DOI: 10.19783/j.cnki.pspc.190481

基于 NB-IOT 的孤岛式微电网密钥协商协议研究

康文洋[1,2]，汤鹏志[1,2]，左黎明[1,2]，张 捧[1]

(1.华东交通大学理学院，江西 南昌 330013；2.华东交通大学系统工程与密码学研究所，江西 南昌 330013)

摘要：针对当前日益突出的电力系统网络安全问题，尤其是较容易接近的孤岛式微电网，在基于公钥密码系统的双方密钥协商协议基础上，设计了孤岛式微电网密钥协商协议。在该微电网中，考虑到监测终端的覆盖范围广、深的要求，采用 NB-IOT 技术进行通信。然后对该密钥协商协议进行了安全性分析、关键代码的实现与仿真。在大量的实验数据分析下得出密钥协商三个阶段分别只需要 40 ms、23 ms 和 4 ms 的计算时间，证明了该协议可以高效快速地实现双方的身份认证与密钥的协商，防止数据篡改、重放、伪造等攻击。

关键词：微电网；NB-IOT；密钥协商协议；公钥密码学；数字签名

Research on key agreement protocol for isolated microgrid based on NB-IOT

KANG Wenyang[1,2], TANG Pengzhi[1,2], ZUO Liming[1,2], ZHANG Peng[1]

(1. School of Science, East China Jiaotong University, Nanchang 330013, China; 2. Institute of Systems Engineering and Cryptography, East China Jiaotong University, Nanchang 330013, China)

Abstract: Aiming at the prominent network security problems of electric power system, especially the islanded microgrid, based on key agreement protocol between two parties of public key cryptosystem, a key agreement protocol is designed for islanded microgrid. Considering the requirement of wide and deep monitoring terminals coverage, the NB-IOT is used to communicate. Then the security of the key agreement protocol is analyzed. Besides, the key code is implemented and simulated. Lastly, a large number of experimental data analysis show that the three stages of key agreement only need 40 milliseconds, 23 milliseconds and 4 milliseconds, respectively. Therefore, the protocol can efficiently and quickly realize the identity authentication and key negotiation between two parties to prevent data tampering, replay, forgery attack and so on.

This work is supported by Science and Technology Project of Jiangxi Province Education Department (No. GJJ180323).

Key words: microgrid; NB-IOT; key agreement protocol; public key cryptography; digital signature

0 引言

随着现代电力系统的发展，以及用电负荷、输电容量的快速增长，远距离传输的大电网运营维护成本高、运行难度大、调控能力弱的问题日益突显，很难适应满足用户越来越高的可靠性、灵活性、多样性的供电需求。在 2001 年，美国威斯康星大学的 B. Lasseter 教授提出微电网的概念[1]，微电网(Micro-Grid, MG)是一种小型发配电系统，涉及分布式电源、负荷、储能装置、能量转换装置、监控和保护装置等各个环节，并且能在孤岛式和并网式两种模式下运行[2-3]。微电网各环节之间通过网络链接传递数据，一旦遭受到网络攻击将可能导致整个微电网大面积停电事件，严重威胁到国家安全与社会经济发展。

近几年来，黑客通过互联网攻击电网的事件常有发生，且造成了一定的破坏。2015 年 12 月 23 日，欧洲东部的乌克兰电力部门遭受到“震网病毒”恶意代码攻击，导致大约 70 万家庭断电数小时[4-6]。2016 年 1 月 25 日，以色列电网同样遭受了一次大规模的互联网钓鱼邮件攻击[7-9]。早在 2013 年，文献[10]对现有的网络安全工作进行了概述，并设计了一个用于微电网安全控制系统的网络安全架构，包括工业控制系统(ICS)、特定漏洞分析、威胁模型、保证信息合规性问题以及微电网控制系统的设计标

基金项目：江西省教育厅科技项目(GJJ180323)；江西省学位与研究生教育教学改革研究项目(JXYJG-2018-095)；江西省研究生创新项目(YC2018-S250)；大学生创新创业训练计划项目(201810404003)

准。2015 年文献[11]研究了微电网中的安全漏洞，如侧信道分析，分布式拒绝服务(DDoS)攻击，隐私数据泄露等，并提出了相应的解决方案。2017 年，文献[12]提出了一种 FDIA 检测框架，该框架可以检测直流微电网中可能存在的虚假数据注入攻击，并将攻击检测问题转化为对候选集合变化的识别问题。

在具体实践当中，传统的远程无线自动数据采集终端使用GPRS、LoRa等无线服务技术进行通信，文献[13-15]对 GPRS、LoRa 技术在智能电网数据采集终端中的应用进行了论述和研究。但现阶段由于智能电网设备覆盖面广，建设专用的无线通信网络投入大，GPRS、LoRa 等通信设备生产成本高，使得这些无线通信技术方案都存在一定的局限性。基于窄带物联网(Narrow Band Internet of Things, NB-IoT)的低成本、多连接、速率快、低功耗和深覆盖等特点的新型无线接入技术，设计了本方案的网络系统架构[16-17]。

本文方案针对电网可能出现的网络攻击问题，在文献[18]中提出的基于公钥密码系统[19]的双方密钥协商协议基础上，使用数字签名[20]方案设计了基于 NB-IOT 的孤岛式微电网密钥协商协议，基于该密钥协商协议，可以较好地实现数据防篡改、防重放、防伪造，并且结合 NB-IOT 无线技术的特性，可以实现较广的覆盖范围，从而提升了整个微电网的安全性与稳定性。

1 基于 NB-IOT 的孤岛式微电网架构[21-25]

如图 1 所示，基于 NB-IOT 的孤岛式微电网网络系统架构可以分为设备层、通信层和集中控制层。设备层中的微电网设备主要是各类能源供应与消耗装置，包括分布式电源、负荷、储能装置、能量转换装置等，通过搭载的 NB-IOT 终端与控制层进行通讯，发送采集监测数据和接收控制指令；通信层为 NB-IOT 构建的蜂窝网络，负责 NB-IOT 终端接入的处理与相关数据的转发工作；集中控制层是整合微电网系统的核心，包括控制服务与安全服务两部分。控制层通过通信服务器与通信层进行数据交换之前，首先双方要通过密钥协商协议进行身份认证，只有身份认证成功的设备，才可获得临时会话密钥 DK 。进一步微电网设备通过对称密码算法将采集监测的原始数据加密发送至集中控制层，集中控制层再使用协商的临时会话密钥 DK 解密，并将解密后的数据存入数据服务器。

微电网设备部署具有数量庞大、形式多样、范围广和非移动性等特点，本文方案利用 NB-IOT 物联网技术深度覆盖、低功耗、低成本、海量连接的特性，实现全面感知，全实时，全程精确监测的微电网系统，有效地监控各种设备的运行状态，提升微电网的运维水平和智能化程度。并且由于从设备层到微电网集中控制层传输很多时候需要通过 NB-IOT 无线网络发送，因此各种监测、控制设备的数据采集封包和控制封包可能存在明文泄露和被篡改的风险，本文提出了基于公钥密码学的密钥协商协议数据安全传输协议。

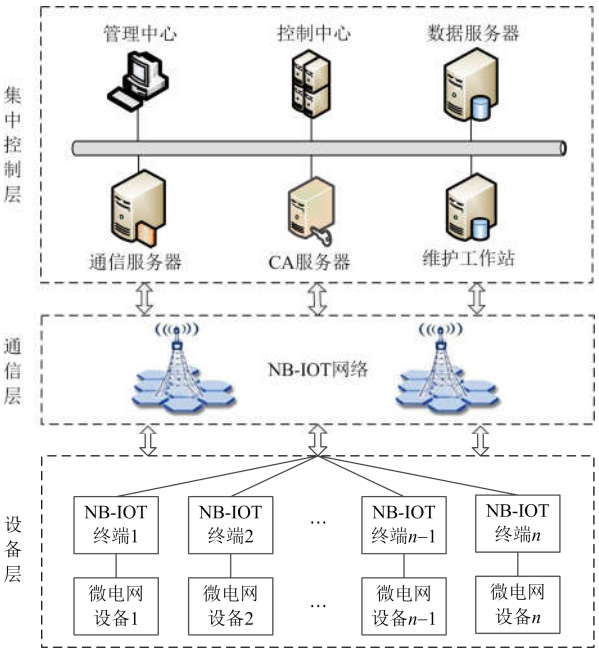

图 1 基于 NB-IOT 的孤岛式微电网网络系统架构图

Fig. 1 NB-IOT-based architecture of isolated microgrid network system diagram

2 基于 NB-IOT 的孤岛式微电网密钥协商协议设计

微电网设备在与集中控制层的通信服务器建立连接之后，数据传输交换之前，应进行双向的身份认证及密钥协商操作，获得临时会话密钥 DK 。只有通过身份认证的设备，才可以使用对称密码算法与控制层进行数据加解密传输，确保通信数据的安全，其中加密密钥与解密密钥为之前获得的临时会话密钥 DK ，本方案在 T-KA 方案[18]的基础上，设计了基于 NB-IOT 的孤岛式微电网密钥协商协议。

T-KA 是一个仅使用数字签名的两方密钥协商协议，如图 2 所示。

在密钥协商之前，CA 服务器分别为微电网设备 U 和通信服务器 A 初始化了私钥、公钥以及证书等系统参数。设 p 是一个大素数， G 是一个 q 阶循环群， g 是 G 的生成元。生成微电网设备 U 的私钥

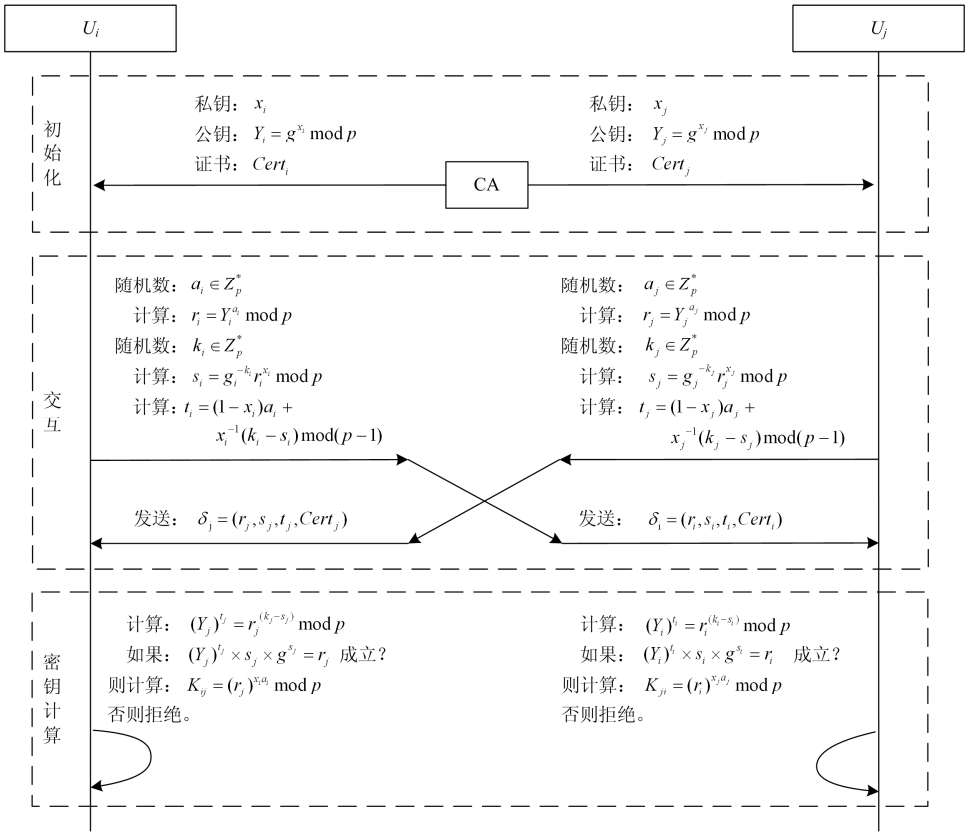

图 2 T-KA 协议描述图

Fig. 2 T-KA protocol description diagram

为 x_1、公钥为 $Y_1 = g^{x_1} \bmod p$ 与证书为 $Cert_1$，通信服务器 A 的私钥为 x_2、公钥为 $Y_2 = g^{x_2} \bmod p$ 与证书为 $Cert_2$，其中 $\gcd(x_i, p-1) = 1$，$i = 1,2$。如图 3 所示，整个密钥协商过程分为三步：密钥协商请求阶段、密钥协商应答阶段以及密钥协商确认阶段，具体协商过程如下所述。

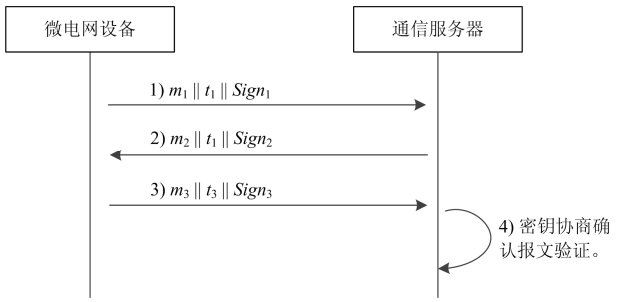

图 3 密钥协商过程图

Fig. 3 Key agreement process diagram

1) 微电网设备 U 生成密钥协商请求报文，并将密钥协商请求报文发送至通信服务器 A。如表 1 所示为密钥协商请求报文数据结构。

具体生成步骤如下所述。

表 1 密钥协商请求报文

Table 1 Key agreement request message

名称	说明
Type	报文类型
Subtype	报文子类型
ID	设备唯一 ID
$Cert_1$	设备自身证书
t_1	时间戳
$Sign_1$	签名

步骤 1：微电网设备 U 选择一个随机数 $a_1 \in Z_p^*$，并使用设备 U 的公钥计算 $r_1 = Y_1^{a_1} \bmod p$；

步骤 2：获取该设备当前时间戳 t_1，对消息 m_1 和当前时间戳 t_1 进行哈希处理(其中 $m_1 = Type \| Subtype \| ID \| Cert_1$)，得到报文哈希值 $h_1 = H(m_1 \|_p^* t_1) \in Z$；

步骤 3：使用设备 U 的私钥计算 $s_1 = g^{-h_1} r_1^{x_1} \bmod p$ 和 $z_1 = (1-x_1)a_1 + x_1^{-1}(h_1 - s_1) \bmod (p-1)$，得到签名 $Sign_1 = (r_1, s_1, z_1)$；

步骤 4：微电网设备 U 通过 NB-IOT 终端发送

$\delta_1 = m_1 \| t_1 \| Sign_1$ 报文至通信服务器 A。

2) 通信服务器 A 接收到 δ_1 后首先进行报文解析和签名验证，然后生成报文结果如表 2 所示的密钥协商应答报文。

表 2 密钥协商应答报文

Table 2 Key agreement response message

名称	说明
Type	报文类型
Subtype	报文子类型
$Cert_2$	服务器自身证书
t_2	时间戳
$Sign_2$	签名

其密钥协商请求报文与应答报文生成的具体步骤如下所述。

步骤 1：通信服务器 A 接收到 $\delta_1 = m_1 \| t_1 \| Sign_1$ 后，首先对该报文进行解析，获取时间戳 t_1 并验证请求报文的新鲜性，验证成功后进入下一步操作，否则拒绝报文；

步骤 2：使用微电网设备 U 的公钥计算 $v_1 = (Y_1)^{z_1} \bmod p$，如果 $v_1 \times s_1 \times g^{s_1} \bmod p = r_1$ 成立，则表明签名验证成功，进入下一步操作，否则拒绝报文；

验证公式如下：

$$v_1 = (Y_1)^{z_1} = (g^{x_1})^{z_1} = g^{(1-x_1)a_1x_1} \times g^{(h_1-s_1)} = r_1^{(1-x_1)} \times g^{(h_1-s_1)} \bmod p$$

$$v_1 \times s_1 \times g^{s_1} = (r_1^{(1-x_1)} \times g^{(h_1-s_1)}) \times (g^{-h_1} \times (r_1)^{x_1}) \times g^{s_1} = r_1$$

步骤 3：通信服务器 A 选择一个随机数 $a_2 \in Z_p^*$，使用服务器 A 的公钥计算 $r_2 = Y_2^{a_2} \bmod p$；

步骤 4：获取服务器当前时间戳 t_2，对消息 m_2 和 t_2 进行哈希处理(其中 $m_2 = Type \| Subtype \| Cert_2$)，得到报文哈希值 $h_2 = H(m_2 \| t_2) \in Z_p^*$；

步骤 5：使用服务器 A 的私钥计算 $s_2 = g^{-h_2} r_2^{x_2} \bmod p$ 和 $z_2 = (1-x_2)a_2 + x_2^{-1}(h_2 - s_2) \bmod (p-1)$，得到签名 $Sign_2 = (r_2, s_2, z_2)$；

步骤 6：服务器 A 进一步计算 $K_{12} = (r_1)^{x_2 a_2} \bmod p$，并得到临时会话密钥 $DK = K_{12} = g^{x_1 x_2 a_1 a_2} \bmod p$；

步骤 7：通信服务器 A 通过 NB-IOT 网络发送 $\delta_2 = m_2 \| t_2 \| Sign_2$ 报文至微电网设备 U。

3) 微电网设备 U 接收到 δ_2 后首先进行报文解析和签名验证，然后生成报文结构如表 3 所示的密钥协商确认报文。

表 3 密钥协商确认报文

Table 3 Key agreement confirmation message

名称	说明
Type	报文类型
Subtype	报文子类型
$Cert_3$	设备自身证书
t_3	时间戳
$Sign_3$	签名

其密钥协商应答报文处理与确认报文生成的具体步骤如下所述。

步骤 1：微电网设备 U 接收到 $\delta_2 = m_2 \| t_2 \| Sign_2$ 后，首先对该应答报文进行解析，获取时间戳 t_2 并验证应答报文的新鲜性，验证成功后进入下一步操作，否则拒绝报文；

步骤 2：使用通信服务器 A 的公钥计算 $v_2 = (Y_2)^{z_2}$，如果 $v_2 \times s_2 \times g^{s_2} \bmod p = r_2$ 成立，则表明签名验证成功，进入下一步操作，否则拒绝报文；

步骤 3：微电网设备 U 进一步计算 $K_{21} = (r_2)^{x_1 a_1} \bmod p$，并得到临时会话密钥 $DK = K_{21} = g^{x_1 x_2 a_1 a_2} \bmod p$；

步骤 4：获取设备 U 当前时间戳 t_3，对消息 m_3、t_3 以及临时会话密钥 K_{21} 进行哈希处理（其中 $m_3 = Type \| Subtype \| Cert_1$），得到报文哈希值 $h_3 = H(m_3 \| t_3 \| K_{21})$，计算签名 $Sign_3 = g^{h_3} \bmod p$；

步骤 5：微电网设备 U 通过 NB-IOT 网络发送 $\delta_2 = m_3 \| t_3 \| Sign_3$ 报文至通信服务器 A。

4) 通信服务器 A 接收到 δ_3 后，获取时间戳 t_3 验证确认报文的新鲜性，验证成功后进入下一步操作，否则拒绝报文；对确认报文解析后的消息 m_3、t_3 以及通信服务器 A 生成的临时会话密钥 K_{12} 进行哈希处理，得到报文哈希值 $h_3' = H(m_3 \| t_3 \| K_{12})$，计算签名 $Sign_3' = g^{h_3'} \bmod p$；比较 $Sign_3'$ 与 $Sign_3$ 是否相等，如果相等，则此时双方已经验证对方身份，并持有临时会话密钥 DK，若不相同，则通信服务器 A 给出协商失败的警告信息，通知微电网设备 U 重新发起密钥协商。

3 安全性分析

1) 抗重放攻击

重放攻击是指一个主动攻击者截获一个报文消息请求，并在之后使用它来假冒一个合法的用户。协议中，在密钥协商请求、应答和确认报文中，使用时间戳 t_1、t_2 以及 t_3 来阻止重放攻击。为了通过认证，攻击者必须将 t_1、t_2、t_3 修改为和接受者本

地时钟相一致的新的时间戳。一旦 t_1、t_2、t_3 已经修改过，$Sign_1$、$Sign_2$ 以及 $Sign_3$ 必定要修改。但是，由于攻击者不知道用户的私钥 x_1、x_2 以及生成的秘密值 a_1、a_2 和临时协商会话密钥 K_{21}，所以攻击者不能够得到有效的 $Sign_1$、$Sign_2$ 以及 $Sign_3$。因此，协议能够抵抗重放攻击。

2) 报文防篡改

篡改攻击是指一个主动攻击者截获一个报文消息请求，并对给请求报文进行篡改以获得合法的请求报文。在密钥协商协议中，在密钥协商请求、应答和确认报文中，使用签名 $Sign_1$、$Sign_2$ 以及 $Sign_3$ 来防止报文篡改攻击。攻击者通过截获报文，知道该报文对应的消息 m_1、m_2、m_3 以及消息对应的哈希值 h_1、h_2、h_3。为了成功篡改报文 δ_1、δ_2 和 δ_3，攻击者必须重新计算得到篡改后消息 m' 的签名 $Sign_1'$、$Sign_2'$ 以及 $Sign_3'$，但是，由于攻击者不知道用户的私钥 x_1、x_2，无法成功计算 s' 和 z'，也就无法获得签名 $Sign_1'$、$Sign_2'$ 以及 $Sign_3'$，导致签名验证失败。因此，协议能够抵抗报文篡改攻击。

4　关键代码与实验仿真

轻量级密码术包 BouncyCastle 是一种 Java 平台开源的轻量级密码术包，该包提供了大量的密码术算法，并且在 JCE1.2.1 进行了实现。本文方案实现的代码通过 C#对 BouncyCastle 进行了封装与调用。操作系统为 Windows Server 2008 64 位，处理器为 Intel(R)Xeon(R)CPU E5-2602 v4 @2.50 GHz，主板为英特尔 82440/1FX 440FX，内存为 4GB(RAM)的实验基准测试环境中，使用 Visual Studio 2012 开发平台，进行了方案实现。

4.1 密钥协商请求阶段仿真

在设备层中，微电网设备终端首先组装密钥协商请求封包，然后计算该封包的哈希值，使用本文方案对封包的哈希值进行签名，最后组成新的数据封包。其具体实现的核心代码如下：

```
//设备 U 选择随机数 a1
BigInteger a1 = new BigInteger(bitLength, new
Random()).NextProbablePrime();
BigInteger r1 = y1.ModPow(a1, p);
String t1 = DateTime.Now.ToString(
"yyyy-MM-dd-HH-mm-ss-fff");
String m1 = "1#1#2019MG00881#"
+ y1.ToString() + "#" + t1;
BigInteger h1 = new BigInteger(HashToNumber(
myhash.TanGetDigest(m1)));
//计算 s1
BigInteger s1 = g.ModPow(h1, p).ModInverse(p)
.Multiply(r1.ModPow(x1, p)).Mod(p);
//计算 temp=(1-x1)^a1
BigInteger temp =
BigInteger.One.Subtract(x1).Multiply(a1);
//计算 temp2=x1^(-1)*(h1-s1)(mod p-1)
BigInteger temp2 = x1.ModInverse(p1).Multiply(
h1.Subtract(s1)).Mod(p1);
//计算 z1=temp2+temp(mpd p-1)
BigInteger z1 = temp2.Add(temp).Mod(p1);
```

如图 4 所示，为使用本文签名方案的密钥协商请求过程，在该实验仿真中，微电网设备 U 的设备唯一 ID 为 2019MG00881，时间戳 t_1 为 2019-04-23-11-22-55-772(格式为：年-月-日-时-分-秒-毫秒)，报文类型为 Type 为 1，报文子类型为 1，设备 U 的证书 $Cert_1$ 为 1179734456286497249569650553077901310127025501624486076913214675942837492943 2，得到请求报文消息 m_1 (使用“#”连接各值)，然后计算得到请求报文哈希值 h_1 与签名 $Sign_1$，整个密钥协商请求过程耗时 40 ms。本实验仿真表明，微电网设备可以高效地生成请求报文封包以及签名处理。

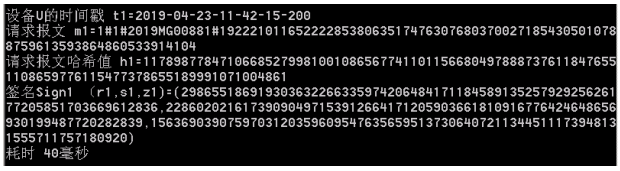

图 4 密钥协商请求阶段签名结果图

Fig. 4 Diagram of key agreement request phase signature result

4.2 密钥协商应答阶段仿真

当集中控制层接收到设备层发送的密钥协商请求报文后，首先根据时间戳验证报文的新鲜性，然后根据等式 $v_1 \times s_1 \times g^{s_1} \bmod p = r_1$ 验证签名是否有效，如果有效，则进一步生成新的密钥协商应答报文封包与会话密钥 K_{12}。其具体实现的核心代码如下：

```
if (IsValidTime(t1))
{
  //计算 v1=y1^z1(mod p)
  BigInteger v1 = y1.ModPow(z1, p);
  //计算 left=v1*s1*g^s1(mod p)
  BigInteger left =
  v1.Multiply(s1).Multiply(g.ModPow(s1, p)).Mod(p);
  //验证等式
```

```
    if (left.CompareTo(r1) == 0)
    {
        Console.Out.Write("密钥协商请求报文签名验证通过:\n");
        BigInteger a2 = new BigInteger(bitLength,
        new Random()).NextProbablePrime();
        r2 = y2.ModPow(a2, p);
        t2 = DateTime.Now.ToString(
        "yyyy-MM-dd-HH-mm-ss-fff");
        String m2 = "1#2#" + y2.ToString() ;
        h2 = new BigInteger(HashToNumber(
        myhash.TanGetDigest(m2 + "#" + t2)));
            //计算 s2
        s2 = g.ModPow(h2, p).ModInverse(p)
        .Multiply(r2.ModPow(x2, p)).Mod(p);
            //计算 temp=(1-x2)^a2
        temp = BigInteger.One.Subtract(x2).Multiply(a2);
        //计算 temp2=x2^(-1)*(h2-s2)(mod p-1)
        temp2 = x2.ModInverse(p1).Multiply(
        h2.Subtract(s2)).Mod(p1);
        //计算 z1=temp2+temp(mpd p-1)
        z2 = temp2.Add(temp).Mod(p1);
        //计算会话密钥 K12=r1^(x2*a2)(mod p)
        K12 = r1.ModPow(x2.Multiply(a2), p);
    }
}
```

如图 5 所示，为通信服务器 A 根据本文签名方案的密钥协商应答过程，在该实验仿真中，服务器 A 成功验证了密钥协商请求报文的有效性，并根据生成的时间戳 t_2 为 2019-04-23-11-42-15-249(格式为：年-月-日-时-分-秒-毫秒)，报文类型为 Type 为 1，报文子类型为 2，服务器 A 的证书 $Cert_2$ 为 3339778740052878643021347984344985474205577379021604631953235866851228814180 9，得到应答报文消息 m_2(使用“#”连接各值)，然后计算得到应答报文哈希值 h_2 与签名 $Sign_2$，最后得到服务器 A 对设备 U 的会话密钥 K_{12} 为 2992964003629790542783219997598278325010363952485933180331549781482087377 56，整个密钥协商应答过程耗时 23 ms。本实验仿真表明，服务器 A 可以高效对设备层发送来的报文进行新鲜性验证和签名验证，同时快速地生成应答报文封包。

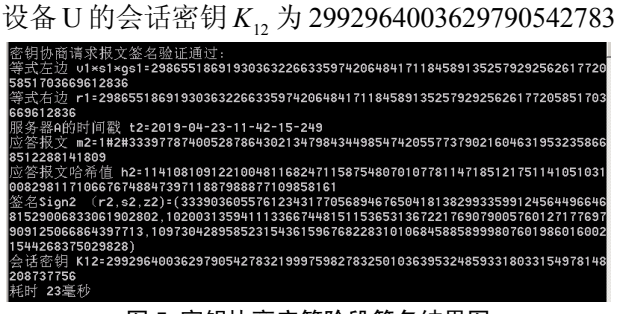

图 5 密钥协商应答阶段签名结果图

Fig. 5 Diagram of key agreement response phase signature result

4.3 密钥协商确认阶段仿真

当设备层接收到集中控制层发送的密钥协商应答报文后，首先根据时间戳验证报文的新鲜性，然后根据等式 $v_2 \times s_2 \times g^{s_2} \bmod p = r_2$ 验证签名是否有效，如果有效，则进一步计算得到会话密钥 K_{21}。其具体实现的核心代码如下：

```
    if (IsValidTime(t2))
    {
        //计算 v2=y2^z2(mod p)
      BigInteger v2 = y2.ModPow(z2, p);
        //计算 left=v2*s2*g^s2(mod p)
        BigInteger left =
        v2.Multiply(s2).Multiply(g.ModPow(s2,p)).Mod(p);
        //验证等式
        if (left.CompareTo(r2) == 0)
        {
            Console.Out.Write("密钥协商应答报文签名验证通过:\n");
          //计算会话密钥 K21=r2^(x1*a1)(mod p)
            K21 = r2.ModPow(x1.Multiply(a1), p);
        }
    }
```

如图 6 所示，为设备 U 根据本文签名方案的密钥协商确认过程，在该实验仿真中，设备 U 成功验证了密钥协商应答报文的有效性，并得到设备 U 对服务器 A 的会话密钥 K_{21} 为 2992964003629790542783219997598278325010363952485933180331549781482087377 56，整个密钥协商确认过程耗时 4 毫秒。本实验仿真表明，设备 U 可以高效对集中控制层发送来的报文进行新鲜性验证和签名验证，同时快速地生成会话密钥。

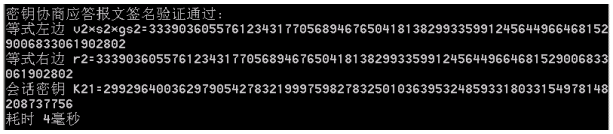

图 6 密钥协商确认阶段签名结果图

Fig. 6 Diagram of key agreement confirmation phase signature result

5 结论

本文提出了一个孤岛式微电网密钥协商协议，该协议分别对密钥协商请求阶段、密钥协商应答阶

段以及密钥协商确认阶段三部分进行了设计，并对该协议进行了安全性分析，发现其可以为传输的数据提供机密性和认证性，能够抵抗消息重放、伪造和篡改攻击。然后结合 NB-IOT 无线通信技术深覆盖、低功耗、海量连接的特点，设计了基于 NB-IOT 的孤岛式微电网系统。最后，对提出的密钥协商协议进行了关键代码实现与仿真，通过大量的实验数据分析得出密钥协商三个阶段分别只需要 40 ms、23 ms 和 4 ms 的计算时间，证明了该协议可以高效、快速地实现双方的身份认证与密钥的协商。在下一步的工作中，将研究如何实现监测数据的高效压缩与加密，从而进一步提高整个微电网数据传输的安全性。

参考文献

[1] LASSETER R H. Microgrids: distributed power generation[C] // Proceedings of the 2001 IEEE Power Engineering Society Winter Meeting, IEEE, January 28-February 1, 2001, Columbus, OH, USA: 146-149.

[2] 丁明, 程清, 李林, 等. 一种基于嵌入式系统的园区微电网中央控制器设计[J]. 电力系统保护与控制, 2019, 47(6): 158-165.
DING Ming, CHENG Qing, LI Lin, et al. A design of central controller of microgrid in the park based on embedded system[J]. Power System Protection and Control, 2019, 47(6): 158-165.

[3] 杨新法, 苏剑, 吕志鹏, 等. 微电网技术综述[J]. 中国电机工程学报, 2014, 34(1): 57-70.
YANG Xinfa, SU Jian, LÜ Zhipeng, et al. Overview on microgrid technology[J]. Proceedings of the CSEE, 2014, 34 (1): 57-70.

[4] 王力军, 周凯, 吴迪, 等. 基于风险传递网络的智能变电站二次系统风险评估[J]. 电力系统保护与控制, 2018, 46(6): 97-105.
WANG Lijun, ZHOU Kai, WU Di, et al. Risk assessment for smart substation secondary system using risk transfer network model[J]. Power System Protection and Control, 2018, 46(6): 97-105.

[5] 刘念, 余星火, 张建华. 网络协同攻击: 乌克兰停电事件的推演与启示[J]. 电力系统自动化, 2016, 40(6): 144-147.
LIU Nian, YU Xinghuo, ZHANG Jianhua. Coordinated cyber-attacks: inference and thinking of incidenton Ukrainian power grid[J]. Automation of Electric Power Systems, 2016, 40(6): 144-147.

[6] LIANG G, WELLER S R, ZHAO J, et al. The 2015 ukraine blackout: implications for false data injection attacks[J]. IEEE Transactions on Power Systems, 2016, 32(4): 3317-3318.

[7] 李中伟, 佟为明, 金显吉. 智能电网信息安全防御体系与信息安全测试系统构建乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化, 2016, 40(8):147-151.
LI Zhongwei, TONG Weiming, JIN Xianji. Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel[J]. Automation of Electric Power Systems, 2016, 40(8): 147-151.

[8] 杨飞生, 汪璟, 潘泉, 等. 网络攻击下信息物理融合电力系统的弹性事件触发控制[J]. 自动化学报, 2019, 45(1): 110-119.
YANG Feisheng, WANG Jing, PAN Quan, et al. Resilient event-triggered control of grid cyber-physical systems against cyber attack[J]. Acta Automatica Sinica, 2019, 45(1): 110-119.

[9] 汤奕, 陈倩, 李梦雅, 等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化, 2016, 40(17): 59-69.
TANG Yi, CHEN Qian, LI Mengya, et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of Electric Power Systems, 2016, 40(17): 59-69.

[10] VEITCH C K, HENRY J M, RICHARDSON B T, et al. Microgrid cyber security reference architecture[J]. Sandia National Laboratories: Albuquerque, NM, USA, 2013.

[11] ZHONG X, YU L, BROOKS R, et al. Cyber security in smart DC microgrid operations[C] // 2015 IEEE First International Conference on DC Microgrids (ICDCM), IEEE, June 7-10, 2015, Atlanta, GA, USA: 86-91.

[12] BEG O A, JOHNSON T T, DAVOUDI A. Detection of false-data injection attacks in cyber-physical DC microgrids[J]. IEEE Transactions on Industrial Informatics, 2017, 13(5): 2693-2703.

[13] 匡洪海, 张曙云, 曾丽琼, 等. 基于 GPRS 和 GPS 的农村智能配电网远程监控系统设计[J]. 电工电能新技术, 2017, 36(4): 83-88.
KUANG Honghai, ZHANG Shuyun, ZENG Liqiong, et al. Design of rural intelligent distribution network remote monitoring system based on GPRS and GPS[J]. Advanced Technology of Electrical Engineering and Energy, 2017, 36(4): 83-88.

[14] LI Y, YAN X, ZENG L, et al. Research on water meter reading system based on LoRa communication[C] // 2017 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC), IEEE, July 23-26, 2017, Singapore,

Singapore: 248-251.

[15] 陈鹏飞, 邓玮璋. 基于 Zigbee 通信网络的低压微电网分布式功率控制[J]. 电力系统保护与控制, 2018, 46(7): 115-122.
CHEN Pengfei, DENG Weiye. Distributed power control for low voltage microgrid based on zigbee communication network[J]. Power System Protection and Control, 2018, 46(7): 115-122.

[16] WANG Y P E , LIN X , ADHIKARY A, et al. A primer on 3GPP narrowband internet of things[J]. IEEE Communications Magazine, 2017, 55(3): 117-123.

[17] MANGALVEDHE N, RATASUK R, GHOSH A. NB-IoT deployment study for low power wide area cellular IoT[C] // 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, September 4-8, 2016, Valencia, Spain: 1-6.

[18] ZHANG H, YUAN Z, WEN Q. A digital signature schemes without using one-way hash and message redundancy and its application on key agreement[C] // 2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007), IEEE, September 18-21, 2007, Liaoning, China: 873-878.

[19] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[20] 汤鹏志, 李彪. Schnorr 数字签名的零知识证明[J]. 微电子学与计算机, 2012, 29(6): 177-179.
TANG Pengzhi, LI Biao. Zero-knowledge proof scheme of schnorr digital signature[J]. Microelectronics & Computer, 2012, 29(6): 177-179.

[21] LI Y, CHENG X, CAO Y, et al. Smart choice for the smart grid: Narrowband Internet of Things (NB-IoT)[J]. IEEE Internet of Things Journal, 2018, 5(3): 1505-1515.

[22] KUMBHAR F H. NB-IoT pervasive communications for renewable energy source monitoring[J]. International Journal of Advanced Computer Science and Applications, 2018, 9(12): 535-541.

[23] BONNEFOI R, MOY C, PALICOT J. Framework for hierarchical and distributed smart grid management[C] // 2017 XXXIInd General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS), IEEE, August 19-26, 2017, Montreal, QC, Canada: 1-4.

[24] GOUDOS S K, DERUYCK M, PLETS D, et al. A novel design approach for 5G massive MIMO and NB-IoT green networks using a hybrid jaya-differential evolution algorithm[J]. IEEE Access, 2019, 7: 105687-105700.

[25] PERSIA S, REA L. Next generation M2M cellular networks: LTE-MTC and NB-IoT capacity analysis for smart grids applications[C] // 2016 AEIT International Annual Conference (AEIT), IEEE, October 5-7, 2016, Capri, Italy: 1-6.

收稿日期：2019-03-31； 修回日期：2019-08-25

作者简介：

康文洋(1993—)，男，硕士研究生，研究方向为信息安全；E-mail: 1981664245@qq.com

汤鹏志(1961—)，男，通信作者，硕士，教授，主要研究方向为信息安全；E-mail: nctpz@126.com

左黎明(1981—)，男，硕士，副教授，研究方向为信息安全，非线性系统。E-mail: limingzuo@126.com

(编辑 姜新丽)