

智能电网中RFID技术应用及其安全性分析

智能电网以高速集成信息通信网络为基础，大量应用先进的传感技术。无线射频识别（Radio Frequency Identification, RFID）技术是一种在物联网中具有广泛应用的非接触式自动识别技术，目前已应用于智能电网的发输变配用等环节，但由于智能电网对环境的特殊要求及RFID技术本身的缺陷，RFID技术在智能电网应用中尚存在诸多安全隐患。针对RFID技术在智能电网中的应用，着重分析其中的安全风险，并对相应的安全策略进行了对比。

吕旭明¹ 刘扬² 张文艳² 赵永彬³ 李钊¹ 雷振江¹ 胡楠³ 1. 国网辽宁省电力有限公司科技信通部 2. 国网辽宁省电力有限公司电力科学研究院 3. 国网辽宁省电力有限公司信息通信分公司



吕旭明/高级工程师

关键词/Keywords

智能电网 ·
RFID ·
安全风险 ·
防护策略 ·

0 引言

智能电网，即电网的“智能化”，以高速集成信息通信网络为基础，通过先进的传感技术、准确的测量与控制方法及决策支持系统的应用，实现电网的可靠、安全、经济、高效和环境友好的目标。而先进的传感技术又是实现电网智能化的前提和保证，通过传感技术应用实现分布式大规模信息的获取，实现输变电设备及线路状态的在线监测，实现电力数据的数字信息化，以供智能电网多个方面的使用^[1]。同时，先进的传感技术对于评估电网设备运行状况与电网完整性、进行表计读取、消除电费估计防止窃电、缓减电网阻塞以及与用户沟通等方面都具有积极的作用^[2]。

无线射频识别(Radio Frequency Identification, RFID)技术是在智能电网

应用较多的一种传感技术。RFID集编码、载体、识别与通信技术于一体，通过射频信号自动识别目标并获取数据，识别过程无须人工干预。RFID作为一种无线技术在实际应用中，RFID标签、通信网络和数据等环节都存在安全隐患，存在通信过程被干扰、通信信息被截获或篡改以及标签本身信息泄露的风险与隐患^[3]。本文针对RFID技术在智能电网中的应用，着重分析其中的安全风险，并对相应的安全策略进行对比。

1 RFID概述

RFID硬件系统主要包括三部分：标签(Tag)、射频读写器(Reader)和通信网络。软件系统包括中间件平台和应用管理软件。中间件平台用于封装底层硬件设备信息，实现底层硬件设备与上层应用管理软件间的无缝连接。RFID数据存储格式与应用管理软件数据保持一致，通信协议用于保证Tag与Reader间的数据传输^[4]。

1.1 Tag

Tag，即应答器，具有唯一的RFID编码，贴在被识别对象上。Tag上存储着实体各类信息，可以被Reader通过非接触的方式读取。Tag按照其是否携带电源可以分主动（有源）和被动（无源）两类。主动式Tag可以主动向外发射射频信号，射频读写器接收信号，并对其进行识别；被动式Tag只能被动的被读写器识别。Tag也可分为只读和读写两类。

1.2 Reader

Reader是带有天线的无线发射与接收设备，Tag与处理系统传递信息的媒介，能够发射射频信号、接收Tag应答信

号以及进行Tag认证与识别；处理通过认证的Tag信息；最后把数据进行上传与计算机系统进行交互，完成包括过滤无用数据、筛除重复数据等操作。

1.3 通信网络

通信网络指Reader读取到数据信息的传输途径，在智能电网应用中，传输给智能电网应用系统之前必须通过中间件进行数据处理，保证数据能够在智能电网应用系统中的可用性。

2 RFID技术在智能电网的应用

智能电网应用系统要求全面及时地掌握电网资产信息，因而需要大量的采集终端对信息进行采集，需要采集信息具备全面性、及时性、准确性和一致性，需要一条安全稳定的通道将信息传输到相关应用中。RFID作为一种非接触式的自动识别技术，能够很好满足上述需求；RFID Tag采用EPC码，信息存储量大，Tag编码具有唯一性，使被标识物体具有唯一性；Tag体积小、形状多样，读取时不受尺寸大小与形状限制，可以应用于不同的电力资产；RFID技术可以在被遮蔽的情况下进行无障碍的信息读取，穿透非金属或非透明的物质，通信信号不会被屏蔽。基于上述特点，将RFID技术应用于智能电网应用系统，可以实现对电力资产信息的自动采集、智能识别、自动巡检和管理资产身份标识等功能。如下图所示。

3 安全风险分析与防护策略对比

3.1 安全风险分析

RFID安全控制标准尚不成熟，在应用过程中存在诸多安全风险，如标签被非法读取、篡改或操控，标签在使用后未被禁用，使敏感信息外泄等。在智能电网RFID技术应用过程中，主要存在以下安全风险：

(1) 窃听。在RFID Tag和Reader之间的通信信息被未授权获取。窃听者可以通过无线通信接收设备截获通信过程中的数据，当通信数据为明文时，替换传输的数据非常容易。当然即使是被加密的数据也存在被截获并被破解的风险。

(2) 拒绝服务。当大量经过特殊设计的Tag同时向Reader发送海量的请求，使Reader超出其处理能力时，就会导致Reader不能正常读取Tag，即使合法的Tag也不能被识别，从而破坏Tag和Reader之间的正常通信，造成拒绝服务。

(3) 欺骗。攻击者使用一种特殊的模拟设备预设了RFID通信使用的协议与密码来欺骗Tag，接着冒充合法的Tag以获取隐私数据，攻击者冒用一个合法的Tag后，就可以接收和读取加密的信息，并可以向Reader发送虚假信息。

(4) 克隆。经常与欺骗联合使用的一种攻击手段，两者都是从一个合法的Tag复制数据，但欺骗是模拟Tag数据的传输，而克隆则复制数据到攻击者自己的Tag中，克隆Tag攻击更具有目的性和

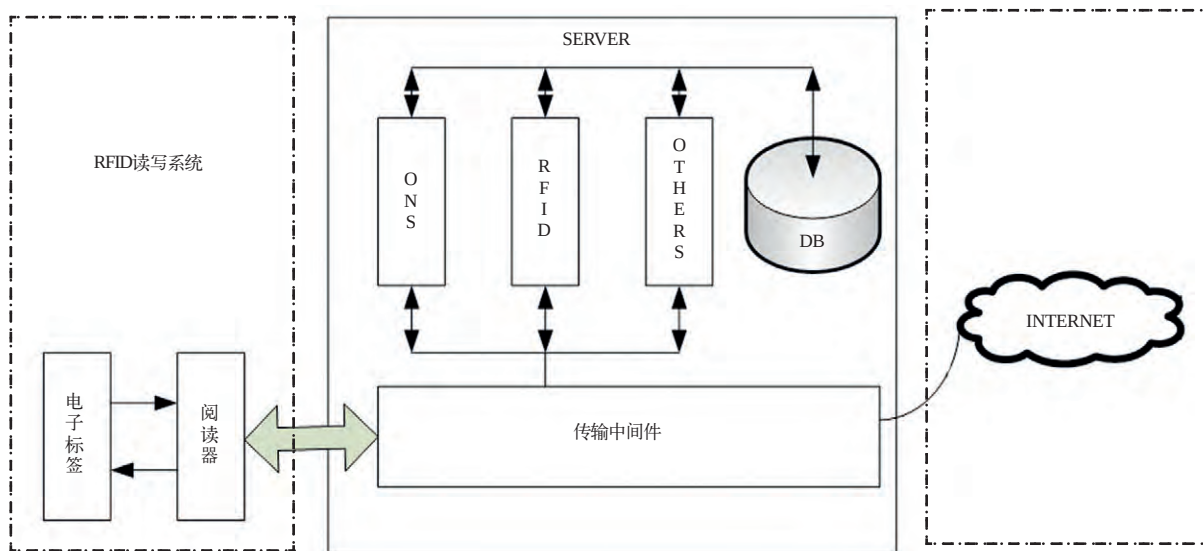


图 RFID技术在智能电网中的应用示意图

危险性。

(5) 跟踪。RFID Tag中含有可被读取的ID, 该ID具有唯一性, 通过该ID就可以唯一标识一个或一组实体的身份。这种关联建立起来后, 通过一个特殊的Reader就可以定位到这个实体的位置信息, 从而可以长时间的跟踪这个实体。

3.2 防护策略分析

针对上述RFID技术在智能电网应用中的安全风险, 本节着重就相关的安全防护策略进行分析。

(1) Tag Kill。在需要的时候使用一个特殊命令Kill使Tag失效, 接收到Kill命令的Tag将失去其所有功能, 无法再发射和接收数据, 其过程不可逆。但是目前只有部分Tag支持Kill命令, Kill命令原理是将特殊PIN码写入Tag, 从而使Tag中所有信息被破坏失效, 从而达到隐私保护目的。由于操作具有不可逆性, 所以Tag Kill方案需谨慎使用, 适用范围有限^[5]。

(2) Tag Lock。与Tag Kill策略一样, Tag Lock同样需要PIN码激活, 将特殊的PIN码写入Tag后, 系统将处于半关闭状态, 但Tag中的信息并未被破坏, 封闭Tag中数据信息只能反馈Tag。但Tag lock防护策略存在着漏洞, 通过读取特殊ID, 可以再次写入PIN码, Tag将被激活并能够进行数据传输。

(3) Tag Block。Tag数据信息获取基于二叉树查询算法, Tag Block通过模拟Tag ID来干扰算法的查询过程。Tag Block方法的优点在于不需要对Tag进行修改或加密, 是一种有效的隐私保护手段。但Tag Block也可以被恶意使用发起攻击, 利用模拟Tag ID, 对隐私保护范围之外的Tag进行Block, 从而干扰正常的RFID应用。

(4) RFID Guard。RFID Guard是一组具备查询、记录和展示RFID Tag的设备, 能够管理RFID Key、鉴别RFID Reader, 并且能够阻止没有授权的Reader读取使用RFID Tag。RFID Guard需随身携带, 使用成本较高, 进行普遍推广有困难。

(5) Cryptonym ID。Cryptonym ID使用对称加密算法将加密后的ID以密文形式存储在Tag上, 防止攻击者窃取真实的Tag ID。Cryptonym ID策略能够防止Tag中数据信息的泄露, 但不能防止Tag被跟踪。若要防止Tag信息被跟踪, 存储在Tag中

的Cryptonym ID需要进行多重加密。多重加密通过特殊的Reader从Tag中获得Cryptonym ID, 并用再次或多次加密(密钥不同)的Cryptonym ID覆盖旧的Cryptonym ID, 但这种多重加密方案对Tag设备的规格要求较高, 硬件成本较高, 并且多重加密的时间代价较大。

(6) 公钥加密。公钥加密通过非对称密码算法进行加密与解密。为RFID Tag与Reader分别分配私钥和公钥, 私钥加密信息将阻止未被授权的RFID Reader读取。公钥加密通过改变RFID Tag的公开密钥来增强实体的隐私, 使实体能够不被标有特殊Tag的公开密钥所追踪。

(7) Hash Lock。Hash Lock使用元ID来代替Tag ID, 避免信息被泄露或追踪, 该机制中ID不会动态刷新, 元ID保持不变。Tag ID以明文的形式在不安全的信道进行传输, 使得Hash Lock机制易受到假冒和重传攻击^[6]。

(8) Random Hash Lock。Random Hash Lock采用基于随机数的询问-应答机制, 通过认证的标识ID以明文的形式在不安全信道中进行传输, 攻击者容易对Tag进行追踪, 在获取到Tag的标识ID以后, 攻击者就可以对Tag进行假冒和重传攻击, 安全性不完善。而且, 每次对Tag进行认证时, 后台数据库都需要将所有Tag的ID数据发送给Reader, 二者之间的进行大量的数据传输, 造成带宽资源的浪费。

(9) Hash Link。在Hash Link中, Tag对使用不同哈希函数发起认证的Reader发送不同的应答, Tag具有主动性, 能够自主更新ID。但是, Hash Link采用单向认证机制, 只能单向对Tag身份进行认证, 不能逆向对Reader身份进行认证, 所以Hash Link易受到重传和假冒攻击。此外, 在每一次Tag认证时, 后台数据库都要对每一个Tag进行一次哈希运算, 其计算载荷很大。同时, 该机制需要两个不同的哈希函数, 增加了Tag设备的制造成本。

(10) Delegation Tree Authentication。基于分享密钥和假名功能的改进算法。使用RFID假名与一个链接RFID Reader的信任中心, 这个信任中心可以操控隐私政策并且限制Reader读取Tag。当一个新的Tag加入这一由信任中心提供的密钥系统

时，信任中心则保持密钥的树状结构，Tag信息和Tag隐私政策以数据库形式呈现。

3.3 防护策略对抗安全风险的能力对比

上述RFID防护策略可以分为密码型防护策略与非密码型防护策略，将五种密码型防护策略与五种非密码型防护策略在对抗窃听、欺骗、拒绝服务、跟踪和克隆安全风险的能力进行对比

如下表所示，RFID防护策略对抗安全风险能力对比，可以发现非密码保护策略对抗RFID安全风险更加有效，但是在智能电网实际环境中非密码保护策略使用有限。而密码保护策略更适用于智能电网应用环境，对安全与隐私的保护更具有弹性。但是从下表中可以看出没有一个防护策略能够对抗目前所有的RFID安全风险。

表 RFID防护策略对抗安全风险的能力对比

防护策略类别		RFID信息安全风险				
		窃听	欺骗	拒绝服务	跟踪	克隆
RFID防护策略	非密码策略	Tag Kill	✓	✓	✓	✓
		Tag Lock	✓	✓	×	×
		Tag Block	✓	✓	✓	✓
		RFID Guard	✓	✓	✓	✓
		Cryptonym ID	✓	✓	×	✓
	密码策略	公钥加密	✓	✓	×	✓
		Hash Lock	✓	✓	×	×
		Random Hash Lock	✓	✓	×	✓
		Hash Link	✓	✓	×	✓
		Delegation Tree Authentication	✓	✓	×	×

4 结束语

由于智能电网的特殊性，随着RFID技术在智能电网中应用的增多，RFID技术的安全性变得愈发重要。虽然RFID技术安全标准逐步出台，但目前仍旧缺乏十分有效抵抗或预防RFID安全风险的策略。RFID技术本身安全技术的完善将影响其未来的应用前景，而RFID在智能电网应用中安全防护策略的研究势必影响智能电网的安全发展。

参考文献

[1] 余贻鑫, 栾文鹏. 智能电网述评[J]. 中国电机工程学报, 2009, 29(34): 1-6.

[2] 蓝毓俊. 智能电网及其关键技术[J]. 智能电网, 2010(1): 9-11.

[3] 胡婕, 宗平. 面向物联网的RFID安全策略研究[J]. 计算机技术与发展, 2011(5): 151-154.

[4] 杨海东, 杨春. RFID 安全问题研究[J]. 微计算机信息, 2008(8): 238-240.

[5] 周永彬, 冯登国. RFID 安全协议的设计与分析[J]. 计算机学报, 2006(4): 581-589.

[6] 祝胜林, 杨波, 张明武. RFID 协议及其安全性研究[J]. 信息安全与通信保密, 2007(8): 168-170.

(收稿日期: 2015-05-15) EA

作者简介

吕旭明 (1981-), 男, 硕士研究生, 高级工程师, 主要研究方向为电力企业信息化、智能电网、信息安全。

刘扬 (1982-), 男, 硕士研究生, 工程师, 主要研究方向为网络与信息安全。