一种物联网温室环境监控系统的身份认证协议

王志辉

摘要：在一种基于物联网技术设计的温室环境监控系统中，需要实现用户智能APP与物联网节点设备（如传感器、控制器等）之间的实现双向身份认证的安全策略，以保证系统的安全。因此，文章设计了一种使用EC加密算法和云服务器协助的双向认证策略。实验证明该策略可在较低的资源需求情况下，满足用户智能手机APP与物联网节点设备之间，进行双向身份认证的要求。

关键词：物联网安全，双向认证，密钥协商，椭圆曲线，安全策略

一、引言

环境因素对温室农业生成影响较大[[[1]](#endnote-0)]。如茶苗生长温度在为22℃-28℃,湿度为 50%-70%，最佳值为 25℃和 60%[[[2]](#endnote-1)]；黄瓜种植湿度一般保持在 60%~80%，温度在18~30℃为最佳，进行光合作用时温度需要提高 3~5℃，长期温度高于 38℃或低于 15℃均会影响黄瓜发育[[[3]](#endnote-2)]，湿度过高会造成真菌繁殖，影响黄瓜生长，进而影响黄瓜品质和产量[[[4]](#endnote-3)]。

随着互联网技术的飞速发展，物联网技术也应运而生[[[5]](#endnote-4)]。使用物联网技术设计的温室环境监控系统如图1所示，可以实现光照、温度、湿度、二氧化碳等温室内部环境参数的自动化采集，存储、分析、预警和远程干预等功能。

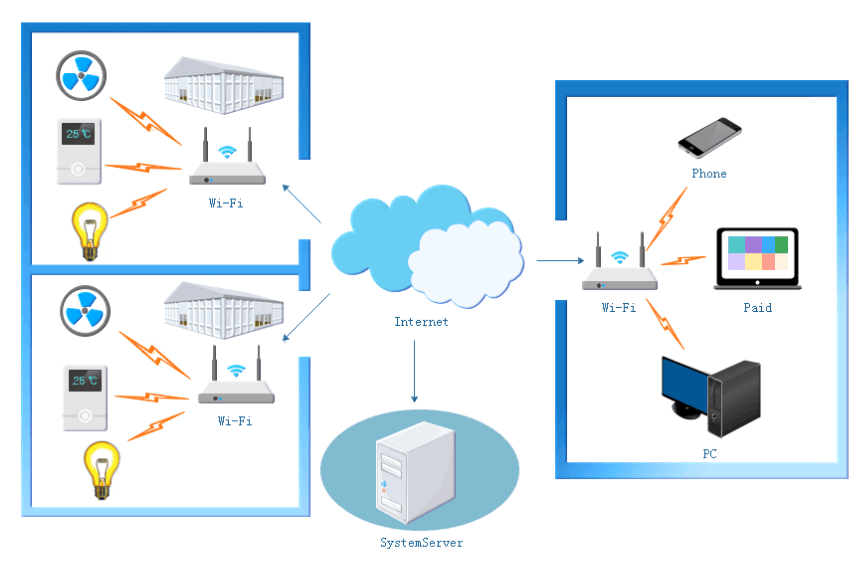


图1物联网温室环境监控系统的架构图

图1中各种环境参数传感器、环境干预控制器等节点设备，构成系统的感知层；系统参数预警服务器和各种用户终端设备构成了系统的应用层；物联网网关（IoT gateway）、云认证服务器（Cloud Authentication Server CAS）、数据存储服务器（Data Server DS）构成了系统的网络层。

物联网网关（IoT gateway）是温室内部网络数据与Internet数据转换的中间件。该设备自动化程度高，对用户透明。其核心业务为通过Internet，向用户App提供实时状态数据上报和干预指令分发服务。网关的核心业务对硬件计算能力的需求较低，使用工作频率为100 MHz 的STM32F412低功耗cpu，完全可以满足需求。

然而，层出不穷的针对物联网的攻击事件，使得物联网系统的安全问题，引起了人们的关注。2015年黑客针对乌克兰的电力系统发起恶意攻击，导致70多万居民家庭停电数小时；2016年的Mirai事件中，攻击者利用网络摄像头等大量的物联网设备向域名服务器发起DDoS攻击，导致大量用户无法使用网络。据Gartner调查，全球近20%的单位和部门，近年来遭受过物联网攻击。

考虑到物联网网关（IoT gateway）进入正常工作状态后，智能手机终端可以直接与网关建立通信链接，并发送数据查询命令和环境干预命令（如风机远程控制，湿帘降温控制等）。物联网网关与用户智能终端之间建立链接之前，需相互验证身份和协商会话密钥，以满足用户控制命令信息的不被冒充，篡改和重放。

2.相关工作

Nicanfar 等[[[6]](#endnote-5)]在 2015 年提出了一个基于椭圆曲线加密的认证协议。尽管他们的方案大大降低了计算复杂度， 但是由于可信任的第三方需要密码表来保存用户信息而易受 到表丢失或被窃取的攻击。之后，Li 等[[[7]](#endnote-6)]提出一个新的密码 协议但同样也被证明易受到窃听，并且由于缺少密钥协商而 易受到模仿攻击。2019年Q.Jiang et al.[[[8]](#endnote-7)]在分析 Das协议[1]的基础上，提出了一种新的在云服务器协助下，实现可穿戴设备认证和密钥协商的安全协议。该协议使用了ECC算法进一步增强了数据的安全性，降低了协议对设备计算资源消耗。2019年Wang et al.[[[9]](#endnote-8)] 提出了一种使用ECC算法和云服务器辅助的物联网网关与用户智能手机进行双向身份认证和密钥协商的协议。

因此，本文针对当前物联网系统感知层设备多数使用对称密钥协议，构建网络安全基础设施。密钥维护工作繁多，运维人员经常接触通信密钥，容易引起密钥泄漏和内部特权人员攻击的情况。以及感知层设备计算、存储和通信资源有限，攻击者容易发起资源耗尽型的DDos攻击的情况。使用EC加密算法设计了一种在系统云认证服务器（Cloud Authentication Server CAS）的辅助下，实现手机APP与系统物联网网关设备之间的双向认证、密钥协商的解决方案。

3.基础理论

3.1.椭圆曲线加密算法

Due to the many benefits of ECC [[[10]](#endnote-9)], it has been used in various environments. One of the most important benefits of ECC is providing the same level of security with a smaller key size compared to other cryptography techniques like RSA. For instance, ECC with 160 and 512 bit keys provide the same level of security as RSA, D-H or ElGamal cryptography with 1024 and 15360 bit keys, respectively. In addition to addressing the resource constraint issue, ECC is also beneficial in enabling an efficient protocol that supports current and future devices with various levels of technology, which is important in emerging SG systems.

Generally, ECC is presented as an Elliptic Curve (EC) nodes/points(x,y) over Zp, 并满足公式（1）。

|  |  |
| --- | --- |
| /var/folders/d3/w9bxxqbs4x16w4c5tgjc67y80000gn/T/com.kingsoft.wpsoffice.mac/wpsoffice.ZdT320wpsoffice | （1） |

公式（1）中p是一个较大的素数，且p值越大安全性越高，计算量也就越大。a，b∈ *Zp*用于确定具体的椭圆曲线，且需要满足公式（2）:

|  |  |
| --- | --- |
| wpsoffice | （2） |

满足上述要求的椭圆曲线Zp(a,b)中，取点G，和整数t 则 K = tG，K也是椭圆曲线Ep(a,b)的点。根据加法法则： tQ  Q  Q  Q...  Q，给定G，t，容易求出 K; 但如果已知K和G，很难求出t。在椭圆曲线加密算法中，G称为基点( base point) ，t称为私钥( private key)，K称为公钥( public key) 。

3.2 攻击者模型

在本文中我们假定攻击者有如下的能力。

1.攻击者可以获取公共传输通道中的一切信息，并且可以修改、重放、伪造任何新的信息去传输给接收者[[[11]](#endnote-10)]。

2.攻击者可以知道这个通信系统中的所有用户的用户名和物联网网关的设备ID。

3.攻击者可以在系统中作为一个合法的用户。

4.攻击者可以与系统中任何一个网关，通过wi-fi建立物理链接。

1. 用户智能手机终端与物联网网关的双向认证

实现物联网网关和用户智能终端设备之间的双向认证和密钥协商，我们需要作出如下约定。（1），物联网网关与云认证服务器CAS之间，已经建立了安全通信信道。（2）所有设备包括云认证服务器CAS，物联网网关、用户终端之间共享一组公共的参数。其中包括一组EC参数E{a,b,p,G,n,h}；一个单项散列函数h()；独立的身份ID和时钟。h()用于将字符信息映射到椭圆曲线上。身份标示IDi用与在系统中唯一标示指定设备，其他设备需要通过ID访问指定的设备。设备时钟用于保证消息的新鲜。

考虑到密钥生成、密钥协商，用户认证，鉴权等操作，需要消耗较多的计算资源和存储资源，我们提出将网关需要进行的上述操作，交由系统云认证服务器完成，以降低网络资源消耗需求的方案。图2描述了用户智能终端在系统云认证服务器辅助下，与指定物联网网关之间，进行双向身份认证和密钥协商的策略。其基本流程如下。

第一步.用户通过智能手机终端app登录系统云服务器，服务器验证用户身份和App的合法性。成功则在用户App与系统云认证服务器之间，使用传统DTLS建立安全通信信道。

第二步.智能手机终端App，随机生成一个数p，通过公式（3）计算出，EC上的点P(x,y)。然后，生成请求接入GWID指定网关的请求信息Requestu-g={Appid,GWID，P}，将Requestu-g通过之前建立的安全信道送给系统认证服务器。

|  |  |
| --- | --- |
| /var/folders/d3/w9bxxqbs4x16w4c5tgjc67y80000gn/T/com.kingsoft.wpsoffice.mac/wpsoffice.qiG320wpsoffice | （3） |

第三步.云服务器接收到Requestu-g后，验证用户访问GWID指定网关的权限。如满足，则选择一个数r，通过公式（4）计算出EC点R。使用公式（5）计算出EC节点形式的会话密钥K。

|  |  |
| --- | --- |
| /var/folders/d3/w9bxxqbs4x16w4c5tgjc67y80000gn/T/com.kingsoft.wpsoffice.mac/wpsoffice.lzM320wpsoffice | （4） |
| /var/folders/d3/w9bxxqbs4x16w4c5tgjc67y80000gn/T/com.kingsoft.wpsoffice.mac/wpsoffice.mHS320wpsoffice | (5) |

第四步.云服务器使用服务器与网关会话密钥，加密{Appid,GWID,TimeStamp,K}，作为用户智能终端指定GWID的临时身份认证证书Au。将点R和证书，返回给用户智能终端App；加密{Appid,GWID,TimeStamp,K, random number}作为证书A’,发送给GWID指定网关。

第五步.网关收到上述证书A’后，解码证书，提出信息，使用公式（6）计算出与用户终端APP通信的对称会话密钥k，等待用户智能终端App接入请求。

|  |  |
| --- | --- |
| /var/folders/d3/w9bxxqbs4x16w4c5tgjc67y80000gn/T/com.kingsoft.wpsoffice.mac/wpsoffice.nKz320wpsoffice | （6） |

第六步.用户终端APP接收到云服务器返回的点R和证书A后，使用公式（7）,计算出EC节点形式的会话密钥K。在通过公式（6），计算出会话密钥k。

|  |  |
| --- | --- |
| /var/folders/d3/w9bxxqbs4x16w4c5tgjc67y80000gn/T/com.kingsoft.wpsoffice.mac/wpsoffice.Rwx320wpsoffice | （7） |

第七步.用户终端APP，使用计算出的密钥k和AES128算法，加密证书A，发送给GWID指定网关。

第八步.网关收到用户终端APP的接入请求后，使用密钥k和AES128算法，解密运算得到证书A，与服务器接收到的证书A'中的信息进行比较。一致则身份验证成功。双方使用密钥k进行后续通信工作。

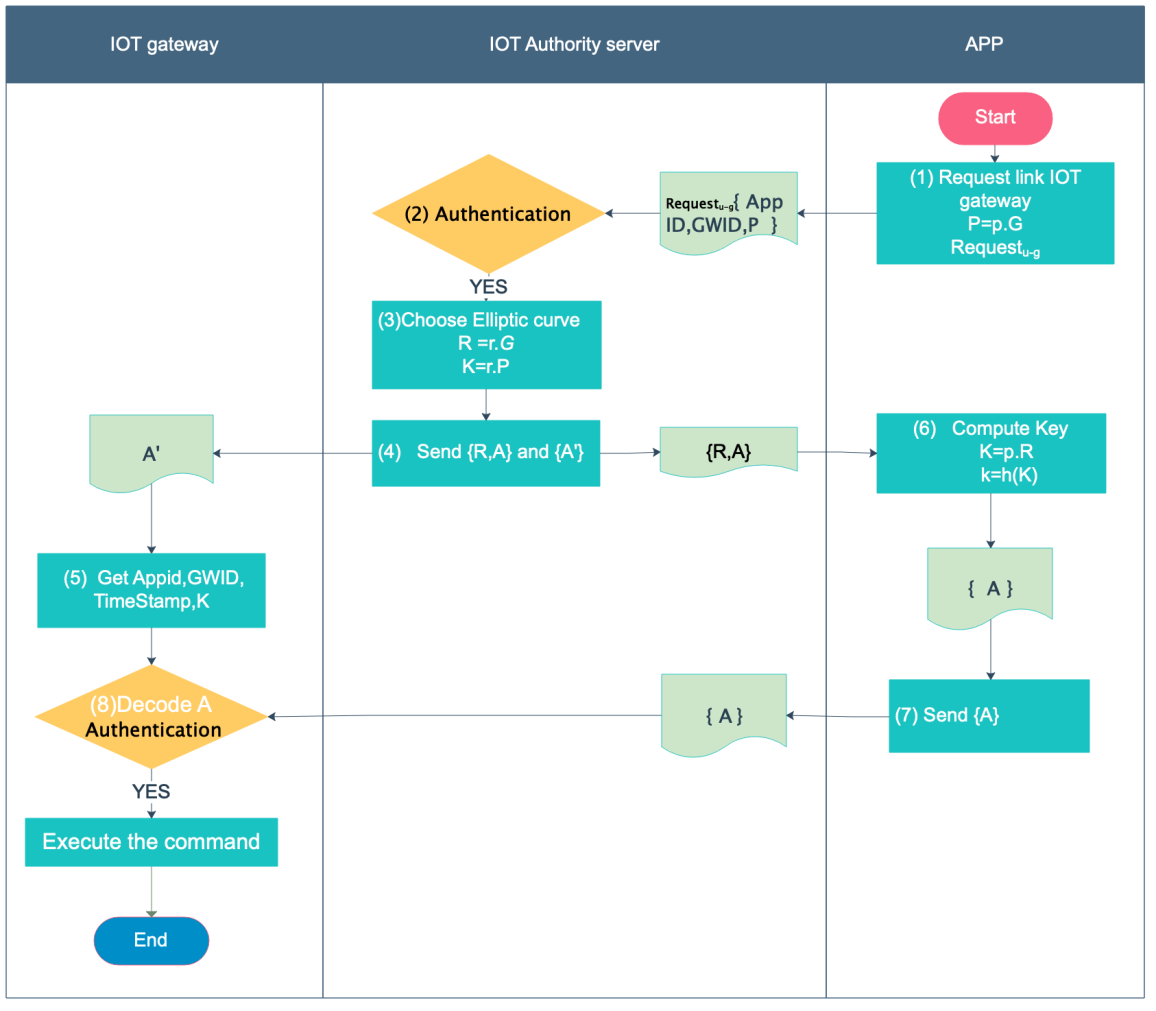


图2云认证服务器协助下网关与用户双向认证的流程

4 系统安全性分析

本节将在 2.3节本文假设的攻击者模型下，对服务器协助下的改进的网关与用户双向认证协议的安全性进行分析。

( 1) 防窃听分析。

通信过程中，服务器与网关之间以及服务器与客户端之间的通信信道，是安全的加密信道。因此，窃听者无法窃听获取，信息的真实内容。客户端与网关之间建立通信信道时，监听者可以获取公钥Kc-g，但无法得到双方的私钥k，即使获取密文C，也无法获取真实信息，因此协议具有防窃听能力。

( 2) 防假冒分析。

系统中通信信息使用存有椭圆曲线 Ep( a,b) 、选定的基点G 和私钥t ，并且M中的双方的身份ID，窃听正无法伪造加密的信息，因此在本系统中，具有防假冒能力。

( 3) 防重传分析。

重传攻击是窃听者在非法获取到网络中的通讯信息后，通过重发先前信息以非法获取信任的攻击 手段。本系统消息中添加了时间戳、有效期和顺序号等信息，使得协议具有防有防重传的能力。

（4）伪装攻击

攻击者如果想要伪装成合法用户与网关进行通信，必须要伪造出合法的认证信息。通过上述的分析知道，只有服务器指定用户具有服务器认证证书，因此协议可以防止伪装攻击。

( 5) 中间人攻击

根据攻击者没有办法伪装成其他用户进行通信，并且攻击者无法伪造出合法的认证信息，所以这个协议可以抵挡住中间人攻击。

**5.实验与结论**

依据图1所示，物联网温室环境监控系统系统架构图，构建了实验测试平台。系统服务器群使用固定IP的10MP光纤专线接入Internet。以Android系统的手机作为客户端平台。以工作频率100 MHz Cortex®-M4内核的STM32F412低功耗cpu，构建物联网网关，实现本文设计的用户认证协议。实验中，根据攻击模型对物联网网关发起计算资源耗尽型DDos攻击，结果表明该方案，具有较高的安全性，占用资源较少，对网关核心业务通信影响较少，网关运行更加稳定。

ACKNOWLEDGMENTS

The work was supported by the Population Health Information in Hebei Province Engineering Research Center。

参考文献

1. [] McSorley R., M. Ozores-Hampton, P.A. Stansly, & J.M. Conner. (1999). Nematode management, soil fertility, and yield in organic vegetable production.Nematropica,29(2), 205. [↑](#endnote-ref-0)
2. [] Nicole Kfoury, Joshua Morimoto, Amanda Kern, Eric R. Scott, & Albert Robbat. (2018). Striking changes in tea metabolites due to elevational effects. Food Chemistry, 264, 334. [↑](#endnote-ref-1)
3. [] C.-F. Zhou, C.-T. Wu, D.-D. Li, X.-W. Zhang, & X.-Z. Ai. (2018). Hydrogen sulfide promotes chilling tolerance of cucumber seedlings by alleviating low-temperature photoinhibition.Plant Physiology Journal, 54(3), 411-420. [↑](#endnote-ref-2)
4. [] JianHua Xu, Sheng Ye, & JiaJun Fu. (2018). Novel sea cucumber-inspired material based on stiff, strong yet tough elastomer with unique self-healing and recyclable functionalities. Journal of Materials Chemistry A, 6. [↑](#endnote-ref-3)
5. [] Kopetz, Hermann. "Internet of things." Real-time systems. Springer US, 2011. 307-323. [↑](#endnote-ref-4)
6. [] Nicanfar H, Leung V C M. Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System[J]. IEEE Transactions on Smart Grid, 2013, 4(1):253-264 [↑](#endnote-ref-5)
7. [] Li D, Aung Z, Williams J R, et al. Efficient and fault-diagnosable authentication architecture for AMI in smart grid[J]. Security & Communication Networks, 2015, 8(4):598-616. [↑](#endnote-ref-6)
8. [] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, “User centric three-factor authentication protocol for cloud-assisted wearable devices,” Int J Commun Syst, vol. 32, no. 6, p. e3900, Apr. 2019. [↑](#endnote-ref-7)
9. [] ZHIHUI WANG, JIANLI ZHAO, BENZHEN GUO, JINGJINGYANG, XIAO ZHANG. Mutual Authentication Protocol for IoT-based Environment Monitoring System[j]Journal of Environmental Protection and Ecology 2019,6(2) [↑](#endnote-ref-8)
10. [] A. H. Koblitz, N. Koblitzb, and A. Menezes, “Elliptic curve cryptog- raphy: The serpentine course of a paradigm shift,” Elsevier J. Number Theory, vol. 131, no. 5, pp. 781–814, May 2011. [↑](#endnote-ref-9)
11. []K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, “[4]An elliptic curve cryptography based lightweight authentication scheme for smart grid communication,” Future Generation Computer Systems, vol. 81, pp. 557–565, Apr. 2018. [↑](#endnote-ref-10)