

# 面向智能用电信息采集终端的访问控制协议

唐良瑞<sup>1</sup>, 李荣荣<sup>1</sup>, 翟峰<sup>2</sup>

(1. 新能源电力系统国家重点实验室(华北电力大学), 北京市 102206; 2. 中国电力科学研究院, 北京市 100192)

**摘要:** 针对智能用电信息采集系统的建设需求,将射频识别(RFID)技术应用于采集终端全过程管理中,为解决RFID系统在终端身份认证及信息传输过程中存在的众多隐私安全漏洞,提出了面向智能用电信息采集终端的访问控制协议。该协议分为终端身份认证和终端信息访问控制两个阶段,采用哈希(hash)函数、私有密钥及随机密钥保证了消息的隐私性与安全性。为满足实际信息采集和终端维护需求,将识别器对采集终端的操作权限融入协议设计中,保证了终端敏感信息的安全。非形式化分析说明新协议能够有效地抵御阻断攻击、欺骗攻击及识别器非法访问攻击等6类攻击。协议在保证采集终端安全接入情况下实现终端信息的合法操作,可从设备层面提高用电信息采集系统的安全防护水平。

**关键词:** 智能用电信息采集系统; 射频识别(RFID); 访问控制; 安全防护

## 0 引言

智能配用电通信网中,为实现电力用户用电信息数据的全面采集,必须要保证智能电表等采集终端的安装数量达到一定的规模<sup>[1]</sup>。如此大批量采集终端的安装、运行、维护等全过程的管理,仅依靠传统的“人力”管理模式,不仅会导致采集终端管理效率的低下,而且还会使得终端的安全性无法得到可靠保证。射频识别(RFID)技术作为物联网中最有应用前景的技术之一,其具有抗电磁干扰、多终端批量识别等优点,非常适用于大批量采集终端的全过程管理,实现对采集终端的全过程监测,确保采集终端的正常运行以及故障后的快速维护。但由于RFID技术采用无线通信技术,其在带来快速便捷性的同时也相应地带来了安全认证、身份信任和数据保密性等信息安全防护问题<sup>[2]</sup>。

目前,国内外针对RFID系统安全认证协议及相关加密算法的研究已取得丰硕的成果。文献[3-5]对各类RFID安全防护方案的抗攻击能力、协议存储量、协议通信次数等方面进行了分析对比。文献[6]利用随机序列来保证认证信息的新鲜性,可

有效抵御多种攻击,但无法实现对读写器的身份认证,且协议安全性依赖于随机序列的长度,不适用于存储能力有限的低成本标签,协议中消息关联性也较大,信息容易暴露。为解决上述问题,文献[7]提出一种基于随机数同步更新的安全协议,协议中随机数不仅在标签认证过程中使用,还作为密钥加密信息,可防止流量分析和位置跟踪等攻击,但协议复杂度较高。文献[8]对文献[9]提出的可抵御一次阻断攻击的协议进行了改进,使得新协议可抵御任何次数的阻断攻击,但后台数据库计算量剧增,无法保证时延要求。此外,现有协议都未考虑到识别器对终端信息操作权限的问题,在实际应用中,终端部分敏感信息需要识别器在授权下才可进行写入更改,这样可防止识别器越权操作引起终端信息与后台数据库备案信息的不一致。

本文针对RFID技术在用电信息采集系统中批量采集终端全过程管理方面的具体应用,提出了一种面向智能用电信息采集终端的访问控制协议。协议分为终端身份认证和终端信息访问控制两个阶段,终端身份认证阶段实现对采集终端和识别器的身份认证,保证本次会话终端的合法性,终端信息访问控制阶段则是保证识别器按照后台数据库为其分配的权限对终端信息进行合法的操作。新协议通过信息的安全合法交互保证了各类采集终端的安全性,从设备层面提高了用电信息采集系统的安全防护水平。

收稿日期: 2015-09-07; 修回日期: 2015-12-08。

上网日期: 2016-01-07。

国家高技术研究发展计划(863计划)资助项目(2014AA01A701); 北京市自然科学基金资助项目(4142049)。

## 1 RFID技术在智能采集终端全过程管理中的应用分析

在用电信息采集系统建设中,智能电表、集中器等采集终端(包括计量设备)的准确可靠直接关系到供电企业和用电客户的切身利益。各类采集终端从采购、维修到报废的整个生命周期内,任何环节出现问题,都将会降低用电信息采集系统的安全性,还会给电网造成因设备购置更换及用电信息缺失引起的经济损失。传统的终端管理采用条形码技术,其识别效率不高,需人工近距离读取,无法同时识别多终端,且标签不能重复使用,从而导致智能采集终端检测不完善、仓储管理成本大、运行维护缺乏有效在线管控等情况。

RFID是一种无线通信技术,能以非接触方式自动识别终端信息并获取相关数据,实现任意时刻的终端状态有章可查。RFID电子标签具有寿命长,存储量大、抗电磁干扰、可轻易嵌入终端、可多终端批量识别,识别距离长等优点<sup>[10]</sup>。在采集终端管理中引入RFID系统,将采集终端信息写入RFID标签,采用支持无线数据通信的RFID识别器对采集终端进行管理,可大幅度提高工作效率,节省人工成本,避免人工盘点中的各种差错,让电力企业更加准确地掌握采集终端的存量、分布状况及检修状况,有效提高各类采集终端及计量设备的管理水平,降低经营管理风险。

图1为RFID技术应用于采集终端全过程管理时所面临的威胁模型。识别器与后台数据库间通过安全信道进行通信,但采集终端标签与识别器间采用非接触式短距离无线通信,信息在无线信道中传输时不安全,可能会面临欺骗攻击、假冒攻击<sup>[11]</sup>、非法访问攻击、篡改攻击<sup>[12]</sup>、重传攻击等威胁。

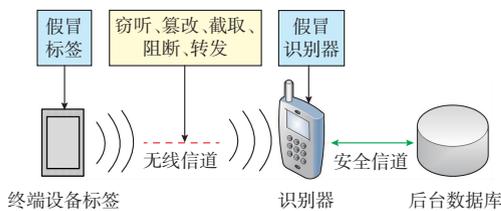


图1 RFID系统的威胁模型  
Fig.1 Threat model of RFID systems

在进行智能用电信息采集终端的访问控制协议设计时,需要特别注意以下问题。

1)对识别器进行权限设定。根据实际采集终端管理需求,识别器对设备终端信息的操作权限分为“只读”和“读写”两种。例如对现场采集终端进行检修后,需要向终端录入本次检修记录。这不仅要求

识别器可以读出终端信息,还能够在后台允许的情况下随时对终端信息进行更改并与后台同步。

2)协议应当是双向认证。即实现终端身份的认证及识别器身份的认证,防止任何一方的虚假接入。

3)后台数据库负责密钥的配发。例如,智能电表进行入库检定后,需要更换电表出厂时的密钥。这样可以提高智能电表的安全性,做到分工明确,加强计量中心对智能电表的控制管理。

4)认证过程简单,协议复杂度不高。由于采集终端上嵌入的是无源标签,功率有限,复杂的认证会超出标签的处理能力,在进行批量终端处理时,还可导致网络流量增加,影响认证速度。

## 2 面向智能用电信息采集终端的访问控制协议

### 2.1 协议符号定义

为简化协议的详细阐述过程,现对有关符号作如下定义。

D, R和T依次代表后台数据库、识别器和采集终端标签; $I_R$ 为R的本次会话ID标识; $Q$ 为识别器发出的会话请求; $S_T$ 为T的假名, $I_T$ 为T的本次会话ID标识, $P_T$ 为T的上次会话ID标识; $H_T$ 为 $I_T$ 经哈希(hash)运算后的散列值;随机数 $r_x$ 由会话实体X的随机数发生器产生,可为每次协议会话提供新鲜性防护,以抵抗重放攻击; $W$ 表示R对T信息的操作权限, $W=0$ 表示“只读”, $W=1$ 表示“读写”; $C$ 为同步更新标识,用来检验D与T会话标识是否完成同步更新, $C=0$ 表示二者同步更新成功, $C=1$ 表示同步更新失败;符号“||”代表两个输入值的串联;符号“?”代表两个输入值的比较。

### 2.2 协议流程描述

首次运行协议前,需进行初始化:后台数据库为R与T分配初始会话标识 $I_R$ 与 $I_T$ 、分配二者与后台数据库通信的密钥 $K_R$ 与 $K_T$ ,将R的权限标识 $W$ 置为“0”,将T的会话更新标识 $C$ 置0,并将该T所对应的 $I_T$ 与 $P_x$ 都置为 $I_T$ , $H_T$ 置为 $H(I_T)$ ;R存储初始会话 $I_R$ 、权限 $W$ 及与后台数据库通信的密钥 $K_R$ ;T存储假名 $S_T$ 、初始会话 $I_T$ 、会话更新标识 $C$ 及与后台数据库通信的密钥 $K_T$ 。当识别器需要对采集终端标签信息进行操作时,首先由识别器发起请求,之后在后台数据库的协助下完成识别器和采集终端身份的双向认证、通信密钥的协商及识别器权限的设定,之后再行终端标签信息的加密传输。面向采集设备的身份认证协议的具体通信过程描述如下。

步骤1:R产生随机数 $r_R$ ,与 $Q$ 一起发送给T,

发起本次会话请求。

步骤2:接收到 $Q$ 和 $r_R$ 后, $T$ 产生随机数 $r_T$ ,并根据 $C$ 的状态计算相应的 $P_T$ 参数,若 $C=0$ ,则 $P_T=H(I_T)$ , $C=1$ ,否则 $P_T=H(I_T \parallel r_T)$ ,之后 $T$ 将 $P_T$ 和 $r_T$ 发送给 $R$ ,作为对 $R$ 发起的 $Q$ 的响应。

步骤3: $R$ 收到 $T$ 发来的 $P_T$ 及 $r_T$ ,令 $P_R=H(I_R \parallel r_R)$ ,将 $P_T, r_T, P_R$ 及 $r_R$ 发送给 $D$ 。

步骤4: $D$ 接收到 $R$ 发来的信息后,首先对 $R$ 进行认证,利用接收到的 $r_R$ ,在数据库中搜索满足 $H'(I_R \parallel r_R)=H(I_R \parallel r_R)$ 的 $I_R$ ,如果未找到,则终止本次会话过程,若能够找到,则接着对 $T$ 进行认证,认证流程如下。

步骤4.1:在数据库中遍历所有 $I_T$ 的 $H_T$ ,比较 $H_T \neq P_T$ ,若存在这样的 $H_T$ ,则认为本次请求认证的标签会话标识为 $I_T$ ,并令 $P_T=I_T$ ,这意味着上次会话过程正常结束。

步骤4.2:若在数据库找不到任何 $H_T$ 与 $P_T$ 相同,那么就利用接收到的 $r_T$ 计算 $H(I_T \parallel r_T)$ ,并比较 $H(I_T \parallel r_T) \neq P_T$ ,若等式可成立,令 $P_T=I_T$ ,这意味着上次会话过程中,在步骤2中 $T$ 向 $R$ 发送的应答信息被阻断,从而导致 $T$ 内的会话更新标识 $C=1$ ,但 $D$ 与 $T$ 中的标签会话标识 $I_T$ 都没有更新, $D$ 在本次会话过程时可发现该错误并有能力对其进行纠正。

步骤4.3:若此时 $D$ 还搜索不到对应于 $I_T$ 的 $T$ ,则计算 $H(P_T \parallel r_T)$ ,并比较 $H(P_T \parallel r_T) \neq P_T$ ,若等式可成立,这意味着上次会话过程中,步骤5中 $D$ 向 $T$ 发送的回复消息受到阻断,导致 $D$ 中的标签会话标识 $I_T$ 更新了,而 $T$ 中的标签会话标识 $I_T$ 却未发生更新, $D$ 在本次会话过程时发现该错误并对其进行纠正。

步骤4.4:经过步骤4.1—4.3,若还未找到可以相匹配的 $T$ ,则 $D$ 终止本次会话过程。

$D$ 完成对 $T$ 的身份认证后,则令 $Q_T=K_T(S_T \parallel r_T \parallel r_R)$ , $M_T=H(I_T \parallel r_T \parallel r_R)$ ,并为 $R$ 与 $T$ 的本次会话任务分配密钥 $K$ ,确定 $R$ 对 $T$ 的本次操作权限 $W$ ,之后将 $K_R[K, W, K[M_T], Q_T]$ 传回给 $R$ ,并更新 $I_T=H(P_T \parallel r_R)$ 和 $H=H(I_T)$ ,以为下次会话任务做准备。

步骤5: $R$ 接收到 $D$ 的回复消息后,利用密钥 $K_R$ 解密,获得权限标识 $W, Q_T, K[M_T]$ 及本次会话密钥 $K$ ,利用 $Q_T$ 加密 $K, W, K[M_T]$ 并将其发送给 $T$ 。

步骤6: $T$ 收到 $R$ 发来的消息后,利用假名 $S_T$ 和密钥 $K_T$ 计算 $Q_T$ ,解出 $D$ 分配的本次会话密钥 $K$ ,权限标识 $W$ 及 $K[M_T]$ ,再利用 $K$ 解出 $M_T$ ,若

$M_T=H(I_T \parallel r_T \parallel r_R)$ ,则 $T$ 更新会话标识 $I_T=H(I_T \parallel r_R)$ ,置 $C=0$ ,本次会话过程身份认证成功,进入数据传输阶段。

在采集设备信息访问控制协议中,本次身份认证成功, $R$ 将需要传输的消息及请求用本次会话密钥 $K$ 加密发送给 $T$ 。 $T$ 收到加密消息后,利用会话密钥 $K$ 解密,依据消息内容进行如下处理。

步骤6.1:若 $R$ 请求读取标签信息,则将 $R$ 所需读取的消息用密钥 $K$ 加密,并返回给 $R$ 。

步骤6.2:若 $R$ 需要向标签写入信息,则 $T$ 通过 $W$ 来验证 $R$ 是否具有该权限。

步骤6.2.1:若 $W=0$ ,则 $T$ 向 $R$ 发送越权警告,越权次数 $i=i+1$ ( $i$ 初始为0),当越权次数超过门限,标签不再响应识别器的任何要求。

步骤6.2.2:若 $W=1$ ,则 $T$ 按 $R$ 的要求写入信息,并向 $R$ 回送该信息以确认该信息已被正确写入;至此, $R$ 对 $T$ 完成一次信息交互后,即可进入下一次信息请求处理过程,直到 $T$ 检测到 $R$ 的信号功率低于阈值功率,代表 $R$ 与 $T$ 完成了本次会话过程。在此过程中,若 $D$ 与 $R$ 需要进行信息交互,则由任何一方发起请求 $K_R$ [信息],另一方根据对方要求回应 $K_R$ [信息]即可。

### 3 协议隐私安全属性及抗攻击能力分析

在智能用电信息采集终端全过程管理中,RFID协议漏洞一般分为安全漏洞与隐私漏洞<sup>[13]</sup>。安全漏洞主要是指攻击者利用该类漏洞能够通过身份认证或者破坏采集终端的正常认证。隐私漏洞主要是指认证协议泄露了采集终端的隐私信息,使得攻击者利用截获的信息伪造终端标签进入系统内部进行有计划的攻击。

#### 1) 假冒攻击

攻击者通过窃听认证过程中标签与识别器间交互的消息,提取出标签包含的信息,复制标签数据到伪造标签中,进而可假冒合法标签侵入RFID系统进行有计划的攻击。

在身份认证协议中, $R$ 与 $T$ 间信息交互共三次:步骤1中交互的信息不涉及标签身份信息;步骤2中随机数 $r_T$ 及每次会话过程中 $I_T$ 的更新保证了每次会话中 $P_T$ 的随机性,hash函数的单向性则使得消息被破解的概率几乎为零;步骤5中的密钥 $Q_T$ 是由标签假名 $S_T$ 、随机数 $r_R$ 及 $r_T$ 、标签密钥 $K_T$ 生成的,密钥 $Q_T$ 在每次会话中都将更新。由于步骤1与步骤2中并没有以任何形式传输标签假

名  $S_T$  和标签密钥  $K_T$ , 因此攻击者仅利用  $r_R$  及  $r_T$  无法获知每次都被更新的密钥  $Q_T$ 。

在信息访问控制协议中, 标签与识别器间的密钥  $K$  在每次会话过程中都会改变, 且传输内容不涉及标签身份信息。

#### 2) 欺骗攻击

与假冒攻击不同, 欺骗攻击不是对标签进行复制伪造, 只是模拟标签数据传输过程, 使得合法识别器认为与其进行信息交互的是可通过认证的标签。同样攻击者也可通过模拟识别器数据传输的过程, 使得合法标签以为与其进行通信的是合法可通过认证的识别器。本协议中, 除非破解认证过程中采用的协议, 否则攻击者无法获知识别器与标签间消息交互的规则, 因此无法达到欺骗攻击的目的。

#### 3) 识别器非法访问攻击

相对于标签的假冒攻击, 若识别器身份是非法的, 则识别器对合法标签的信息读取就为非法访问攻击。在身份认证协议中, 当非法识别器申请身份认证时, 由于当前采用的认证协议未知, 攻击者只能先阻断合法识别器的认证消息, 然后将截获的消息  $\{P_T, r_T, P_R, r_R\}$  发送给后台数据库, 后台数据库则可成功认证识别器的身份, 并发送响应消息  $\{K_R[K, W, K[M_T], Q_T]\}$ 。但由于非法识别器无法获知与后台通信的密钥  $K_R$ , 无法从响应消息中获得本次会话密钥, 且在步骤 5 中无法通过终端标签的身份认证, 因此不能对标签信息进行访问。

另外, 针对合法识别器的非法“写”操作, 标签通过识别权限标识  $W$  来判断识别器是否有“写”操作权限, 若无, 则向识别器返回相应的“写”权限错误报告, 若识别器在明知无权“写”操作时仍不断对终端标签发起“写”请求, 当次数  $i$  达到阈值后, 终端标签在本次会话过程中将不再响应该识别器任何请求。

#### 4) 重传攻击

RFID 系统中, 重传攻击分为两种: 一种是攻击者伪装成识别标签, 重传标签发送给识别器的响应消息; 另一种是攻击者伪装成识别器, 重传识别器对终端标签的认证请求。抵抗重传攻击主要包括时间

戳和随机数两种方法。本协议采用随机数的方法抵抗重传攻击, 识别器与终端标签交互的信息中都包含识别器产生的随机数  $r_R$  以及标签产生的随机数  $r_T$ , 通过比较发送和接收到的随机数是否一致, 便可以识别出攻击者的攻击行为。

#### 5) 篡改攻击

由于无法获知认证密钥, 通常攻击者无法将原信息篡改成另外一条合法信息, 所以篡改攻击只能造成认证失败, 而不会造成错误认证。但对于密钥更新, 攻击者先阻断消息的传输, 然后进行篡改攻击却是致命的。

新协议中  $T$  与  $D$  间的通信密钥  $K_T$ ,  $R$  与  $D$  间的会话密钥  $K_R$  均不进行更新, 但  $T$  与  $R$  间的会话密钥  $K$  是由  $D$  随机分配, 每次会话过程都会进行更新, 但  $D$  并不存储该密钥  $K$ 。在步骤 5 中, 由于攻击者无法破解密钥  $Q_T$ , 对消息的篡改攻击只能造成  $T$  对  $R$  认证的失败, 本次认证过程将终止。

#### 6) 阻断攻击

若识别器与终端标签信息交互的过程可能会遭遇攻击者阻断, 通常阻断攻击还会导致后台数据库与标签密钥更新不同步, 从而引起非同步攻击。若攻击者阻断步骤 1 中发送的消息, 将对终端标签及识别器无任何影响; 若阻断了步骤 2 中  $T$  对  $R$  的响应消息, 将导致  $T$  内的会话更新标识  $C=1$ , 但  $D$  与  $T$  中的标签会话标识  $I_T$  都没有更新; 若在步骤 5 中,  $D$  向  $T$  发送的回复消息受到阻断, 将导致  $D$  中的标签会话标识  $I_T$  发生更新, 但  $T$  中的标签会话标识  $I_T$  却未发生更新。在本协议中,  $D$  在收到  $R$  发送的消息后, 可以通过  $P_T$  来验证上次会话过程中步骤 2 或步骤 5 发送的消息是否被阻断, 并有能力在本次会话过程对其进行纠正, 因此可以很好地抵御阻断攻击。

综上所述, 本协议与现有其他 RFID 安全协议在身份认证能力、抵御攻击能力等方面的对比如表 1 所示, 其中,  $\checkmark$  和  $\times$  分别代表该协议是否可抵御此类攻击。表 2 所示为计算量、存储量和通信量等性能指标的对比。

表 1 RFID 协议安全性分析  
Table 1 Security analysis of RFID protocols

方案	认证性	重传攻击	假冒攻击	篡改攻击	阻断攻击	信息读取权限
本文提出的协议	具备	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
基于密钥阵列的 RFID 认证协议	具备	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
基于随机序列的 RFID 安全协议	具备 $R \rightarrow T$	$\checkmark$	$T(\checkmark)R(\times)$	$\checkmark$	$\times$	$\times$
文献[8]提出的协议	具备	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\times$
文献[14]提出的协议	具备	$\checkmark$	$\checkmark$	$\checkmark$	$\times$	$\times$

表 2 性能分析对比  
Table 2 Performance analysis of RFID protocols

方案	通信次数		存储量/bit			运算量	
	D 与 R	R 与 T	D	T	R	T	R
本文提出的协议	2	3	5L+2K	1L+1K	2L+1K	3H+1U	1H+1U
基于密钥阵列的 RFID 认证协议	2	3	$nL+nK$	$nL+nK$	1L+1K	3U	3U
基于随机序列的 RFID 安全协议	2	4	1S+1A	1S+1A	0	5X+3H	1X+1H
文献[8]提出的协议	0	2	0	1L	1L	2H	nH
文献[14]提出的协议	0	5	3L+6K	2L+6K	1L+3K	3X	6X

注: A:密钥矩阵;L:标签标识符;S:随机序列;K:密钥;H:hash 运算;X:异或运算;U:解密运算; $n$  表示若干次;存储量:以表 2 中第一行 5L+2K 为例,其表示后台数据库 D 中存储有 5 个标签标识符和 2 个密钥;运算量:以表 2 中第一行 3H+1U 为例,其表示阅读器需要进行 3 次 hash 运算和 1 次解密运算。

由表 1 和表 2 可知,对比其他现有 RFID 协议,本文所提出的访问控制协议在未大幅增加通信次数、存储量及计算复杂度的情况下,不仅可抵御常见的重放、假冒等攻击类型,还可抵御较难处理的信息阻断攻击,尤其是新协议对识别器权限的设定,保证了终端信息只能在授权下才可被识别器读写,加强了终端全过程管理中终端信息的安全性,从设备层面为用电信息采集系统的安全性提供保证。

## 4 结语

本文针对 RFID 技术在智能用电信息采集系统终端全过程管理方面的具体应用,提出了一种面向智能用电信息采集终端的访问控制协议。协议分为终端身份认证和终端信息访问控制两个阶段,采用单向 hash 函数、标签假名及随机密钥保证了消息的隐私性与安全性。在终端身份认证阶段通过引入随机数  $r_T$  和  $r_R$ ,避免了重放及篡改攻击的威胁;后台数据库记录标签上次会话标识  $P$ 、会话更新标识  $C$  则有效地抵御了假冒攻击、欺骗攻击及阻断攻击;在终端信息访问阶段,将识别器对智能电表标签的操作权限融入协议中,可防止合法识别器非法访问攻击,实现识别器对终端信息进行有限权限的操作,以满足实际设备管理需求。新协议从设备层面保证了采集设备的安全,为下一步研究用电信息采集系统网络层安全防护机制奠定了基础。

## 参考文献

- [1] 徐震,刘韧,于爱民.智能电网中的移动应用安全技术[J].电力系统自动化,2012,36(16):82-87.  
XU Zhen, LIU Ren, YU Aimin. Mobile application security technology for smart grid[J]. Automation of Electric Power Systems, 2012, 36(16): 82-87.
- [2] 赵兵,高欣,郝盼盼,等.适用于用电信息采集的轻量级认证密钥协商协议[J].电力系统自动化,2013,37(12):81-86.  
ZHAO Bing, GAO Xin, GAO Panpan, et al. A light authenticated protocol with key agreement for power utilization information collecting [J]. Automation of Electric Power Systems, 2013, 37(12): 81-86.
- [3] 胡江溢,祝恩国,杜新纲,等.用电信息采集系统应用现状及发展趋势[J].电力系统自动化,2014,38(2):131-135. DOI: 10.7500/AEPS20130617005.  
HU Jiangyi, ZHU Enguo, DU Xingang, et al. Application status and development trend of power consumption information collection system[J]. Automation of Electric Power Systems, 2014, 38(2): 131-135. DOI: 10.7500/AEPS20130617005.
- [4] HE D, ZEADALLY S. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography [J]. IEEE Internet of Things Journal, 2015, 2(1): 72-82.
- [5] 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 Wei, GUO Tao, DONG Guowei, et al. Vulnerability analysis of RFID authentication protocols [J]. Journal of Tsinghua University (Science and Technology), 2013, 53(12): 1719-1725.
- [6] 杨漾,黄小庆,曹一家,等.变电站通信报文安全认证及其实时性仿真[J].电力系统自动化,2011,35(13):77-82.  
YANG Yang, HUANG Xiaoqing, CAO Yijia, et al. Security authentication for substation communication message and its real-time simulation[J]. Automation of Electric Power Systems, 2011, 35(13): 77-82.
- [7] 钱权,贾彦龙,张瑞.基于随机数同步更新的 RFID 安全协议[J].计算机工程,2013,39(8):9-14.  
QIAN Quan, JIA Yanlong, ZHANG Rui. RFID security protocol based on synchronous update of random number[J]. Computer Engineering, 2013, 39(8): 9-14.
- [8] SUN D, ZHONG J. A hash-based RFID security protocol for strong privacy protection [J]. IEEE Trans on Consumer Electronics, 2012, 58(4): 1246-1251.
- [9] HA J H, MOON S J, ZHOU J Y, et al. A new formal proof model for RFID location privacy [C]// Proceedings of 13th European Symposium on Research in Computer Security, September 6-10, 2008, Malaga, Spain: 267-281.
- [10] MORSHED M, ATKINS A, YU H. Efficient mutual authentication protocol for radiofrequency identification systems[J]. IET Communications, 2012, 6(16): 2715-2724.
- [11] ARCO P D, DE SANTIS A. On ultralightweight RFID authentication protocols[J]. IEEE Trans on Dependable and Secure Computing, 2011, 8(4): 548-563.
- [12] HERNANDEZ-CASTRO J C, PERIS-LOPEZ P, PHAN R C, et al. Cryptanalysis of the david-prasad RFID ultralightweight authentication protocol [J]. 2010 International Workshop on

Radio Frequency Identification: Security and Privacy Issues, 2010, 12(10): 22-34.

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

[14] TIAN Y, CHEN G, LI J. A new ultralightweight RFID authentication protocol with permutation[J]. IEEE Communication Letters, 2012, 16(5): 702-705.

电力系统通信与信息处理、无线传感器网络与物联网技术。

E-mail: tangliangrui@163.com

李荣荣(1990—),女,通信作者,硕士研究生,主要研究方向:配用电通信网业务模型与安全性分析。E-mail: l\_r\_r1990@126.com

翟峰(1979—),男,工程师,主要研究方向:电能计量及用电信息安全。

(编辑 杨松迎)

唐良瑞(1966—),男,教授,博士生导师,主要研究方向:

## An Access Control Protocol for Intelligent Electricity Consumption Information Acquisition Terminals

TANG Liangrui<sup>1</sup>, LI Rongrong<sup>1</sup>, ZHAI Feng<sup>2</sup>

(1. State Key Laboratory of Alternate Electric Power System with Renewable Energy Sources (North China Electric Power University), Beijing 102206, China; 2. China Electric Power Research Institute, Beijing 100192, China)

**Abstract:** In view of implementation demands of the intelligent consumption information acquisition system, radio frequency identification (RFID) technology is applied to ensure acquisition terminals management. To solve the numerous privacy and security vulnerabilities in the process of terminals authentication and information transmission in RFID systems, an access control protocol for intelligent electricity consumption information acquisition terminals is proposed. The novel protocol is divided into two stages, the terminal identity authentication and the terminal information access control. The hash function, the private key and the random key are employed to ensure the privacy and security of messages. In order to satisfy the demands of actual information collection and terminal maintenance, the reader's operating authority over the acquisition terminal is taken into consideration, which ensures the security of the terminal sensitive information. The non-formalized method analysis indicates the new protocol can effectively resist as many as 6 kinds of attacks including the blocking attack, spoofing attack and recognizer illegal access attack, and it ensures safe access to acquisition terminals as well as legal operation of terminals information, which will improve safety protection level of the electricity consumption information acquisition system.

This work is supported by National High Technology Research and Development Program of China (863 Program) (No. 2014AA01A701) and Beijing Natural Science Foundation (No. 4142049).

**Key words:** intelligent electricity consumption information acquisition system; radio frequency identification (RFID); access control; safety protection