基于PUF的低开销物联网安全通信方案

李森森,黄一才,郁 滨,鲍博武
(信息工程大学,河南郑州 450001)

摘 要: 将物理不可克隆函数(Physical Unclonable Function,PUF)与椭圆曲线上的无证书公钥密码体制相结合,提出一种面向物联网的安全通信方案,在节点设备不存储任何秘密参数的情况下,实现设备间消息的安全传递.方案无需使用高计算复杂度的双线性对运算,并提供了消息认证机制.安全性分析表明,该方案不仅能够抵抗窃听、篡改、重放等传统攻击,而且可以有效防范节点设备可能遭到的复制攻击.对比结果显示,相较于同类方案,该方案明显降低了设备的资源开销.

关键词: 物联网;物理不可克隆函数;椭圆曲线密码;安全通信;消息认证
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2019)04-0812-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.04.007

A PUF-Based Low Cost Secure Communication Scheme for IoT

LI Sen-sen,HUANG Yi-cai,YU Bin,BAO Bo-wu
(*Information Engineering University*,*Zhengzhou*,*Henan* 450001,*China*)

Abstract: By combining the Physical Unclonable Function (PUF) with the certificateless public key cryptosystem on the elliptic curve,a secure communication scheme for IoT is proposed. The secure transmission of messages is realized on the condition of node devices not storing any secret parameters. The proposed scheme eliminates the need for bilinear pairing whose computing complexity is high and provides a message authentication mechanism. Security analysis demonstrates that the scheme can not only resist the traditional attacks such as eavesdropping,tampering and replay,but also protect the node device from replication attacks. Compared with related schemes,the proposed scheme obviously decreases the resource overhead of devices.

Key words: Internet of Things;Physical Unclonable Function (PUF);elliptic curve cryptosystem;secure communication;message authentication

1 引言

物联网将网络通信的实体由人与人扩展至人与物、物与物,是“智慧城市”发展战略的重要支撑,目前已被用于医疗监护、智能交通、环境监测等众多领域[1].随着其应用范围的拓展,物联网的安全问题越来越受到重视.

基于对称密码体制的方案[2-6]和基于公钥密码体制的方案[7-11]是实现物联网安全通信的基本方式.相较于公钥体制,对称密码体制具有密钥规模小、算法易实现等优势,但该类方案不能实现消息签名,无法追踪消息源.文献[7]基于RSA公钥算法提出一种物联网设备认证方案,但方案涉及X.509公钥证书的管理问题且RSA算法所需密钥量较大.针对该问题,He等[8]利用椭圆曲线密码实现无线体域网中的设备认证,该方案将设备身份标识作为其公钥,无需使用证书,但双线性对运算的使用增加了方案的计算开销.文献[9,10]将公钥签名用于资源受限设备的安全通信,无需双线性对运算,具有实现效率高、计算复杂度小等特点.

然而,基于传统密码体制的方案需要将敏感的秘密参数保存于设备存储器.由于物联网中节点设备通常资源受限,难以实现自我保护,攻击者可通过物理手段捕获开放环境中的节点设备,从其存储介质中提取秘密参数并复制恶意设备[11].因此,要将传统方案用于军事、金融等领域,必须在设备中增加安全防护机制,但该方式实现成本较高[11],并不适用于需要大量部署的

收稿日期:2018-02-08;修回日期:2018-08-23;责任编辑:李勇锋
基金项目:国防信息保障技术重点实验室开放基金(No. KJ-15-104)

节点设备.

PUF[12]是建立在设备特有物理特征基础上的一种特殊映射关系,具有不可预测、不可克隆、轻量级等性质[13]. 文献[14]提出一种基于 PUF 的物联网安全传输协议,可有效抵抗复制攻击,但该方案未实现节点设备对服务器的身份认证,不能防止恶意设备伪造服务器的身份,并且方案使用了复杂度高的双线性对运算,具有较高的计算开销.

综上所述,本文将 PUF 与椭圆曲线上的无证书公钥密码体制相结合,提出一种基于 PUF 的物联网安全通信方案. 该方案能够以较小的通信、计算和存储开销实现设备间消息的安全、可信传递. 由于节点设备不需要存储任何秘密参数,方案在抵抗链路安全威胁的同时,提供了对复制攻击的防范,可以满足物联网设备的安全需求.

2　PUF 简介

PUF 由 Pappu 等人提出[12],主要利用设备的随机性物理特征,建立起输入挑战 c 与输出响应 r 之间特殊的映射关系. 不可克隆性和不可预测性是 PUF 的最基本属性,其具体含义如下.

①不可克隆性[13]:对于给定的 PUF,按照相同的电路结构,构造一个 PUF′,使得对任意输入参数 c 都有 $PUF'(c)=PUF(c)$ 是不可行的.

②不可预测性[13]:给定一个输入/输出对集合 $L=\{(c_i,PUF(c_i))\mid i=1,2,\cdots,l\}$,以不可忽略的概率预测 $PUF(c_x)$ 是困难的,其中,c_x 为随机的输入参数且 $(c_x,PUF(c_x))\notin L$.

基于仲裁器的 PUF[15]和基于环形振荡器的 PUF[13]是常用的 PUF 实现方式. 前者结构简单,但要求两条传输路径完美对称,实现难度较大;后者对电路对称性要求不高,更易实现. 为便于实验环境搭建,本文重点研究基于环形振荡器的 PUF.

基于环形振荡器的 PUF 通过比较环形振荡电路(RO)产生的时钟信号的频率差异来实现,其结构如图 1 所示. 每个环形振荡电路由奇数个反相元件构成,可以产生高、低电平交替的时钟信号. 由于材料和工艺存在差异,信号经过每个反相元件所需的时延不同,因而不同环形振荡电路产生的时钟频率不同.

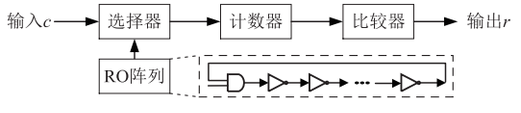


图1　RO-PUF结构

PUF 良好的性质和实现成本低的优势,使其在设备认证、密钥生成等领域有着广泛的应用前景. 利用 PUF 可以有效提取设备的底层物理特征,将其与传统密码体制相结合设计物联网安全方案,能够有效提高物联网通信的安全性.

3　方案设计

本文方案分为参数选取、设备注册、密钥预分配和消息安全传递四个过程. 其中,参数选取和设备注册过程只需执行一次,密钥预分配和消息安全传递过程在节点设备每次通信时执行.

3.1　参数选取

服务器选择椭圆曲线 $e:y^2=x^3+ax+b\bmod p$,并从 e 上选取阶为 q、生成元为 P 的群 G. 然后随机选择私钥 $s\in Z_q^*$,计算相应公钥 $P_{pub}=sP$,并选择四个哈希函数:

$$H_0:\{0,1\}^*\rightarrow\{0,1\}^n,$$

$$H_1:\{0,1\}^*\times G\rightarrow Z_q^*,$$

$$H_2:\{0,1\}^*\times G\times G\rightarrow Z_q^*,$$

$$H_3:\{0,1\}^*\times G\times G\times G\rightarrow Z_q^*.$$

最后,服务器公布基本参数 $Paras=\{e,a,b,p,q,P,P_{pub},H_0,H_1,H_2,H_3\}$.

3.2　设备注册

设备注册过程用于提取节点设备的 PUF 参数,该过程在安全环境下进行. 对于节点设备 $Node_i$,服务器 $Server$ 随机选取挑战信号 c_i,利用 $Node_i$ 的 PUF 得到相应的响应信号 $r_i=PUF_i(c_i)$,并存储三元组 (id_i,c_i,r_i). 初始化过程完成后,$Node_i$ 销毁其 PUF 外部访问接口,即芯片外只能得到协议交互数据,不能直接获得 PUF 的挑战-响应对.

3.3　密钥预分配

密钥预分配过程如图 2 所示,可分为如下 3 步.

(1)基于 PUF 的身份认证

$Node_i$ 选择随机数 $n_1\in Z_q^*$,向 $Server$ 发送请求 $\{id_i,id_j,n_1\}$;$Server$ 向 $Node_j$ 发送 $\{id_i\}$,表明 $Node_i$ 要与其通信;$Node_j$ 回复随机数 $n_2\in Z_q^*$;$Server$ 在数据库中查找 PUF 参数 (id_i,c_i,r_i) 和 (id_j,c_j,r_j),随机选取 $n_3,n_4\in Z_q^*$,计算 $hash_1=H_0(r_i,n_1,n_3,id_i,id_j)$、$hash_2=H_0(r_j,n_2,n_4,id_j,id_i)$,向 $Node_i$ 回复 $\{c_i,n_3,hash_1\}$,并向 $Node_j$ 回复 $\{c_j,n_4,hash_2\}$.

$Node_i$ 收到回复后,利用其 PUF 得到响应信号 $r_i=PUF_i(c_i)$,并验证 $hash_1$ 的正确性. 若正确,则 $Node_i$ 实现对 $Server$ 的身份认证;反之,认证失败. 认证成功后,$Node_i$ 随机选取 $x_i,c_i'\in Z_q^*$,将 x_i 作为秘密值,计算公开参数 $X_i=x_iP$. 利用 PUF 得到 $r_i'=PUF_i(c_i')$,计算 $hash_3=H_1(c_i',r_i',r_i,n_3,X_i)$. 然后,向 $Server$ 回复 $\{X_i,r_i\oplus r_i',c_i',hash_3\}$. $Node_j$ 收到 $Server$ 发来的消息后按同样过程处理,并向 $Server$ 回复 $\{X_j,r_j\oplus r_j',c_j',hash_4\}$.

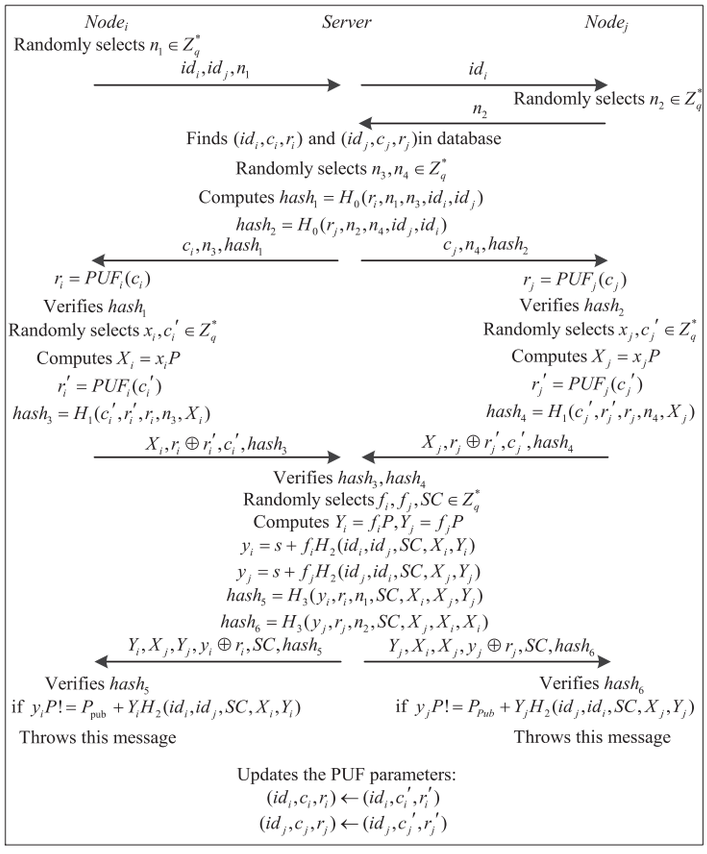


图2 密钥预分配

Server 收到消息后，计算r_i'和r_j'，并验证 $hash_3$ 和 $hash_4$ 的正确性. 若正确，则 *Server* 实现对 $Node_i$ 和 $Node_j$ 的身份认证；反之，认证失败.

(2)公/私钥参数分配

Server 选取随机数 *SC* 作为 $Node_i$ 和 $Node_j$ 的同步序列. 然后，选择随机参数 $f_i \in Z_q^*$，计算 $Node_i$ 的部分公钥 $Y_i = f_i P$ 和部分私钥 $y_i = s + f_i H_2(id_i, id_j, SC, X_i, Y_i)$. 按同样过程可以计算出 $Node_j$ 的部分公/私钥对 (Y_j, y_j).

Server 计算 $hash_5 = H_1(y_i, r_i, n_1, SC, X_i, X_j, Y_j)$ 和 $hash_6 = H_1(y_j, r_j, n_2, SC, X_j, X_i, Y_i)$，分别向 $Node_i$ 和 $Node_j$ 发送 $\{Y_i, X_j, Y_j, y_i \oplus r_i, SC, hash_5\}$ 和 $\{Y_j, X_i, Y_i, y_j \oplus r_j, SC, hash_6\}$.

$Node_i$ 收到后，通过 $hash_5$ 验证消息的完整性，并通过等式 $y_i P! = P_{\text{Pub}} + Y_i H_2(id_i, id_j, SC, X_i, Y_i)$ 验证部分公/私钥对 (Y_i, y_i) 的合法性. 若 $hash_5$ 正确且 (Y_i, y_i) 合法，则 $Node_i$ 的完整公/私钥对为 $< PK_i = (X_i, Y_i), SK_i = (x_i, y_i) >$. $Node_j$ 收到消息后，按同样过程验证消息完整性和 (Y_j, y_j) 的合法性. 若 $hash_6$ 正确且 (Y_j, y_j) 合法，则 $Node_j$ 的完整公/私钥对为 $< PK_j = (X_j, Y_j), SK_j = (x_j, y_j) >$.

(3)PUF 参数更新

Server 将数据库中 $Node_i$ 的 PUF 参数 (id_i, c_i, r_i) 替换为 (id_i, c_i', r_i')，将 $Node_j$ 的 PUF 参数 (id_j, c_j, r_j) 替换为 (id_j, c_j', r_j').

3.4 消息安全传递

密钥预分配过程完成后，$Node_i$ 可与 $Node_j$ 进行安全通信，该过程如图 3 所示.

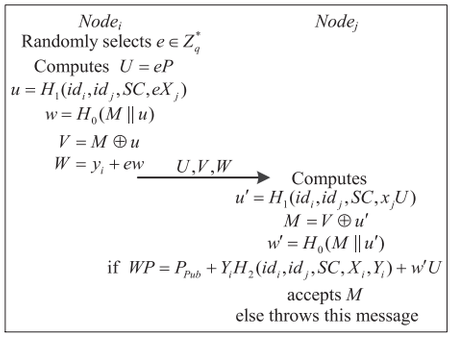


图3 消息安全传递

$Node_i$ 产生要传递的明文消息 M，并选取秘密参数 $e \in Z_q^*$，计算 $U = eP$、$u = H_1(id_i, id_j, SC, eX_j)$、$w = H_0(M \| u)$、$V = M \oplus u$ 和 $W = y_i + ew$. 然后，向 $Node_j$ 发送消息 $\{U, V, W\}$.

$Node_j$ 收到后，计算 $u' = H_1(id_i, id_j, SC, x_j U)$、$M = V$

$\oplus u'$ 和 $w'=H_0(M\|u')$. 由 $x_jU=x_jeP=eX_j$ 可知,计算得到的 u' 在合法状态下应等于 u. $Node_j$ 通过验证 $WP=P_{Pub}+Y_iH_2(id_i,id_j,SC,X_i,Y_i)+w'U$ 是否成立来判断消息 M 的合法性. 若等式成立,则 $Node_j$ 接受消息 M;反之,$Node_j$ 丢弃该消息.

4　安全性分析

方案的安全性主要基于 PUF 的不可克隆性和不可预测性以及椭圆曲线上的 CDH 假设. 基于上述条件,可以得到本文方案具有以下安全性结论.

定理 1　密钥预分配过程能够实现交互设备间的双向身份认证.

证明　密钥参数分配过程利用 PUF 参数实现服务器 *Server* 与节点设备 *Node* 间的双向认证,该过程 *Node* 与 *Server* 的双向认证可简化描述为如下的"三次握手"过程:

①$Node\rightarrow Server:\{n\}$;

②$Server\rightarrow Node:\{c,n',H_0(r,n,n')\}$;

③$Node\rightarrow Server:\{H_0(r,n')\}$.

由 PUF 的不可克隆性和不可预测性可知,挑战信号 c 对应的 PUF 响应 r 具有机密性,即攻击者无法得到 r. 因而,消息②和消息③中的哈希值只能由合法设备计算. 又由于方案中引入随机数 n 和 n' 来保证消息的新鲜性,可抵抗重放攻击. 因此,密钥参数分配过程能够实现设备间的双向认证.

定理 2　通信过程传递的消息具有完善机密性.

证明　节点设备通信时,攻击者能够从链路中得到的参数为 $\{U,V,W\}$. 由 $V=M\oplus u$ 可知,要得到消息明文 M,攻击者必须求出参数 u. 由于 $u=H_1(id_i,id_j,SC,eX_j)$,攻击者需要通过参数 $eX_j=ex_jP$ 来求出 u. 由 CDH 假设知,利用 $U=eP$ 和 $X_j=x_jP$ 来求解 ex_jP 是困难的. 因而,攻击者无法得到 M. 此外,由于参数 e 由节点设备随机选取,与服务器无关,故服务器也无法得到明文 M. 因此,通信过程中传递的消息具有完善的机密性.

定理 3　方案提供了对消息的合法性认证机制.

证明　消息接收方 $Node_j$ 收到消息后,可以利用等式 $WP=P_{Pub}+Y_iH_2(id_i,id_j,SC,X_i,Y_i)+w'U$ 来验证消息的合法性. 该计算过程中引入了设备的身份标识 id,因而 $Node_j$ 可以实现对消息发送者的身份确认. 此外,同步序列 SC 的引入,可以防止攻击者对旧的消息 $\{U',V',W'\}$ 进行重放.

此外,由于节点设备不需要存储任何秘密参数且 PUF 具有不可克隆性,方案在抵抗窃听、篡改、重放及中间人攻击等传统安全威胁的同时,可以有效防范节点设备可能遭到的物理攻击和复制攻击.

5　实验及性能分析

5.1　实验测试

(1)实验环境

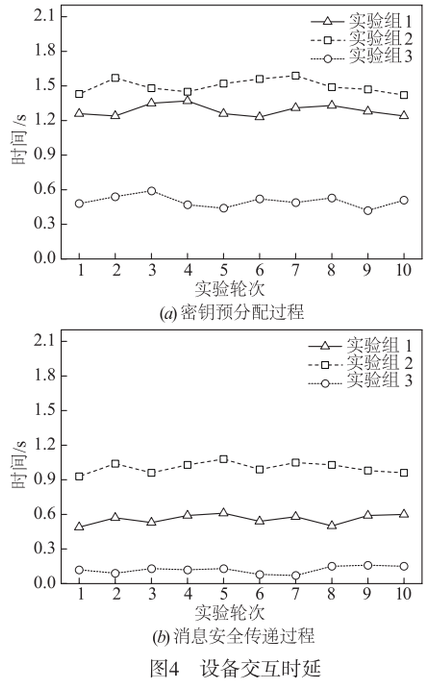
在蓝牙 4.0 协议栈的基础上构建原型系统进行实验. 实验采用 NIST 推荐的 P-192 椭圆曲线,各参数的长度和符号定义如表 1 所示.

表 1　参数长度及符号

参数	长度	长度符号
设备标识 *id*	48 bits	$L(id)$
同步序列 *SC*	48 bits	$L(SC)$
随机数 *n*	192 bits	$L(n)$
PUF 挑战信号 *c*	192 bits	$L(c)$
PUF 响应信号 *r*	192 bits	$L(r)$
哈希值 *hash*	192 bits	$L(hash)$
服务器私钥 *s*	192 bits	$L(s)$
椭圆曲线点 *Point*	384 bits	$L(Point)$
网络公开参数	1344 bits	$L(Paras)$

(2)实验结果

为直观反映方案的性能,设置了对照实验:实验组 1 实现本文安全方案,实验组 2 实现文献[14]方案,实现组 3 仅实现基本的通信功能. 在实验室环境下进行 10 轮测试,其结果如图 4 所示.



(a) 密钥预分配过程

(b) 消息安全传递过程

图4　设备交互时延

由实验结果可知,密钥预分配过程和消息安全传递过程均可在较短的时间内完成,且本文方案的时间消耗优于文献[14]方案.

5.2　性能分析

从存储、通信和计算开销三个方面对方案的性能

进行分析,并与文献[14]方案进行对比.

(1)存储开销

当节点设备数为 N 时,本文方案服务器存储开销为$(L(id)+L(c)+L(r))\times N+L(s)+L(Paras)$,每个节点设备的存储开销为 $L(id)+L(Paras)$;文献[14]方案中服务器和每个节点设备的存储开销分别为$(L(id)+K\times L(c)+K\times L(r))\times N+L(Paras)$和 $L(id)+L(Paras)$.

通过分析可知,两种方案中节点设备的存储开销相差不大,服务器的存储开销对比如图 5 所示.

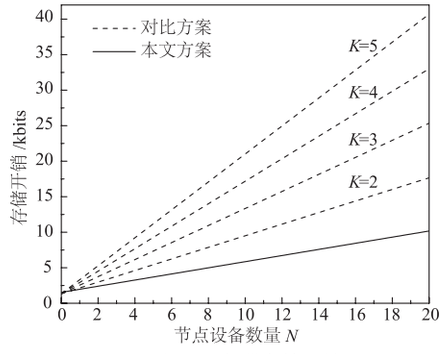


图5 服务器存储开销

(2)通信开销

以 $Node_i$向 $Node_j$发送消息的过程为例,分析方案的通信开销,并利用设备在交互过程中发送的消息长度来衡量其通信开销.

在参数长度相同的条件下,通过计算可得两种方案的通信开销对比如图 6 所示.

由图 6 可知,两种方案的总体通信开销相差不大,而本文方案中资源受限的节点设备的通信开销略优于文献[14]方案.

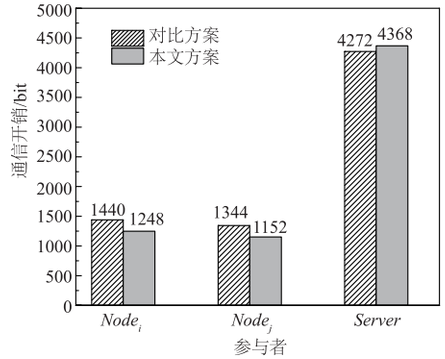
(3)计算开销

利用方案中设备执行复杂密码算法所需的时间来衡量其计算开销. 本文方案采用非奇异椭圆曲线密码设计,而文献[14]方案采用双线性对密码. 文献[16]在 Windows 系统中测试了相同条件下各密码运算的执行时间. 由此可得,两种方案的计算开销对比如图 7 所示.

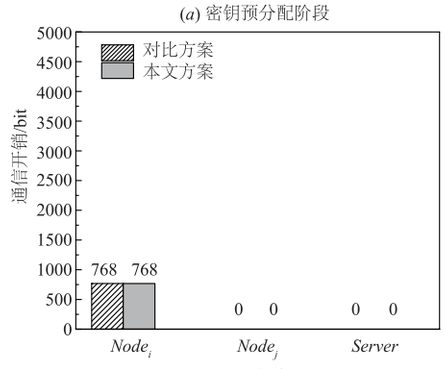
可知,相较于文献[14],本文方案计算开销明显改善. 密钥预分配阶段,节点设备和服务器的计算开销分别下降 72% 和 44%;消息安全传递阶段,$Node_i$和 $Node_j$的计算开销分别下降 90% 和 81%.

6 结束语

本文分析了现有物联网安全方案存在的不足,在此基础上将 PUF 与椭圆曲线上的无证书公钥密码体制相结合,提出一种面向物联网的安全通信方案. 该方案

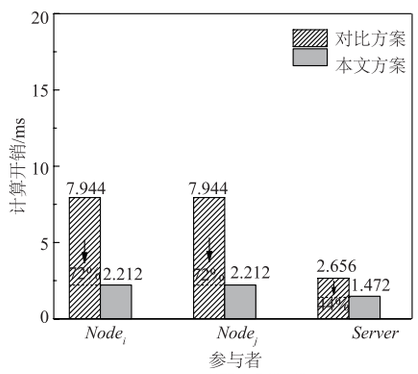


(a) 密钥预分配阶段

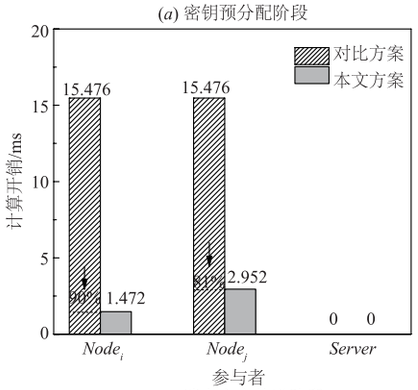


(b) 消息安全传递阶段

图6 通信开销



(a) 密钥预分配阶段



(b) 消息安全传递阶段

图7 计算开销

的安全性可归约为 PUF 的不可克隆性、不可预测性及椭圆曲线上的 CDH 问题. 相较于同类方案,本文方案明显降低了设备的资源开销且具有更高的安全性,可使物联网设备获得更好的网络免疫力,能够满足高安全要求领域的应用需求.

参考文献

[1] Li S,Xu L D,Zhao S. The Internet of things:a survey[J]. Information Systems Frontiers,2015,17(2):243 – 259.

[2] Wenliang Du,Jing Deng,Yunghsiang S Han,et al. A pairwise key predistribution scheme for wireless sensor networks[J]. ACM Transactions on Information and System Security (TISSEC),2005,8(2):228 – 258.

[3] 苏忠,林闯,任丰原. 无线传感器网络中基于散列链的随机密钥预分发方案[J]. 计算机学报,2009,32(1):30 – 41.
SU Zhong,LIN Chuang,REN Feng-yuan. Hash chain based random keys pre-distribution scheme in wireless sensor networks[J]. Chinese Journal of Computers,2009,32(1):30 – 41. (in Chinese)

[4] Delgado-Mohatar O, Ster-Sabater A, Sierra J. A lightweight authentication scheme for wireless sensor networks [J]. Ad Hoc Networks,2011,9(5):727 – 735.

[5] Huang J J,Juang W S,Fan C I. An efficient authentication and service key agreement scheme in IOT environments [J]. Frontiers in Artificial Intelligence & Applications, 2015,274:715 – 723.

[6] Hague-Chung,Choi K C,Jun M S. A design of key agreement scheme between lightweight devices in IoT environment[A]. International Conference on Computer Science and Its Applications[C]. GER:Springer Singapore,2016: 224 – 229.

[7] Kothmayr T,Schmitt C,Hu W,et al. DTLS based security and two-way authentication for the Internet of Things[J]. Ad Hoc Networks,2013,11(8):2710 – 2723.

[8] He D,Zeadally S,Kumar N,et al. Anonymous authentication for wireless body area networks with provable security [J]. IEEE Systems Journal,2016,PP(99):1 – 12.

[9] Seo S H,Won J,Sultana S,et al. Effective key management in dynamic wireless sensor networks[J]. IEEE Transactions on Information Forensics & Security,2015,10(2): 371 – 383.

[10] Challa S,Wazid M,Das A K,et al. Secure signature-based authenticated key establishment scheme for future IoT applications[J]. IEEE Access,2017,5(99):3028 – 3043.

[11] Marchand C,Bossuet L,Mureddu U,et al. Implementation and characterization of a physical unclonable function for IoT:a case study with the TERO-PUF[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,2018,33(1):97 – 109.

[12] Pappu R,Recht B,Taylor J,et al. Physical one-way functions[J]. Science,2002,297(5589):2026 – 2030.

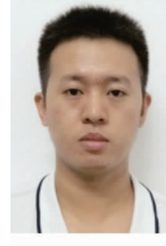
[13] G Eaward Suh, Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation[A]. Design Automation Conference[C]. USA: ACM/IEEE,2007. 9 – 14.

[14] Chatterjee U,Chakraborty R S,Mukhopadhyay D. A PUF-based secure communication protocol for IoT[J]. ACM Transactions on Embedded Computing Systems,2017,16 (3):1 – 25.

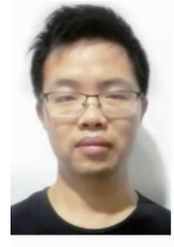
[15] Lim D,Lee JW,Gassend B,et al. Extracting secret keys from integrated circuits[J]. IEEE Transactions on Very Large Scale Integration Systems,2005,13(10):1200 – 1205.

[16] 谢永,吴黎兵,张宇波,等. 面向车联网的多服务器架构的匿名双向认证与密钥协商协议[J]. 计算机研究与发展,2016,53(10):2323 – 2333.
XIE Yong,YU Li-bing,ZHANG Yu-bo,et al. Anonymous mutual authentication and key agreement protocol in multi-server architecture for VANETs[J]. Journal of Computer Research and Development, 2016, 53(10): 2323 – 2333. (in Chinese)

作者简介



李森森　男,1993 年 7 月,河南洛阳人,硕士,信息工程大学助教,主要研究方向为网络安全、无线通信技术等.
E-mail:lss589@163.com



黄一才　男,1985 年 8 月,湖北巴东人,硕士,信息工程大学讲师,主要研究方向为网络安全、无线通信技术等.

郁　滨　男,1964 年 7 月,河南郑州人,博士,信息工程大学教授、博士生导师,主要研究方向为网络安全、无线通信技术、视觉密码等.