物联网加密技术研究

赵 文，吴传伟，罗 敏
(中国电子科技集团公司第三十研究所，四川 成都 610041)

[摘　要] 物联网是一种虚拟网络与现实世界实时交互的新型系统，随着物联网技术的迅猛发展，物联网终端的安全问题也逐渐被重视。文中通过分析物联网终端设备存在的认证、私隐等安全问题，针对终端设备计算能力、网络资源有限的特点，研究了基于 IBE 密钥参数协商和身份鉴别技术、轻量级加密算法和密码自同步技术，提出了将几种技术相结合的加密技术方案，并对这种方案的安全性进行了分析。

[关键词] 物联网；基于身份加密；轻量级加密
[中图分类号] TP309　　[文献标识码] A　　[文章编号] 1009-8054(2012)07-103-03

Study on Encryption Technology in Internet of Things

ZHAO Wen，WU Chuan-wei，LUO Min
(No.30 Institute of China Electronic Technology Corporation，Chengdu Sichuan 610041，China)

[Abstract] IoT(Internet of Things) is a new real-time interactive system in virtual network with the real world. With the rapid development of IoT technology，the security of IoT terminal gradually attracts much attention from the people. Based on analysis of its terminal equipment certification，privacy，and other security issues，and for its terminal equipment limitation in computing power，network resources，the IBE-based key parameter negotiation and identity authentication technologies，lightweight encryption algorithm，and self-synchronous encryption for password are studied，and the encryption technical scheme in combination of these technologies is proposed. And also the security of this scheme is analyzed and proved in detail.

[Keywords] IoT；identity-based encryption；lightweight encryption

0 引言

物联网 (Internet of Things) 是继计算机、互联网之后，世界信息产业的第三次浪潮，它以终端感知网络为触角，深入物理世界的每一个角落[1]，其应用理念使得机器间可以不通过人的交互直接进行信息交互，大大方便了人们的生活。物联网是一种虚拟网络与现实世界实时交互的新型系统，其核心和基础仍然是互联网，是在互联网基础上的延伸和扩展，其特点是无处不在的数据感知、以无线为主的信息传输、智能化的信息处理，用户端可以延伸和扩展到任何物品与物品之间，进行信息交换和通讯。因为与物联网相结合的互联网本身就早已存在许多安全问题，传感网和无线网络与一般网络相比存在着特殊的安全问题，而物联网又以传感网、无线网络为核心技术，更是给各种针对物联网的攻击提供了可能，使物联网所面临的安全问题更加严峻。

收稿日期：2012-06-08
作者简介：赵文，1977 年生，男，工程师，研究方向：信息安全；吴传伟，1982 年生，男，工程师，研究方向：信息安全；罗敏，1974 年生，男，高工，研究方向：信息安全。

1 物联网终端的安全问题

由于物联网在现有移动网络基础上集成了感知网络和应用平台，物联网的广泛应用，必将引起物联网终端设备的认证问题和私隐问题[2]。

1.1 终端的认证问题

在物联网中，终端设备无人值守，终端设备本身的安全以及信息源的安全无法保障，攻击者可以轻易接触到这些设备，对它们进行破坏，篡改其数据，甚至能够通过复制他人的终端信息顶替别人使用。这种篡改、克隆终端设备数据的行为是由终端设备信息被读取时无需认证引起的。

1.2 终端的私隐问题

物联网终端设备主要使用 RFID(Radio Frequency Identification)、传感器、二维码等方式的感知设备，使信息获取更加方便，同时也方便了恶意攻击者获取信息，如通过监听感知器和读写器的交互数据，读取感知器的内容。甚至，恶意攻击者通过测量设备的使用情况及所在位置等信息，获取用户的隐私信息，从而对用户造成伤害。

2 物联网加密技术

虽然物联网构造复杂，面临的环境和安全威胁也复

杂，安全基础要求也变高了，但是最基础的安全技术实质上没有改变，所依赖的依然是通信保障、加密技术手段。因此，作为保护信息私隐性的基本手段，需要针对物联网的特点，采用相应的认证技术、加密技术，对物联网终端信息进行安全保护[3]。

2.1 密钥协商和身份鉴别技术

物联网终端资源有限，例如，对于基于 ISO/IEC18000-6B 协议的电子标签，内部存储容量为 256 字节[4]，为阻止非法用户获取信息，还需要进行身份鉴别以保证物联网的安全。由于物联网大多没有固定的管理域，传统 PKI 的认证体制不能满足物联网的安全需求。

基于身份加密的 IBE(Identity-Based Encryption) 是一种将用户公开的字符串信息 (例如邮件地址、手机号码、身份证号码等) 用作公钥的加密方式[5]。2001 年，美国斯坦福大学的 Dan Boneh 和加利弗尼亚大学戴维斯分校的 MattFranklin 共同提出了具有开创性的基于标识的 IBE 算法[6]。在 IBE 方式下，公钥就是一段标志用户身份的字符串，而私钥由私钥产生机构 PKG(Private Key Generator) 产生，用户需要私钥时，由 PKG 根据用户标识计算后产生，并通过安全信道发给用户。

以终端 A 向终端 B 发送消息为例，密钥参数协商和身份鉴别流程如下 (见图 1)：

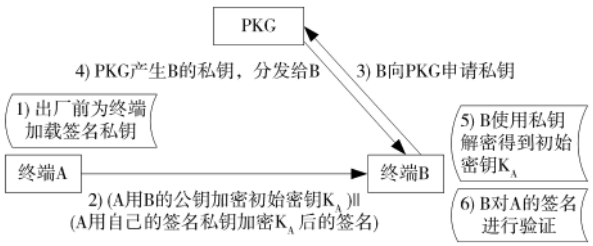

图 1 密钥参数协商和身份鉴别流程

1) 终端出厂前，首先为每个终端加载各自的签名私钥。

2) 终端 A 产生一段随机数种子，作为 A 加密的初始密钥 K_A；A 用终端 B 的公钥 (B 的用户身份标志) 加密初始密钥 K_A，并用自己的签名私钥计算 K_A 的数字签名，一同发送给终端 B。

3) 终端 B 第一次接收到加密信息时，由于没有可供解密的私钥，需要向 PKG 申请 B 的私钥。

4) PKG 验证了终端 B 的身份后，产生 B 的私钥后分发给终端 B。

5) 终端 B 使用私钥解密得到解密初始密钥 K_A。

6) 终端 B 利用终端 A 的签名公钥对 A 的签名进行鉴别。

为了提高随机数种子的安全性，终端 A 需要定期更换随机数种子，若终端 A 再次发起和终端 B 的通信，只需要用之前使用的 B 的公钥加密随机数种子，终端 B 直接通过自己的私钥来解密，无需 PKG 在线。

这种密钥协商方案的最大特点就是通过使用随机数种子及用户设备 ID 号等变量，直接实现初始密钥协商和身份鉴别，具有较高的安全性，其后续运行不需要可信第三方，对于终端的性能要求较低，适合于物联网安全应用。

这样，利用 IBE 技术，终端 A 和终端 B 完成了身份鉴别和初始密钥同步，解决了终端的认证问题，下节将讨论利用轻量级加密技术解决终端的私隐问题。

2.2 轻量级加密算法和密码自同步技术

物联网终端设备具有计算能力较弱、存储空间较小等特点，因资源的受限，物联网加密技术必须是一种易实现、安全系数较大、适合于敏感级信息环境下使用的轻量级加密技术。物联网小算法是解决物联网信息安全的可行方案。

文献 [7] 中提出过一种适合于 VoIP 传输的轻量级加密算法。由于物联网终端设备具有计算能力较弱、存储空间较小等特点，这种具有 “ 一次一密 ” 特性的小算法，速度快、实现简单、计算量小，适合于资源受限的物联网终端设备的业务加密，能够代替传统的复杂算法来保障物联网的安全性。

小算法的核心是采用数轮迭代方式，每轮的算法都是不固定的，每轮从预置的包含 n 种小算法的算法库中临时选择一种小算法，总的算法就是每轮选择的小算法之和。这样，通过适当的策略，算法的组合种类不断增大，从而在加解密过程中达到算法近似 “ 一次一密 ”。

小算法的密码参数同步依靠密文来维护，只要接收端能够连续正确接收到密文数据，就能够正确维护与发端之间的密码参数同步，实现密码自同步。

在图 1 的密钥参数协商和身份鉴别过程中，终端 A 和终端 B 之间完成了身份鉴别和初始密钥同步，利用已经协商好的初始密钥，终端 A 向终端 B 发送加密信息，流程如图 2 所示。

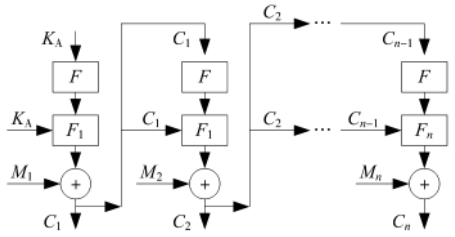

图 2 信息加密流程

图 2 中，K_A 为终端 A、终端 B 之间身份鉴别过程中协商的初始密钥；F 为小算法库；F_1，F_2，…，F_n 为每次加密前从小算法库中选出的加密算法；M_1，M_2，…，M_n 为待加密的明文；C_1，C_2，…，C_n 为加密后的密文。

首先，终端 A 使用初始密钥 K_A 选择出小算法 F_1，使用 K_A 加密第一个数据包 M_1，得到第一个密文包 C_1，即 $C_1=F_1(K_A, M_1)$。然后，终端 A 使用以上一次加密产生的密文 C_1 为参数选择小算法 F_2，并用 C_1 加密需要保护的第二个数据包 M_2，得到第二个密文包 C_2，即 $C_1=$

$F_2(C_1, M_2)$。同理，终端 A 选择小算法 F_n，完成 n 个数据包的加密，即 $C_n=F_n(C_{n-1}, M_n)$。由于使用的是对称算法，解密端用相同的密钥和小算法完成密文的解密。同样，终端 A 可以得到解密初始密钥 K_B，实现对终端 B 发送的密文数据包的解密。

加密时每一轮算法都是一种小算法，加解密速度快，满足物联网终端计算能力弱的特点，同时，终端间的密码自同步技术，使得终端之间能够自动完成后续密钥及算法选择参数的同步，不需要在后续加解密过程中在终端间传递同步参数，大大简化了密钥参数协商过程，满足了物联网网络资源受限的特点。

3 安全性分析

(1) 身份合法性

物联网终端设备 ID 号及参数可固化在终端设备中，保证身份的唯一性，业务通信时，终端设备采用 IBE 认证机制，有效验证了身份合法性。

(2) 数据机密性

物联网终端设备的初始密钥参数利用终端身份鉴别的过程，加密传输；设备间的业务信息通过小算法加密传输，保证了密钥参数传递、业务数据传递等交互流程的数据机密性。

(3) 算法随机性

轻量级加密算法采用小算法库方法，通过算法不断变化提供“一次一密”的特性，来代替传统算法提供的安全性。对于 n 种小算法，根据排列组合的原理，经过 m 轮之后，所有各轮算法之和即总的算法就可能有 N^M 种，保证了加密信息使用算法的随机性。

4 结语

对物联网安全技术的研究，目前仍然处于起步阶段，物联网终端的安全问题是决定物联网发展的关键，通过对物联网加密技术的研究，提出了一种将 IBE 密钥参数协商和身份鉴别技术、轻量级加密算法和密码自同步技术相结合的加密方案，在下一阶段的研究过程中，还将进一步考虑加密算法和认证算法的融合问题。

参考文献

[1] 孙论强，秦海权，尹丹 . 物联网安全接入网关的设计与实现 [J]. 信息网络安全，2011(9)：16-18.
[2] 姜丽芬，李章林，辛运帏 . 一种实用的轻量级 RFID 安全协议研究 [J]. 计算机科学，2009(9)：105-107.
[3] 周雪 . 陈克非：综合考量成为现有密码主要挑战 [J]. 信息安全与通信保密，2012(5)：9-11.
[4] 黄银龙，张辉，徐旭，等 . 车辆管理 RFID 电子标签内存规划研究 [J]. 通信技术，2010(2)：141-142.
[5] BONECH D，FRANKLIN M. Identity based Encryptionfrom Weil Pairing[C]. KILIAN J. CRYPTO2001. Berlin：Springer-Verlag 2001.
[6] 周棟淞，卿昱，谭平嶂，等 . 一种改进的基于标识的认证系统的实现 [J]. 信息安全与通信保密，2009(2)：61-63.
[7] 王飞，辛阳，杨义先，等 . 新型的适合于 VoIP 传输的轻量级加密算法 [J]. 电子科技大学学报，2009(1)：63-66.

(上接第 102 页)

加密技术相结合，降低了单纯的口令方式容易遭受破解的缺陷。该方法通过 RFID 技术来进行电子密钥的识别和判断，允许认证成功的用户进入 U 盘存储区进行正常的文件加密存储。

而对于认证不成功的用户，转入 U 盘引导区重新进行密码认证。该方法通过双重的身份认证，确保只有合法用户才能进入 U 盘存储区进行正常的加密存储，有效提高了 U 盘的数据安全。相信随着 RFID 技术的不断发展，发射器和感应装置的体积不断缩小，识别精度越来越高，该 U 盘加密方法将会不断发展。

参考文献

[1] 夏辉，张尧粥 . 移动存储介质安全防护系统设计 [J]. 通信技术，2008，41(9)：147-149.
[2] 马士超，王贞松 . 一种扇区级存储安全体系结构 [J]. 计算机工程，2007，33(4)：1-3.
[3] MAIS N，ZONG Ziliang，QIN Xiao. StReD：A Quality of Security Framework for Storage Resources in Data Grids[J]. Future Generation Computer Systems，2007，23(6)：816-824.
[4] 万晨妍，欧阳麟 . RFID 系统中信息保密机制研究与设计 [J]. 信息安全与通信保密，2011(9)：100-101.
[5] 沃尔玛，麦德龙 . RFID 革命的推动引擎 [EB/OL]. (2005-10)[2011-03-05]. http//www.233633.com/rfid/RFIDretailsals/20051001156101.htm.
[6] 孔令荣，樊矾 . 一种 RFID 标签信息安全传输协议 [J]. 信息安全与通信保密，2011(7)：90-94.
[7] 高正中，盛惠兴，宋依青 . 射频识别系统中安全认证协议的研究 [J]. 信息安全与通信保密，2010(8)：41-43.
[8] 王珺吉，王新征，汪松，等 . 基于 RFID 的军事物资管理系统 [J]. 信息安全与通信保密，2011(2)：64-66.