R 收到标签 T 返回的信息时,计算 $N=h(M\oplus r_T\oplus x_T\oplus r_R)$,之后将 r_T, r_R, M, N 发送给后台数据库,由后台数据库进行识别器 R 和标签 T 身份的认证。

(5)后台数据库收到 r_T, r_R, M, N 后,首先验证识别器 R 的合法性:计算 $N'=h(M\oplus r_T\oplus x_T\oplus r_R)$,判断是否存在 x_R ,使得 $N'=N$,若不存在,本次认证失败;若存在,对标签 T 进行认证: $S'=h(P\oplus x_T), M'=h(r_T\oplus r_R\oplus P)\oplus S'$,判断是否存在 x_T 及 P ,使得 $M'=M$,若不存在,则标签 T 认证失败;若存在,标签 T 认证成功,令 $N'=h(M'\oplus S')$,将 N' 发送给识别器 R。

(6)识别器 R 接收到 N' 后,将其转发给标签 T。

(7)标签 T 根据内存信息计算 $N=h(M\oplus S)$,并与接收到的 N' 比较,如果 $N=N'$,则更新自己内存中的 P 和 S ,本次认证过程成功结束。

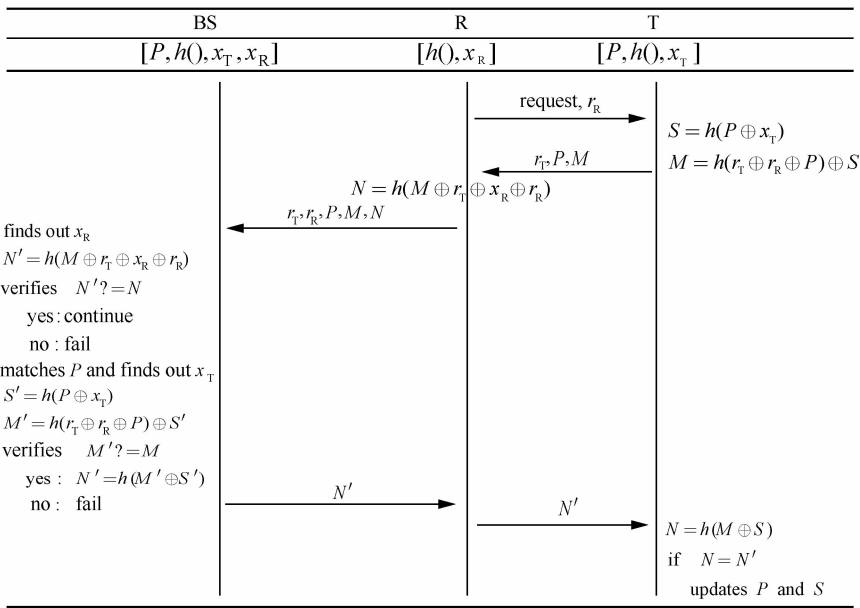


图 3 DARAP 的认证过程



4 DARAP 安全性分析

衡量一个 RFID 系统安全协议的优劣,除了协议的复杂度及计算效率外,对各种攻击的抵御能力也是至关重要的因素。在此,为了验证本文提出的新协议 DARAP 的安全性,以智慧园区中常见的几种攻击类型为例加以分析说明,其中 G 为攻击者,R 为合法的识别器,T 为合法标签,BS 为后台数据库,message<R-T>为 R 发给 T 的消息,message<T-R>为 T 发给 R 的消息。

(1) 重放攻击

G 在上次会话过程中,截取到了 message<T-R>,在本次会话过程中,T 重新在假名库里面选取新的假名 P ,且 r_T 和 r_R 的值也发生变化。G 先阻断本次的 message<T-R>,然后向识别器发送上次会话中截获的 message<T-R>,该 message<T-R>经过识别器转发给 BS,但由于本 message<T-R>中的 P 及 r_T 和 r_R 跟上次是一样的,因此 BS 根本无法搜索到满足条件的 T,本次会话过程即刻被终止。

(2) 欺骗攻击

由于 G 无法获知共享的散列函数及假名库 P ,G 无法向 R 发送 BS 可以满足识别格式条件的 message<T-R>,因此无法拟造虚假信息欺骗 T 或者 R,也不能获取系统的信任以得到相关的隐私数据。

(3) 跟踪攻击

T 在每次会话任务时,采用的不是自己的真实 ID 值,而是从假名库里选择假名 P 来替代真实 ID,并且即使某次选择到了曾经使用过的假名 P ,假名的覆盖值 S 、R 产生的随机数 r_R 及 T 产生的随机数 r_T 也是不同的。因此,G 无法通过向 T 发送相同的认证信息来跟踪标签的运动。

(4) 克隆攻击

由于 G 无法获知 T 的真实 ID、散列函数及假名库 P ,因此 G 也就无法克隆出合法的标签。即使克隆出了标签,该标签也会因与协议不符合而被系统识别出来,无法达到侵入目的 RFID 系统进行有计划攻击的目的。

(5) 去同步攻击

去同步攻击针对的是 T 与 BS 信息更新不同步的问题,新协议的信息更新只在 T 中进行,每完成一次成功的会话过程,T 就会在假名库里面重新选取新的假名 P 。而对于后台数据库而言,不需要进行 P 的更新,即不需要对每次 T 所使用的假名 P 进行记录,因为后台数据库是通过寻找 T 的 ID 并把假名库里面的 P 都匹配一遍来完成对标签 T 的认证的。

5 结束语

本文针对 RFID 系统在智慧园区中的具体应用,提出了一种新型轻量级双向安全认证协议——DARAP。该协议通过引入假名库和随机数,定期对标签假名进行更新,有效地抵御了跟踪及去同步攻击。此外,由于采用的是轻量级数据,新协议减轻了阅读器及后台数据库的计算复杂度,在节约成本的基础上,可抵抗包括重传、跟踪、欺骗、克隆和去同步等在内的多种攻击手段,具有较高的安全性和实用性。

参考文献:

- [1] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR J M E, et al. M2AP: a minimalist mutual-authentication protocol for low cost RFID tags [J]. Lecture Notes in Computer Science, 2006, 4159(10): 912-923.
- [2] LI T, WANG G. Security analysis of two ultra-lightweight RFID authentication protocols[C]//IFIP RC-11 International Information Security Conference, May 14-16, 2007, Sandton, South Africa. Berlin: Springer US, 2007: 109-120.
- [3] CHIEN H Y. SASI: a new ultra lightweight RFID authentication protocol providing strong authentication and strong integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4): 337-340.
- [4] CAO T, BERTINO E, LEI H. Security analysis of the SASI protocol [J]. IEEE Transactions on Dependable and Secure Computing, 2009, 6(1): 73-77.
- [5] PHAN R C W. Cryptanalysis of a new ultralight-weight RFID authentication protocol [J]. IEEE Transactions on Dependable and Secure Computing, 2009, 6(4): 316-320.
- [6] SUN H M, TING W C, WANG K H. On the security of Chien's ultralight-weight RFID authentication protocol [J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(2): 315-317.
- [7] ARCO P D, SANTISA D E. On ultralight-weight RFID authentication protocols [J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(4): 548-563.
- [8] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR J M E, et al. Advances in ultra lightweight cryptography for low-cost RFID tags: gossamer protocol [C]//International Workshop on Information Security Applications, September 23-25, 2008, Jeju Island, Korea. Berlin: Springer US, 2008: 56-68.
- [9] HERNANDEZ-CASTRO J C, PERIS-LOPEZ P, PHAN R C W, et al. Cryptanalysis of the david-prasad RFID ultralightweight authentication protocol [C]//International Workshop on Radio Frequency Identification: Security and Privacy Issues, June

8-9, 2010, Istanbul, Turkey. Berlin: Springer US, 2010: 22-34.

- [10] 辛伟, 郭涛, 董国伟, 等. RFID 认证协议漏洞分析[J]. 清华大学学报(自然科学版), 2013, 53(12): 1719-1725.

XIN W, GUO T, DONG G W, et al. Vulnerability analysis of RFID authentication protocols[J]. Journal of Tsinghua University (Science and Technology), 2013, 53(12): 1719-1725.

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

- [12] 丁治国, 郭立, 王昱洁. 基于密钥阵列的 RFID 安全认证协议[J]. 电子与信息学报, 2009, 3(13): 722-726.

DING Z G, GUO L, WANG Y J. An authentication protocol based on key array for RFID [J]. Journal of Electronics and Information Technology, 2009, 3(13): 722-726.

[作者简介]



李荣荣(1990-),女,华北电力大学新能源电力系统国家重点实验室硕士生,主要从事配用电通信网业务需求分析与网络安全性的研究工作。



寇建涛(1978-),男,国家电网公司客户服务中心高级工程师,主要从事电力系统通信与信息处理、物联网技术等方面的研究工作。



董刚(1963-),男,北京国电通网络技术有限公司高级工程师,主要从事电力系统通信与信息处理、物联网技术等方面的研究工作。



唐良瑞(1966-),男,华北电力大学新能源电力系统国家重点实验室教授、博士生导师,主要从事电力系统通信与信息处理、无线传感器网络与物联网技术等方面的研究工作。