基于自签名隐式证书的认证密钥协商协议研究

赵 敏[1],江凌云[1],李占军[2]
(1. 南京邮电大学 通信与信息工程学院,江苏 南京 210000;
2. 国家电网辽宁省电力有限公司,辽宁 沈阳 110006)

摘 要:用户的身份认证和数据的保密传输是物联网信息安全中最基本的需求,而物联网中的终端设备一般呈分布式设置,大多数设备无人值守,因此需要有一个端到端的安全机制来保护物联网中的信息传输;物联网终端受带宽、计算能力和内存等限制,无法部署开销太大的安全协议。为了解决上述问题,提出并设计了一种基于 ECQV(Elliptic Curve Qu-Vanstone)自签名隐式证书的认证密钥协商协议,主要基于 ECQV 自签名隐式证书生成机制和公钥提取机制,可完成感知节点和用户之间的相互认证及安全传输通道的建立,占用内存小,认证效率高。以 C 语言编写的双向认证密钥协商协议基于 Contiki 操作系统在 WiSMote 节点上接受了实验验证和评估分析。实验结果表明,由于 ECQV 证书比传统证书所需要的数据量小,故减少了带宽的占用,且时间和能量消耗也有降低,效率大幅提升。所设计的协议完全可以部署在资源限制型物联网上,且具有良好的安全性。

关键词:物联网;ECQV;隐式证书;安全性
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2017)05-0128-05
doi:10.3969/j.issn.1673-629X.2017.05.027

Research on Authenticated Secret Key Agreement Protocol with Self-signed Implicit Certificate

ZHAO Min[1], JIANG Ling-yun[1], LI Zhan-jun[2]
(1. School of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210000, China;
2. State Grid Liaoning Electricity Power Company, Shenyang 110006, China)

Abstract: As well known, among all the information security requirements in Internet of Things (IoT) network, user authentication and data transmission confidentiality both are the most essential. However, edge devices in IoT are commonly distributed, and most of them are unattended, so it has become pressing to create an end-to-end security mechanism to secure the information transmission in IoT. Considering the confinations of devices in IoT network are bandwidth, computing power and memory limit, the IoT nodes cannot support heavy security protocol. In order to solve the above problems, a new authenticated key agreement protocol based on ECQV (Elliptic Curve Qu-Vanstone) self-signed implicit certificate has been introduced, which is based primarily on ECQV self-signed certificate generation scheme and ECQV self-signed implicit certificate public key extraction scheme and can perform mutual authentication between the user and node, with smaller footprint and higher authenticate efficiency. This proposed protocol programmed with C language run by Contiki operation system has been tested and evaluated with WiSMote nodes. Experiment results show that the ECQV certificate is smaller than traditional certificate, and thus the system bandwidth has been reduced as well as the time and energy consumption. In general the proposed protocol can be deployed on resource-constrained devices in IoT, and with better secure performance.

Key words: Internet of Thing; ECQV; implicit certificate; security

0 引 言

物联网(Internet of Things, IoT)致力于实现人物互连、物物互连。尽管 IoT 的概念和一些应用对大众来说已不再陌生,但是物联网安全目前还处于研究的初级阶段。无线传感网(Wireless Sensor Network, WSN)是物联网中一个很重要的技术领域,在物联网

收稿日期:2016-06-16 **修回日期**:2016-09-28 **网络出版时间**:2017-03-13
基金项目:国家自然科学基金资助项目(61271237)
作者简介:赵 敏(1991-),女,硕士,研究方向为网络与应用技术、物联网安全;江凌云,副教授,研究方向为下一代网络技术。

环境中,WSN 架构可分为集中式和分布式[1]。分布式网络的特点是设备分散化,这就需要安全管理身份信息,并验证连接用户的身份。在大多数物联网应用中,多个实体(比如感知节点、服务提供商和消息处理者)应通过彼此认证来首先建立一个受信任的网络,后续节点在成功完成身份验证后才可加入网络。设计这样的认证协议,不仅要能抵抗恶意攻击[2],还应该能在无线传感网中低性能的节点上轻量化部署。

为了解决物联网中的设备认证和数据加密传输问题,到目前为止学者们已经做出了大量研究[3]。提出的协议有:主机标识协议(Host Identity Protocol,HIP)[4],基于轻量级主机交换协议的、用于主机和用户之间的认证协议[5],Smart 协议[6]—基于双线性配对的身份基密钥协商协议。

对于处理能力不足的物联网节点来说,通常使用的 X.509 证书和 RSA 公钥产生的开销太大,于是文献[7]中提出了基于椭圆曲线(Elliptic Curve Cryptography,ECC)算法的隐式证书,使得引入限制型网络的开销减少。该隐式证书可以用于分布式 IoT 的一般认证机制中。

因此,基于 ECQV(Elliptic Curve Qu-Vanstone)自签名隐式证书机制设计了一种双向认证密钥协商协议,该 ECQV 隐式证书的生成基于 ECC 算法,它的证书更小,计算速度更快,可以显著提高认证效率[8]。传统证书中,公钥和数字签名是分开的,而在 ECQV 自签名隐式证书中,数字签名是嵌入到公钥中的,这也是"自签名"的含义,接收方可以从中提取公钥来验证其身份。由于边缘节点和终端用户在相互认证时使用的是隐式证书,所以该协议也是轻量级的,最终实现了这个机制,并且在资源限制的感知节点上进行了性能测试和安全分析。

1　系统模型

图 1 为所提认证密钥协商机制的网络架构,这里的终端用户可以与不同的感知节点通信,来获得特定的数据或服务。WSN 中可能包括不同类型的感知节点,终端用户可以是人,也可以是虚拟实体。

如图 1 所示,双向认证和数据保护一般发生在以下三种通信场景中:

(1)Link A:同一 WSN 内的两个感知节点之间;

(2)Link B:不同 WSNs 内的两个感知节点之间;

(3)Link C:一个终端用户和一个感知节点之间。

在两个网络实体开始相互认证之前,有必要首先对每个通信端进行注册,目的是将在认证阶段使用的加密证书分发给各个通信端,这样才能保证两个实体可以成功完成相互认证。可见,每个末梢节点和终端用户必须在注册阶段就获得加密证书(比如,密码套件和隐式证书),加密证书的来源是可信的第三方,如证书管理中心(Certificate Authority,CA),它是一个资源丰富的服务器。假设 CA 可以识别网络实体身份的合法性,也可以与网络实体通信。如图 1 所示,网络实体首先通过互联网云与 CA 通信;之后,末梢节点和终端用户可以相互认证并建立安全的通信信道。低层通信的安全性要依靠其他安全机制,这里不做赘述。

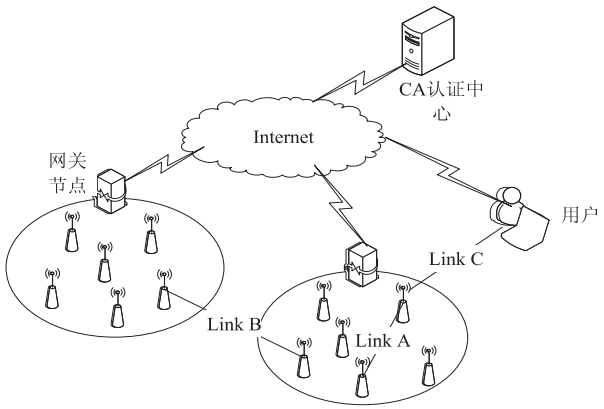

图 1　认证密钥协商机制应用的网络场景

2　双向认证密钥协商协议

协议中的隐式证书机制使用在以下三个实体中:证书中心 CA、证书请求者 U 和证书处理者 V。证书请求者 U 从 CA 获取一个隐式证书,该证书可以证明 U 的身份,该过程称为 ECQV 自签名隐式证书生成机制;并且 V 可以从隐式证书中提取 U 的公钥,该过程称为公钥提取机制[9]。

使用到的符号如表 1 所示。

表 1　认证密钥协商协议中使用的符号及含义

符号	含义
K	原始信息认证的对称密钥
r_U	U 生成的秘密随机整数值,作为临时私钥
R_U	节点 U 发送的证书请求
Cert_U	节点 U 的隐式证书
e	用来保持 Cert_U 的哈希值的证书
s	用于计算证书请求节点的私钥
d_U	节点 U 的私钥
Q_U	节点 U 的公钥
N_U	节点 U 生成的加密随机数
N_{CA}	CA 生成的加密随机数
B_U	节点 U 的公钥重建值
K_{UV}	节点 U 和 V 之间的链路密钥

椭圆曲线的域参数包含 q,a,b,G 和 n。q 代表有限域 F_q;变量 a 和 b 是椭圆曲线 $y^2 = x^3 + ax + b$ 的系数,这里 $4a^3 + 27b^2 \neq 0$;G 是基点发生器[10]。首先由

CA 生成一条椭圆曲线,并选择基点 G,满足它的阶是整数 n。

双向认证机制包含两个阶段:注册阶段和认证阶段。注册阶段,网络实体从可信第三方获取加密证书;认证阶段,使用该加密证书建立两个网络实体之间的安全通信。

2.1 注册阶段

图 2 为协议的流程图,图中的未加框文字代表实体要完成的动作,加框的文字代表使用到的变量和相关公式。图 2(a)为注册阶段的协议流程图,末梢节点(如感知节点)和终端用户从 CA 请求安全材料和证书。只有证书请求者的身份得到确认后,CA 才发行隐式证书[11]。证书请求者(节点 U)可以是感知节点,也可以是终端用户。

注册阶段的信息传递与处理过程如下:

(1)握手的一开始由证书请求者发送一个 Requestor Hello 消息、节点身份(U)和密码套件。

假定密码套件是嵌入到感知节点中的,并且在部署阶段或授予网络接入权利阶段对终端用户是已知的。密码套件包含请求者一端可用的密码选项,比如 EC 参数、MAC 的消息认证密钥(K)、哈希函数(H)和分组加密的 AES 密钥大小。例如,CERT_ECC160_K1_SHA1_AES128 代表 160 bit EC 曲线,K1 是消息认证密钥,使用 SHA1 和 128 bit AES。

(2)CA 使用证书请求者的身份信息来验证其合法性,当验证成功后,CA 从发来的密码套件选项中选择一个,并将 CA Hello 消息连同它的公钥 Q_{CA} 发送给证书请求者,该消息不受保护。

(3)接收到 CA Hello 消息后,证书请求者生成一个证书请求(R_U)和一个随机数(N_U),r_U 作为临时私钥,计算它们的消息认证码(MAC)值并将 Certificate Request 消息一并发送给 CA。随机数和 MAC 值分别用来保证消息的新鲜性和完整性。

(4)CA 首先确认 MAC 值来鉴定请求消息的完整性,然后计算隐式证书($\mathrm{Cert_U}$)和用于计算私钥的整数(s),该过程即 ECQV 自签名隐式证书生成机制。计算过程如下:

根据证书请求者 U 的临时私钥 r_U 计算出临时公钥 $G_U = r_U G$;

计算 CA 自己的临时密钥对(d,Q),其中 d 是临时私钥,Q 是临时公钥,满足 $Q = dG$;

计算公钥重建值 $B_U = Q + G_U$;

构造 U 的证书信息 I_U(比如身份和其他有效性信息);

构造隐式证书 $\mathrm{Cert_U}$,包含 B_U 和 I_U;

计算 $s = ed + d_{CA} \pmod n$,其中 d_{CA} 是 CA 的私钥,$e = \mathrm{Hash}(\mathrm{Cert_U})$。

CA 发送 Certificate 消息和随机数(N_{CA})与 MAC 值,Certificate 消息中包含隐式证书 $\mathrm{Cert_U}$ 和 s。

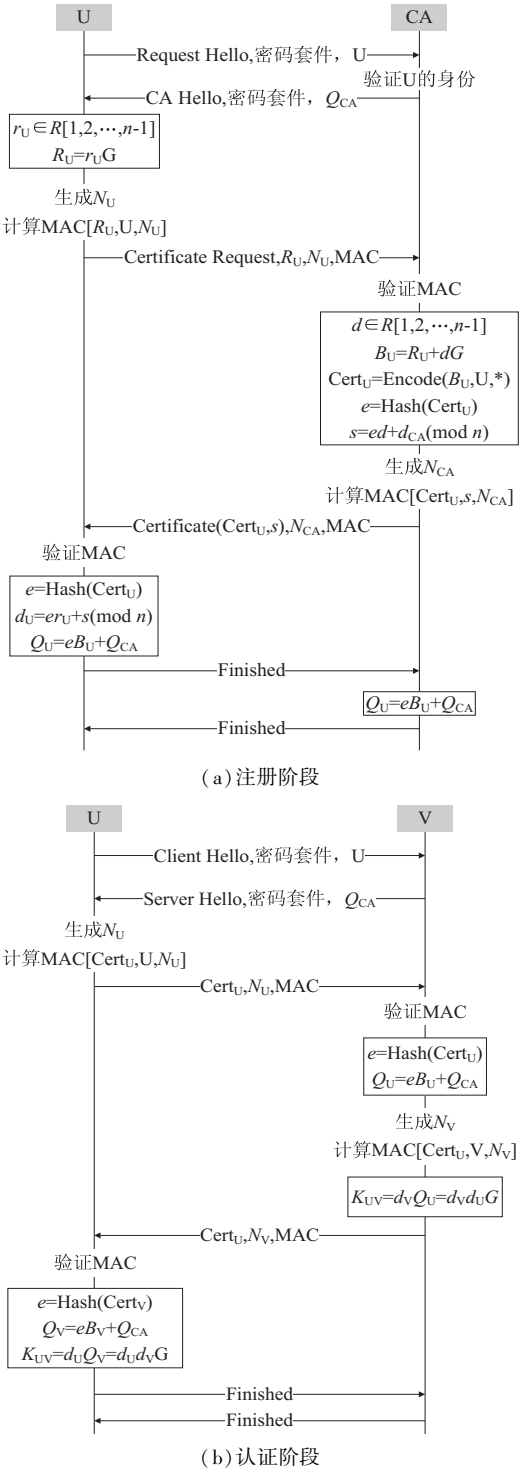

图 2 协议流程图

(5)证书请求者接收到 Certificate 消息后确认 MAC 值,然后计算它自己的私钥(d_U)与公钥(Q_U),即 ECQV 公钥提取机制。计算过程如下:

从 $\mathrm{Cert_U}$ 消息中解析出 B_U 和 I_U,并且确认其有效性;

计算 $e = \mathrm{Hash}(\mathrm{Cert_U})$,并确认 $e \neq 0$;

计算 U 的私钥 $d_U = er_U + s \pmod n$;

计算 U 的公钥 $Q_U = eB_U + Q_{CA}$。

其他节点(比如 V)也可以通过同样的方法从 U 的隐式证书 $Cert_U$ 中计算出 U 的公钥 Q_U。

证书请求者发送 Finished 消息,包含用公钥 Q_U 加密之前握手消息的加密消息摘要。

(6)根据用于计算密钥的 EC 数学算法,CA 可以计算出 Q_U,并用它来加密之前的消息,生成 Finished 消息并发送,注册阶段的握手便完成了。

2.2　认证阶段

在认证阶段,一个感知节点或终端用户作为客户端,另一感知节点作为服务器端,如图 2(b)所示,这里考虑的是客户端节点 U 和服务器端节点 V 之间的认证过程。

认证阶段的信息传递与处理过程如下:

(1)客户端首先向服务器端发送 Client Hello 消息、密码套件选项和身份信息(U),客户端的隐式证书由密码套件组成。

(2)如果服务器端获得的证书与客户端所给的密码套件相匹配,服务器端将选择一个密码套件,并回应 Server Hello 消息和身份消息。否则,服务器端将发送 End 消息和它的密码套件选项来结束此次握手,客户端只能重新获取新的证书,并从头开始握手过程。

(3)接收到 Server Hello 消息后,客户端发送它的证书信息、加密随机数和 MAC 值。

(4)如果 MAC 值验证成功,服务器端用接收到的证书($Cert_U$)和 CA 的公钥(Q_{CA})来计算客户端的公钥(Q_U);用它的私钥 d_V 和客户端的公钥 Q_U 计算双方的共用密钥 $K_{UV} = d_V Q_U$。服务器端发送它的证书 $Cert_V$、随机数 N_V 和 MAC 值。

(5)客户端作相似的处理。

最后交换 Finished 消息,包含用共用密钥 K_{UV} 加密的原握手消息。

在六个握手消息传输完成后,两个节点便可以验证彼此的身份,并建立一个共用的密钥和一条安全通信链路,可以用于保护客户端和服务器端数据交换的安全。

3　实验环境

双向认证密钥协商协议用 C 语言编写,运行在 Contiki[12] 操作系统上;部署在 WiSMote[13] 感知节点上,WiSMote 硬件平台的配置有:MSP430 5-系列微控制器;128/16 kB 的 ROM/RAM;1 个 IEEE 802.15.4 (CC2520)收发器;光照、温度传感器。

利用开源软件 OpenSSL 在 Linux 下创建了一个简单的 CA 认证中心,来为服务器端和客户端颁发数字证书。

在物联网的感知层 WSN 中,源节点到目的节点之间的典型路径是由多跳组成的,该路径上的中间节点充当转发节点,因此,WSN 中的任何无线设备节点都可以同时作为无线访问接入点和路由器。性能评估实验的网络结构图可参见图 1。

4　性能分析和安全性分析

对所提出的认证密钥协商协议的性能和安全性做出分析,并证明该解决方法可以部署在分布式 IoT 应用中的资源限制型设备上。

文献[14]比较了隐式证书与传统证书在相同安全级别时的公钥、证书长度。比如,在安全级别是 192 时,RSA 的证书大小为 15 360 bit 加上身份信息数据,而 ECQV 隐式证书的大小为 385 bit 加上身份信息数据。可见,隐式证书在传输过程中可以减少带宽占用,而且安全级别越高,这种优势越明显,所以更适合传感器网络等资源受限环境。

4.1　内存占用

使用 MSP430 工具链中的 msp430-size 和 msp430-objdump 工具分析 RAM 和 ROM 的消耗情况,如表 2 所示,内存占用值按每个通信节点的两个阶段来分别列出。

表 2　内存占用测量值

阶段	操作	RAM/bytes	ROM/bytes
注册阶段	节点的操作	1 398	11 703
注册阶段	CA 的操作	2 311	16 562
认证阶段	节点的操作	1 585	11 690

由表 2 可见,一个 WiSMote 感知节点在整个认证协议中消耗约 2 983 字节 RAM 和 23 393 字节 ROM,仍然低于 WiSMote 节点提供的 16 kB RAM 和 128 kB ROM。虽然 CA 操作消耗的内存更大,但 CA 是资源丰富的设备,不受资源局限。

4.2　时间与能量消耗

由于传输时间依赖于网络的规模和两个节点之间的距离,所以表 3 只列出了边缘节点或 CA 某些特定操作的执行时间。

能量消耗的计算公式为 $V * I * t$,其中 $V = 3$ V 是 WiSMote 节点上的电压,$I = 1.8$ mA 是电流,t 是操作的执行时间。

由表 3 可知,注册阶段证书请求者消耗的时间是 8 286 ms,CA 消耗 10 893 ms;认证阶段每个节点消耗 8 396 ms。一个 WiSMote 节点在注册阶段和认证阶段消耗的能量分别是 43.71 mJ 和 46.12 mJ。

所以,实验结果表明使用更加优化的 ECC 操作可

以减少时间、能量和内存消耗,所提的机制可以很容易部署在低能量低性能的设备上。而且,在该双向认证协议中,隐式证书作为 160 位 EC 点来使用,因此证书的长度仅为 44 字节。使用优化设计的 EC 曲线可以减小证书长度,未来使用压缩技术也可以减小整个消息的长度。

表 3 特定操作的时间消耗和能量消耗值

阶段	操作	时间消耗 /ms	能量消耗 /mJ
注册阶段	初始化	2 810	14.92
注册阶段	生成 Certificate Request	2 647	13.28
注册阶段	生成 Certificate	5 882	15.75
注册阶段	U 确认证书	2 826	15.37
注册阶段	U 的 Finished 消息	3	0.14
注册阶段	CA 的 Finished 消息	2 201	9.77
认证阶段	初始化	2 619	13.98
认证阶段	计算密钥	5 773	32.04
认证阶段	Finished 消息	4	0.19

4.3 安全性分析

所提端到端认证密钥协商协议基于 ECQV 隐式证书,而该隐式证书使用的是 ECC 算法,这为协议的设计带来了很大的好处:它提供与 RSA 相同的安全性,而且开销更小(比如,160 bit 的 ECC 与 1 024 密钥长度的 RSA 的安全性等同),具有可靠的安全性。

在分布式物联网中很容易遇到 DoS 攻击。在方案的注册阶段,第一个 Hello 消息中包含证书请求者的身份信息,这个身份信息经过 CA 的鉴定。如果非法请求者尝试接入,CA 可以在身份验证的一开始就识别出来,保护网络免受 DoS 攻击。而且,在认证阶段,仅在成功交换 Hello 消息后才交换加密证书,这也可以避免 DoS 攻击。另外,随后传送的消息都包含 MAC,这也可以避免由入侵者和 DoS 攻击导致的非法信息交换,并且 MAC 中的通用密钥 K 可以保证数据完整性,随机数用于保证握手期间的消息新鲜性。

根据以上的性能与安全性分析可以看出,所提的认证密钥协商协议可以很容易地部署在资源限制型设备上,并且具有较高程度的安全保护。因为该协议是基于标准 ECC 操作的,而所有感知节点都支持 ECC 算法,所以不论感知节点的生产商是否一样,都可以部署该协议。

5 结束语

为了解决物联网环境中用户认证和数据传输的不安全性,提出并分析了一种适用于分布式物联网的认证密钥协商协议,可以很容易地部署在资源限制型节点上,且具有较高的安全性。实验结果表明,该认证协议可以部署在 WSNs 中的低性能资源限制型网络设备上,并且可以抵抗 DoS 等攻击。

参考文献:

[1] Gubbi J, Buyya R, Marusic S, et al. Internet of Things (IoT): a vision, architectural elements, and future directions[J]. Future Generation Computer Systems, 2013, 29(7): 1645-1660.

[2] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things[J]. Computer Networks, 2013, 57(10): 2266-2279.

[3] Hu W, Tan H, Corke P, et al. Toward trusted wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2010, 7(1): 2019-2021.

[4] Gurtov A, Komu M, Moskowitz R. Host Identity Protocol (HIP): identifier/locator split for host mobility and multihoming[J]. Internet Protocol Journal, 2009, 12(1): 27-32.

[5] Pellikka J, Faigl Z, Gurtov A. Lightweight host and user authentication protocol for All-IP telecom networks[C]//Proceedings of 3rd IEEE workshop on data security and privacy in wireless networks. [s. l.]: IEEE, 2012.

[6] Smart N P. An identity based authenticated key agreement protocol based on the Weil pariring[J]. Electronics Letters, 2002, 38(13): 630-632.

[7] Kotzanikolaou P, Magkos E. Hybrid key establishment for multiphase self-organized sensor networks[C]//Proceedings of the 6th IEEE international symposium on a world of wireless mobile and multimedia networks. [s. l.]: IEEE, 2005: 581-587.

[8] Porambage P, Kumar P, Schmitt C, et al. Certificate based pairwise key establishment protocol for wireless sensor networks[C]//Proceedings of IEEE 16th international conference on computational science and engineering. [s. l.]: IEEE, 2013: 667-674.

[9] SEC4: Elliptic Curve Qu-Vanstone implicit certificate scheme (ECQV), version 1.0. [EB/OL]. 2013. http://www.secg.org/sec4-1.0.pdf.

[10] Hankerson D, Vanstone S, Menezes A J. Guide to elliptic curve cryptography[M]. [s. l.]: Springer, 2004.

[11] Porambage P, Schmitt C, Kumar P, et al. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications[C]//2014 IEEE wireless communications and networking conference. [s. l.]: IEEE, 2014: 2728-2733.

[12] Dunkels A, Grönvall B, Voigt T. Contiki-a lightweight and flexible operating system for tiny networked sensors[C]// IEEE international conference on local computer networks. [s. l.]: IEEE, 2004: 455-462.

[13] LCIS and Aragosystems. WiSMote sensor node[EB/OL]. 2013. http://wismote.org/lib/exe/detail.php? id=start&media=wismote_small.png.

[14] 顾海华. 隐式认证在移动设备中的应用[J]. 中国集成电路, 2010, 19(11): 54-56.