一种基于 Chebyshev 混沌映射和 CRT 的 ZigBee 网络匿名认证方案

廖伟，何乐生，尹恒，余圣涛，权家锐
（云南大学信息学院，云南 昆明 650091）

摘 要：针对 ZigBee 网络信任中心不完全可靠、入网时缺乏身份认证等问题，提出了一种基于 Chebyshev 混沌映射和中国剩余定理（CRT, Chinese remainder theorem）的 ZigBee 网络匿名认证方案。该方案不仅能实现匿名身份的双向认证，还可以保障 ZigBee 网络结构动态变化时密钥分发的安全；其主要基于一个 ZigBee 与 NB-IoT 的无线异构网关，使服务器能够通过该网关对网络中的节点进行有效的管理。从安全性分析以及与其他相关文献对比结果可以看出，所提方案具有更高的安全性，还具有匿名性、不可链接性。此外，实验结果表明所提方案在计算开销上较其他方案有更大的优势。

关键词：ZigBee 网络；Chebyshev 混沌映射；双向身份认证；匿名性；密钥分发
中图分类号：TP309.1
文献标志码：A
doi: 10.11959/j.issn.2096−3750.2023.00368

A ZigBee network anonymous authentication scheme based on Chebyshev chaotic mapping and CRT

LIAO Wei, HE Lesheng, YIN Heng, YU Shengtao, QUAN Jiarui
College of Information, Yunnan University, Kunming 650091, China

Abstract: A ZigBee network anonymous authentication scheme based on Chebyshev chaotic mapping and Chinese remainder theorem (CRT) was proposed to solve the problems such as the incomplete reliability of ZigBee network trust center and the lack of identity authentication when accessing the network. The proposed scheme can not only realize two-way authentication of anonymous identity, but also ensure the security of key distribution when ZigBee network structure changes dynamically. It is mainly based on a ZigBee and NB-IoT wireless heterogeneous gateway, so that the server can effectively manage the nodes in the network through this gateway. From security analysis and comparison with other related literature, the proposed scheme has higher security, with anonymity and unlink ability. In addition, the results show that the proposed scheme has more advantages than other schemes on the computational overhead.

Key words: ZigBee network, Chebyshev chaotic mapping, two-way identity authentication, anonymity, key distribution

0 引言

近年来，物联网技术的蓬勃发展，提高了物联网对新连接技术的需求。ZigBee 是 ZigBee 联盟维护的低速率无线个人局域网的开放标准，因低成本、低功耗以及安全性而被广泛应用于各种物联网场景。尽管 ZigBee 网络在多个领域有不错的应用，但由于网络中各节点需要相互通信，所以安全性、身份隐私和一些其他问题仍然存在重大挑战。特别是在集中式 ZigBee 网络架构中，根据 ZigBee 协议规范的描述[1]，每个集中式 ZigBee 网络架构中都有一个控制器，又称信任中心（TC, trust center）。它是 ZigBee 网络中的一个关键组成部分，需要负责整个网络的形成、信道选择、密钥分发、数据路由

收稿日期：2023−04−10；**修回日期：**2023−08−22
通信作者：何乐生，he_lesheng@263.net
基金项目：国家自然科学基金资助项目（No.U1631121）
Foundation Item: The National Natural Science Foundation of China (No.U1631121)

和网络的有效管理。因此，整个网络的安全性首先取决于它的可靠性。此外，安全性一直是 ZigBee 网络研究的焦点，许多提高安全性的方案也被提出。然而，现有的大多数方案在认证过程中使用的都是节点的真实身份，而真实身份的泄露可能会带来巨大的隐患[2]；此外，最近出现的 ZigBee 网络攻击大多是所采用的认证方案中的漏洞造成的。因此，设计一种高安全性且适用于资源受限环境，并可保护隐私的认证方案是至关重要的。

在对 ZigBee 网络安全的研究中，Hoceini 等[3]提出了一种用于 ZigBee 网络的认证机制。该机制基于椭圆曲线数字签名，通过访问控制列表防止未注册的节点进入网络，并通过信任中心验证节点的身份确保安全的通信，但该方案无法提供完美的后向安全性。由于在开放环境中 ZigBee 节点容易受到复制攻击和设备捕获等物理攻击，Xiong 等[4]提出了一种基于物理不可克隆函数的认证方案，该方案能够抵御物理攻击和复制攻击，然而，它无法提供隐私保护。混沌映射在密码学中的应用一直是研究的热点[5-12]。扩展的 Chebyshev 混沌映射因具有完美的随机性、半群性以及高安全性被广泛应用于认证和匿名通信[13]。此外，在安全性和计算效率方面，它比椭圆曲线密码学系统或 RSA 密码系统更有效[14]。因此，基于 Chebyshev 混沌映射的认证方案成为一个合适选择[15-17]。移动 Ad Hoc 网络的出现使许多学者对 CRT 产生了浓厚的兴趣。Zheng 等[18]介绍了两种基于 CRT 的集中式组密钥管理方案。常相茂等[19]提出了一种低开销的 NB-IoT 节点群组身份安全认证方案，该方案采用了基于 CRT 的密钥分发机制，保证了密钥分发的后向安全性。

综上所述，现有文献提出的 ZigBee 网络认证方案大多对匿名性、信任中心可靠性等安全问题考虑不全，且很少考虑 ZigBee 网络密钥分发的安全性。因此，本文针对上述问题，提出了一种 ZigBee 网络的匿名认证方案。本文的主要贡献如下。

1) 针对 ZigBee 网络信任中心不可靠问题，提出了一种 ZigBee 与 NB-IoT 结合的异构网络，实现了服务器对网络中各节点的有效管理。

2) 结合 Chebyshev 混沌映射和 CRT，提出了一种更安全的 ZigBee 网络匿名认证方案，不仅解决了 ZigBee 网络入网节点身份认证的问题，还为合法节点提供了良好的隐私保护。此外，基于 CRT 的密钥分发机制也为所提方案提供了更完美的后向安全性。

1　预备知识

1.1　Chebyshev 混沌映射

Chebyshev 混沌映射原理简单，是认证方案中最常用的混沌映射之一[20-22]。设 n 为正整数，x 为 $[-1,1]$ 的变量。Chebyshev 多项式 $T_n(x):[-1,1]\to[-1,1]$ 定义为 $T_n(x)=\cos(\cos^{-1}\theta)$。$n$ 维 Chebyshev 多项式 $T_n(x):\mathbf{R}\to\mathbf{R}$ 定义为

$$T_n(x)=2xT_{n-1}(x)-T_{n-2}(x) \tag{1}$$

其中，$n\geqslant 2, T_0(x)=1, T_1(x)=x$。

Chebyshev 多项式的半群性质表示为

$$T_r(T_s(x))=T_{sr}(x)=T_s(T_r(x)),\ s,r\in\mathbf{Z}^+ \tag{2}$$

为了增强安全性，Zhang[23]证明了在 $(-\infty,+\infty)$ 上定义 Chebyshev 多项式的半群性质仍然成立。在所提方案中，使用了扩展的 Chebyshev 多项式。

定义 1　给定 x 和 y，很难找到整数 s，使得 $T_s(x)=y \bmod p$。这被称为基于混沌映射的离散对数问题。

定义 2　给定 $x, T_r(x) \bmod p$ 和 $T_s(x) \bmod p$ 这很难找到 $T_{rs}(x) \bmod p$。这被称为基于混沌映射的 Diffie-Hellman 问题。

1.2　中国剩余定理

CRT 是数论中的一个重要定理。它指出，在一元线性同余方程组中，除数是成对互素的条件下，可以唯一地确定 x 除以这些互素数乘积的余数[24-25]。

2　系统模型

本文提出的 ZigBee 异构网络系统模型如图 1 所示。该模型主要由服务器、信任中心、终端节点 3 部分实体组成。

其中，服务器拥有强大的计算、存储能力，是一个完全可信的机构，主要负责节点的注册、密钥更新以及假名更新和数据处理。信任中心作为服务器与终端节点间的网关节点，除了需要转发消息，还需要维护节点假名与公钥的映射表以及匿名身份认证、密钥分发。终端节点主要负责数据的收集，此外，它还存储了身份验证的各种秘密参数。

在本文所讨论的系统中，信任中心与服务器之间的通信是安全的。但信任中心本身并不可靠，当它被攻击者捕获或者非法占有时，终端节点将不再上传数据到服务器。

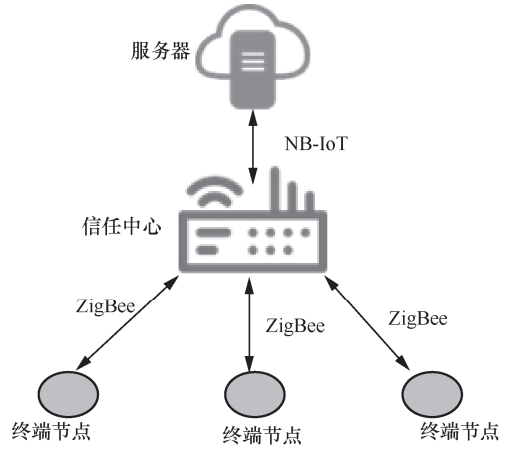


图 1　ZigBee 异构网络系统模型

3　双向认证方案

本节所使用的符号定义见表 1。

表 1　　符号定义

符号	定义
$\mathrm{Nod}_{i,j}$	终端节点 i,j
$\mathrm{ID}_{i,j}$、ID_{c}、$\mathrm{PID}_{i,j}$、$\mathrm{PID}_{\mathrm{c}}$	终端节点 i,j、信任中心 IEEE 地址以及假名
$\mathrm{Ts}_{i,j}$、x	假名有效期、切比雪夫随机种子 ρ
P、$p_{i,j}$、p_{c}	大素数、终端节点以及信任中心的组密钥生成密钥
$r_{i,j}$、r_{c}、$\mathrm{sk}_{\mathrm{TA}}$	终端节点示 i,j、信任中心、服务器私钥
Pub_i、$\mathrm{Pub}_{\mathrm{c}}$、$\mathrm{pk}_{\mathrm{TA}}$	终端节点 i、信任中心、服务器公钥
hash(·)、$H(\cdot)$	防碰撞单向哈希函数
$\mathrm{enc}_k(\cdot)$、$\mathrm{dec}_k(\cdot)$	AES 加/解密函数
$\|\|$	字符串连接符
$T(\cdot)$	切比雪夫混沌映射
GK	组密钥生成信息
Pgk_i、Rgk	组密钥载体、组密钥
List、$t_{i,j}$、t_{c}、t_{TA}	哈希映射表、时间戳
symk	对称链接密钥

3.1　初始化阶段

在此阶段，服务器首先选择 Chebyshev 混沌映射 $T(\cdot)$、$x\in\mathbf{Z}_P^*$ 作为它的随机种子，再选择随机数 $\mathrm{sk}_{\mathrm{TA}}$ 作为私钥，计算公钥 $\mathrm{pk}_{\mathrm{TA}}$

$$\mathrm{pk}_{\mathrm{TA}}=T_{\mathrm{sk}_{\mathrm{TA}}}(x)\bmod P \tag{3}$$

其中，P 是一个大素数。最后选择一个单向哈希函数 hash(·) 以及 AES 对称加/解密函数 $\mathrm{enc}_k(\cdot)/\mathrm{dec}_k(\cdot)$，并将 $\{T(\cdot),\mathrm{pk}_{\mathrm{TA}},\mathrm{hash}(\cdot),\mathrm{enc}_k(\cdot)/\ \mathrm{dec}_k(\cdot),x,P\}$ 作为公共参数公布。

3.2　信任中心注册阶段

服务器首先会为其生成假名 $\mathrm{PID}_{\mathrm{c}}=\mathrm{ID}_{\mathrm{c}}\oplus H(\mathrm{sk}_{\mathrm{TA}})$。选择一个随机数 r_{c} 作为其私钥，并计算其公钥 $\mathrm{Pub}_{\mathrm{c}}=\mathrm{Tr}_{\mathrm{c}}(x)\bmod P$。接着为其生成组密钥生成密钥 p_{c} 并计算 $\mathrm{GK}:\mathrm{GK}=\mathrm{Pgk}_i\sum_{i=1}^{n}\mathrm{Var}_i \bmod P$，其中 $\mathrm{Var}_i=M_iM_i^{-1}$，$\mathrm{Pgk}_i=\mathrm{Rgk}\oplus\mathrm{ID}_i$，$M_i=P/p_i$，$M_i^{-1}$ 是 M_i 的乘法逆元。此外，信任中心需要维护一个终端节点假名哈希值与其公钥的映射表 List。最后服务器通过安全通道将 $\{\mathrm{PID}_{\mathrm{c}},r_{\mathrm{c}},\mathrm{Pub}_{\mathrm{c}},p_{\mathrm{c}},\mathrm{GK},\mathrm{List}\}$ 发送给信任中心。

3.3　终端节点注册阶段

服务器首先会为终端节点 Nod_i 生成其假名 $\mathrm{PID}_i=\mathrm{ID}_i\oplus\mathrm{H}(\mathrm{sk}_{\mathrm{TA}}\|\mathrm{Ts}_i)$。选择一个随机数 r_i 作为其私钥，并计算公钥 $\mathrm{Pub}_i=\mathrm{Tr}_i(x)\bmod P$。接着再为其生成 p_i。最后服务器通过有线连接将 $\{\mathrm{PID}_i,\mathrm{Ts}_i,p_i,r_i,\mathrm{Pub}_i,\mathrm{PID}_{\mathrm{c}}\}$ 下载到终端节点的只读存储器（ROM, read-only memory）中。

3.4　双向认证以及组密钥分发阶段

当终端节点 Nod_i 入网时，它会收到来自信任中心的信标消息。而终端节点会验证它的真实性，如果发现信任中心是真实的，终端节点将执行双向认证阶段。双向认证流程如图 2 所示，具体步骤如下。

终端节点通过同步时钟生成时间戳 t_i，然后选择一个随机数 $r_s\in\mathbf{Z}_P^*$ 并生成密文

$$\begin{aligned}&\mathrm{C1}=\mathrm{Tr}_s(x)\bmod P;\\&\mathrm{C2}=\mathrm{PID}_i\cdot\mathrm{Tr}_s(\mathrm{Pub}_{\mathrm{c}})\bmod P;\\&\mathrm{C3}=t_i\oplus\mathrm{PID}_i;\\&\mathrm{C4}=\mathrm{hash}(\mathrm{t}_i\|\mathrm{PID}_i)\end{aligned}\tag{4}$$

终端节点将 $\{\mathrm{C1},\mathrm{C2},\mathrm{C3},\mathrm{C4}\}$ 发送给信任中心。

当信任中心接收到终端节点发送的认证请求消息时，执行以下操作。首先计算 $\mathrm{PID}_i'=\mathrm{C2}/\mathrm{Tr}_{\mathrm{c}}(\mathrm{C1})\bmod P$。检查 List 中是否存在此 PID_i' 的哈希值，若不存在，则拒绝接收此消息；若存在，则接着验证 $t_i'=\mathrm{C3}\oplus\mathrm{PID}_i'$。当 $t-t_i'\leqslant\Delta t$ 成立时，再比较 $\mathrm{hash}(t_i'\|\mathrm{PID}_i')\overset{?}{=}\mathrm{hash}(t_i\|\mathrm{PID}_i)$，若相等，则验证成功；否则信任中心将会通过函数 ZDSecMgrAPSRemove(·)将节点移出网络。最后通过 List 查找对应的 Pub_i，选择随机数 $r_m,r_k\in\mathbf{Z}_P^*$ 以及时间戳 t_{c}，生成密文

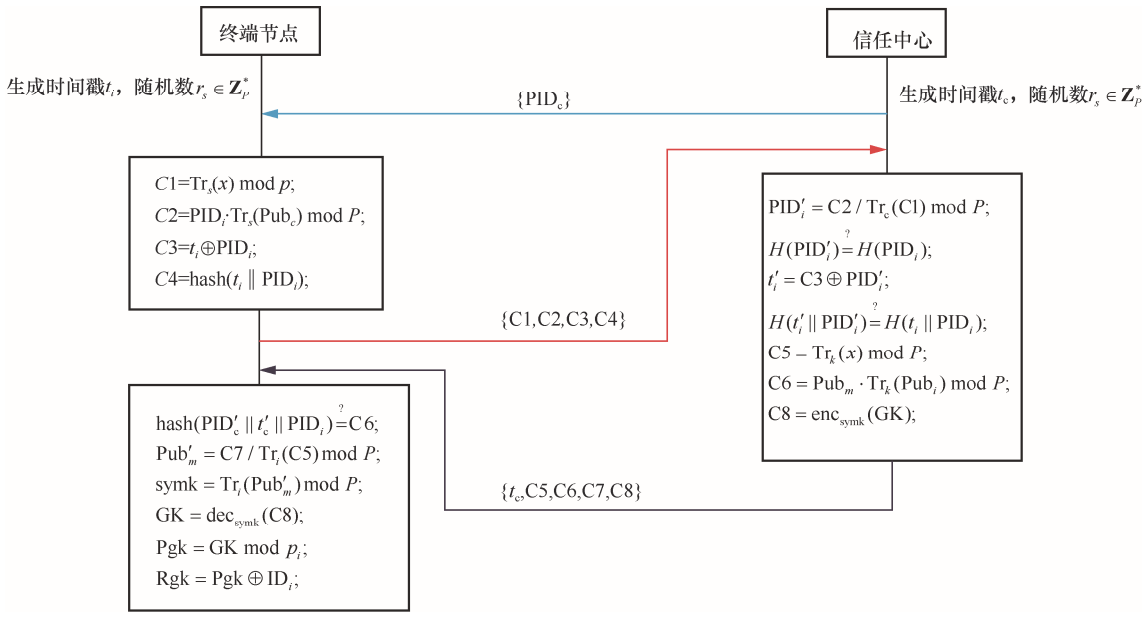


图 2　双向认证流程

$$\begin{aligned}
&\mathrm{C5}=\mathrm{Tr}_k(x) \bmod P;\\
&\mathrm{C6}=\mathrm{hash}(\mathrm{PID_c} \,\|\, \mathrm{PID}_i \,\|\, t_\mathrm{c});\\
&\mathrm{C7}=\mathrm{Pub}_m \cdot \mathrm{Tr}_k(\mathrm{Pub}_i) \bmod P;\\
&\mathrm{C8}=\mathrm{enc}_{\mathrm{symk}}(\mathrm{GK})
\end{aligned} \tag{5}$$

其中，$\mathrm{symk}=T_{r_m \oplus \mathrm{ID_c}}(\mathrm{Pub}_i) \bmod P$。信任中心将$\{t_\mathrm{c},\mathrm{C5},\mathrm{C6},\mathrm{C7},\mathrm{C8}\}$发送给终端节点。

当终端节点接收到来自信任中心的认证回复消息时，将执行以下操作：首先验证t_c，若$t-t_\mathrm{c} \leqslant \Delta t$成立，则继续计算$\mathrm{hash}(\mathrm{PID}'_\mathrm{c} \,\|\, t'_\mathrm{c} \,\|\, \mathrm{PID}_i) \stackrel{?}{=} \mathrm{C6}$，若相等，则验证成功；若不成立，则拒绝接收此消息。通过$\mathrm{Pub}'_m = \mathrm{C7} / \mathrm{Tr}_i(\mathrm{C5}) \bmod P$计算出$\mathrm{symk}=\mathrm{Tr}_i(\mathrm{Pub}'_m) \bmod P$并得到GK，再使用$p_i$解出组密钥Rgk，随即就可以在网络中进行安全的通信了。

3.5　组密钥更新阶段

当有新的终端节点加入或旧的终端节点离开网络时，信任中心将发送组密钥更新请求消息到服务器。服务器收到该请求消息后，将重新计算$\sum_{i=1}^{n}\mathrm{Var}_i - \mathrm{Var}_i^{\mathrm{old}}$或$\sum_{i=1}^{n}\mathrm{Var}_i + \mathrm{Var}_i^{\mathrm{new}}$并生成新的组密钥$\mathrm{Rgk}^{\mathrm{new}}$，从而得到新的组密钥生成信息$\mathrm{GK}^{\mathrm{new}}$，并通过信任中心将其广播到网络中的各终端节点。

3.6　假名生成以及分发

在此阶段，当终端节点Nod_j假名有效期到期，服务器会为其分配一个新的假名。该过程基于 Kerberos 协议[26]，一个基于对称加密的认证协议。终端节点假名更新流程如图 3 所示，详细过程如下。

终端节点通过同步时钟添加时间戳t_j，选择随机数r_g计算Pub_g。并生成假名请求消息$\mathrm{Ms}_{\mathrm{Pseu}}=\{\mathrm{UpdatePseudonyms标识符},\mathrm{Ts}_j,\mathrm{at}_j\}$。其中，$\mathrm{at}_j=\mathrm{hash}(\mathrm{ID}_j \,\|\, t_j)$。再用$\mathrm{Pub}_g(\mathrm{pk_{TA}}) \bmod P$加密假名请求消息$\mathrm{Ms}_{\mathrm{pseu}}$生成$\mathrm{Cs}_{\mathrm{pseu}}$。最后使用symk加密生成密文$C_j=\mathrm{enc}_{\mathrm{symk}}(t_j,\mathrm{PID}_j,\mathrm{Pub}_g,\mathrm{Cs}_{\mathrm{pseu}})$。终端节点将密文$C_j$发送给信任中心。

当信任中心接收到密文C_j时，首先使用symk对它解密得到$\{t_j,\mathrm{PID}_j,\mathrm{Pub}_g,\mathrm{Cs}_{\mathrm{pseu}}\}$。再检查$t_j$，若$t-t_j \leqslant \Delta t$成立，则继续检查中是否存在此的哈希值，若存在，则验证成功。信任中心通过同步时钟添加时间戳t'_j，生成消息$M=\{t'_j,\mathrm{at_c},t_j,\mathrm{PID}_j,\mathrm{Pub}_g,\mathrm{Cs}_{\mathrm{pseu}}\}$，其中$\mathrm{at_c}=\mathrm{hash}(\mathrm{Cs}_{\mathrm{pseu}} \,\|\, t'_j \,\|\, r_\mathrm{c})$。

当服务器收到消息M后，先检查t'_j，再计算$\mathrm{at}'_\mathrm{c}=\mathrm{hash}(\mathrm{Cs}_{\mathrm{pseu}} \,\|\, t'_j \,\|\, r_\mathrm{c})$。如果$\mathrm{at_c}'=\mathrm{at_c}$，则该信任中心合法。接下来，先使用$\mathrm{Pub}_{\mathrm{sk_{TA}}}(\mathrm{Pub}_j) \bmod P$解密$\mathrm{Cs}_{\mathrm{pseu}}$得到$\mathrm{Ms}_{\mathrm{pseu}}$。通过终端节点假名$\mathrm{PID}_j$找到其真实身份$\mathrm{ID}_j$并计算$\mathrm{at}'_j=\mathrm{hash}(\mathrm{ID}_j \,\|\, t_j)$。如果$\mathrm{at}'_j=\mathrm{at}_j$。则为其生成新的节点假名$\mathrm{PID}_j^{\mathrm{new}}=\mathrm{ID}_j \oplus H(\mathrm{sk_{TA}} \,\|\, \mathrm{Ts}_j^{\mathrm{new}})$。最后服务器生成节点假名更新消息$\mathrm{Ms}_{\mathrm{update}}=\{\mathrm{UpdatePseudonyms标识符},\mathrm{ID}_j,\mathrm{PID}_j^{\mathrm{new}},\mathrm{Ts}_j^{\mathrm{new}}\}$，

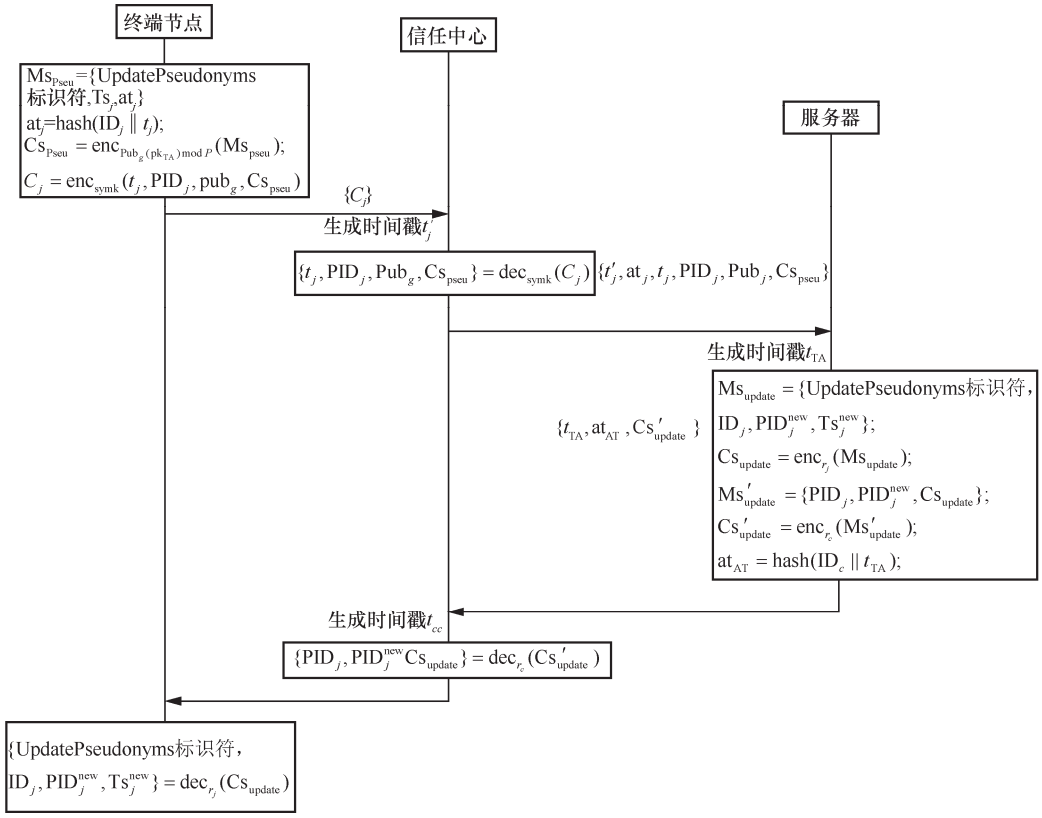


图 3　终端节点假名更新流程

并用对称密钥 r_j 加密成密文 $Cs_{update} = enc_{r_j}(Ms_{update})$。再使用对称密钥 r_c 对消息 $Ms'_{update} = \{PID_j, PID_j^{new}, Cs_{update}\}$ 加密生成 $Cs'_{update} = enc_{r_c}(Ms'_{update})$。最后服务器发送消息 $\{t_{TA}, at_{AT}, Cs'_{update}\}$ 给信任中心。其中 $at_{AT} = hash(ID_c \| t_{TA})$。

当信任中心接收到更新回复消息的时候，首先检查 t_{TA}，再计算 $at'_{AT} = hash(ID_c \| t_{TA})$。如果 $at'_{AT} = at_{AT}$，则使用对称密钥 r_c 解密 Cs'_{update} 得到 $\{PID_j, PID_j^{new}, Cs_{update}\}$。再更新 List 中对应的假名哈希值，最后将消息 $\{Cs_{update}, t_{cc}\}$ 发送给终端节点。

当终端节点接收到假名更新回复消息后，首先检查 t_{cc}，再使用对称密钥 r_j 解密 Cs_{update} 得到消息 $\{UpdatePseudonyms标识符, ID_j, PID_j^{new}, Ts_j^{new}\}$ 并获得新的假名。

4　方案分析

4.1　安全分析

4.1.1　双向认证

该方案提供双向认证。信任中心通过节点发来的加密假名验证其合法性。其中假名的安全性是基于 $T_{r_i}(Pub_c) \bmod P = T_{r_i}(T_{r_c}) \bmod P = T_{r_c}(T_{r_i}) \bmod P$ 的。而该密钥的安全性是基于 Chebyshev 混沌映射的 Diffie-Hellman 问题：已知 $T_n(x) \bmod p, T_m(x) \bmod P$、$x$、$p$ 的值，在常规多项式线性时间无法求出 $T_{nm}(x) \bmod P$，所以只有具有私钥 r_c 的信任中心才能解出终端节点的假名。同样地，终端节点通过信任中心的假名来验证其合法性。

4.1.2　匿名性

匿名性意味着攻击者无法从通信消息中直接获取终端节点的真实身份 ID_i，因为该真实身份隐藏在终端节点假名 PID_i 中，只有合法的服务器能够通过其主密钥 sk_{TA} 以及 Ts_i 获得终端节点的真实身份 ID_i，故攻击者很难获取终端节点的真实身份。此外，信任中心的真实身份假名包含于 PID_c 中，只有合法的服务器能够通过其主密钥 sk_{TA} 获得信任中心的真实身份 ID_c，故攻击者也很难获得信任中心的真实身份。

4.1.3　已知密钥安全性

已知组密钥生成信息 $GK = Pgk_i \sum_{i=1}^{n} Var_i \bmod P$，其中，$Pgk_i = Rgk \oplus ID_i$，$M_i = P / p_i$，$M_i^{-1}$ 是 M_i 的逆元；要想获得组密钥 Rgk，除了组密钥生成密

钥 p_i，还需要合法节点身份 ID_i。而 p_i 和 ID_i 仅有服务器和终端节点本身知道。

4.1.4 前后向安全性

当终端节点离开网络时，组密钥将被更新，离开网络的终端节点无法计算新的组密钥。因此，方案满足前向安全性。当有新的终端节点加入网络时，如果它想获得以前的消息，它需要以前的组密钥。由于新加入的终端节点无法计算前一个组密钥，因此方案满足后向安全性。

4.1.5 抵抗重放攻击

重放攻击是指恶意攻击者将先前收到的消息重新发送给网络中的节点，以达到攻击合法节点的目的。为了防止所提方案受到重放攻击，在通信的过程中添加了时间戳，以便接收者可以通过验证时间戳的新鲜度来抵抗重放攻击。

4.1.6 抵抗模拟攻击

在假名生成和分配阶段，终端节点发送消息请求新的假名。终端节点使用 symk 加密 t_j、PID_j、Pub_g、$\mathrm{Cs}_{\mathrm{pseu}}$，而该对称密钥仅终端节点和信任中心可知。因此，为了模拟终端节点，必须获得对称密钥，这是很困难的。此外 $\mathrm{Cs}_{\mathrm{pseu}}$ 是由 $\mathrm{Pub}_g(\mathrm{pk}_{\mathrm{TA}}) \bmod P$ 加密的，而该消息只有知道私钥 $r_g, \mathrm{sk}_{\mathrm{TA}}$ 才可以解出。因此，为了在假名更新阶段模拟终端节点，必须知道对称链接密钥 symk 或者私钥 r_g, $\mathrm{sk}_{\mathrm{TA}}$。

4.1.7 不可链接性

在终端节点与信任中心进行双向认证时，通信双方发送的均为假名，因此攻击者无法获取到通信双方的真实身份。此外，假名会被频繁地更新，因此攻击者无法将消息和消息的发送者连接起来。

4.2 ProVerif 工具安全性验证

ProVerif 是一个形式化的自动密码协议分析工具，提供对多种加密原语的支持。它也可以检查协议的可达性，验证协议的一致性和等价性。在 ProVerif 中，攻击者可以监视公共信道以控制系统，并可以拦截、篡改和重放信道中的所有数据消息。因此，为了进一步验证方案的安全性和可行性，本节通过在 ProVerif 中对所提方案进行建模，并对一些常见的攻击进行查询，证明了所提方案的匿名性、双向认证以及保密性。ProVerif 工具验证结果如图 4 所示。

4.3 安全性对比

安全性对比见表 2。

4.4 计算开销

本节主要讨论整个通信过程本方案与其他相关方案在计算开销方面的比较。为了方便讨论，T_{h}、T_{c}、T_{eca}、T_{ecm}、T_{sym}、T_{asy}、T_{F} 分别表示进行一次哈

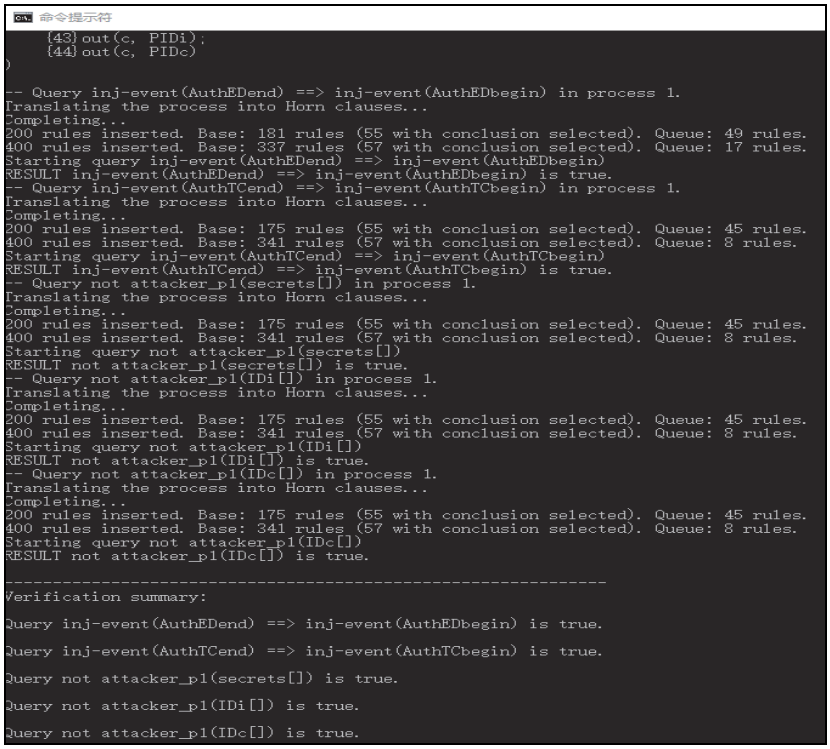


图 4　ProVerif 工具验证结果

表 2　　安全性对比

对比项	Hoceini[3]方案	Xiong[4]方案	Cao[27]方案	Zhang[28]方案	所提方案
双向认证	√	√	√	√	√
匿名性	×	×	×	√	√
已知密钥安全性	×	√	√	√	√
前向安全性	√	√	√	√	√
后向安全性	×	√	×	×	√
抵抗重放攻击	×	√	√	√	√
抵抗模拟攻击	√	√	√	√	√
不可链接性	×	×	×	×	√

希运算、一次 Chebyshev 混沌映射、一次椭圆曲线中的点加、一次椭圆曲线中的点乘、一次对称加密算法、一次对称解密算法、生物特征的检测和提取所用的时间。根据文献[23,28]可知上述密码学的平均执行时间以及相互的比例关系。各认证方案计算开销对比见表 3。

表 3　　各认证方案计算开销对比

方案	T_h/ms	T_c/ms	T_{eca}/ms	T_{ecm}/ms	T_{sym}/ms	T_{asy}/ms	T_F/ms
Hoceini[3]方案	2	0	2	7	0	0	0
Xiong[4]方案	8	0	6	10	0	0	0
Cao[27]方案	18	8	0	0	0	0	0
Zhang[28]方案	17	10	0	0	4	4	3
所提方案	5	9	0	0	1	1	0

各方案认证过程计算开销如图 5 所示，可以看出 Hoceini[3]方案、Xiong[4]方案的计算开销较大，而所提方案与 Zhang[28]方案、Cao[27]方案计算开销相当。因此，从上述分析结果可知，相较于现有的基于椭圆曲线密码学的方案，基于 Chebyshev 混沌映射的方案在计算开销上具有显著优势。且在计算开销相当的情况下，所提方案具有较少的通信轮数，仅通过 3 轮通信消息便可保证通信双方的安全认证，极大地提高了通信效率。此外，假名以及假名更新机制，进一步提高了整个网络的安全性。

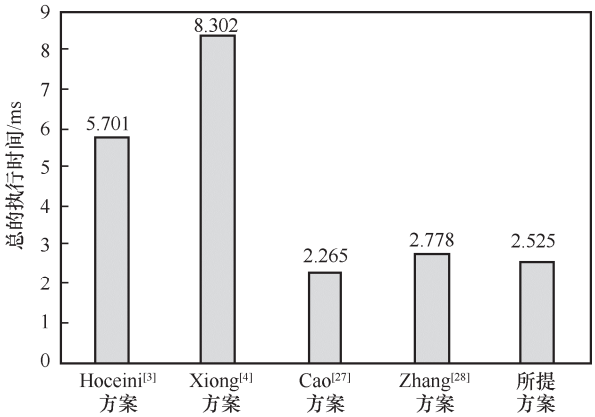


图 5　各方案认证过程计算开销

4.5　资源占有

本文在配置为 AMD Ryzen 5 4600H、RAM 大小为 16 GB 的 Windows10 系统以及 IAR 8.32.1 编译环境下对 ZigBee 设备 CC2538（具有 512 KB 内存和 32 KB RAM 的 32 位 Arm Cortex-M3 Zigbee 和 6LoWPAN、IEEE802.15.4 无线 MCU）的资源占有情况进行测试，信任中心、终端节点资源占有情况分别见表 4、表 5。

表 4　　信任中心资源占有情况

类型	标准容量/KB	实际占有/KB	占比
FLASH	512	145.56	25.43%
RAM	32	16.01	50.05%

表 5　　终端节点资源占有情况

类型	标准容量/KB	实际占有/KB	占比
FLASH	512	122.54	23.93%
RAM	32	13.01	40.68%

5　结束语

在 ZigBee 网络中，认证与隐私保护是一个重要且具有挑战性的问题[29-30]。因此，本文提出了一种基于 Chebyshev 混沌映射和 CRT 的 ZigBee 网络匿名

认证方案。通过结合 NB-IoT 和 ZigBee 两种无线通信技术，构造了一个异构网络。不仅解决了信任中心不可靠带来的安全问题，还实现了身份的双向认证。在该方案中，通过传输假名进行认证而不是真实身份，从而保护了节点的身份隐私。此外，使用 ProVerif 工具验证了方案的安全性，且与其他方案相比，所提方案有更高的安全性能，除了能抵抗常见攻击，还具有匿名性。实验表明，所提方案的计算开销较其他方案均具有优势，且硬件资源消耗均少于 55%，更适用于资源受限的 ZigBee 网络环境。

参考文献：

[1] ZigBee Alliance. ZigBee security specification overview[EB]. 2010.

[2] GUPTA A, KASBEKAR G S. Secure, anonymity-preserving and lightweight mutual authentication and key agreement protocol for home automation IoT networks[C]//Proceedings of 2022 14th International Conference on Communication Systems & Networks (COMSNETS). Piscataway: IEEE Press, 2022: 375-383.

[3] HOCEINI O, AFIFI H, AOUDJIT R. Authentication based elliptic curves digital signature for ZigBee networks[C]//International Conference on Mobile, Secure, and Programmable Networking. Cham: Springer, 2017: 63-73.

[4] XIONG J, YU B. A novel secure communication scheme for ZigBee mesh network based on physical unclonable function[C]//Proceedings of 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS). Piscataway: IEEE Press, 2021: 783-789.

[5] CHUNG H L H. Chaos based RFID authentication protocol[D]. Canada: University of Ottawa, 2013.

[6] LI X, WU F, KHAN M K, et al. A secure chaotic map-based remote authentication scheme for telecare medicine information systems[J]. Future Generation Computer Systems, 2018(84): 149-159.

[7] 杨吉云, 姚锐冬, 周洁, 等. 基于切比雪夫混沌映射的车联网高效认证方案[J]. 计算机工程, 2021, 47(10): 34-42, 51.
YANG J Y, YAO R D, ZHOU J, et al. Efficient authentication scheme based on Chebyshev chaotic map for VANET[J]. Computer Engineering, 2021, 47(10): 34-42, 51.

[8] YANG J Y, DENG J M, XIANG T, et al. A Chebyshev polynomial-based conditional privacy-preserving authentication and group-key agreement scheme for VANET[J]. Nonlinear Dynamics, 2021, 106(3): 2655-2666.

[9] 蒋东华, 朱礼亚, 沈子懿, 等. 结合二维压缩感知和混沌映射的双图像视觉安全加密算法[J]. 西安交通大学学报, 2022, 56(2): 139-148.
JIANG D H, ZHU L Y, SHEN Z Y, et al. A double image visual security encryption algorithm combining 2D compressive sensing and chaotic mapping[J]. Journal of Xi'an Jiaotong University, 2022, 56(2): 139-148.

[10] 郭琰, 石飞, 汪烈军, 等. WSNs 中一种基于 Chebyshev 混沌映射的认证密钥协商协议[J]. 中国科技论文, 2017, 12(8): 900-904.
GUO Y, SHI F, WANG L J, et al. An authentication key agreement protocol based on Chebyshev chaotic map in WSNs[J]. China Sciencepaper, 2017, 12(8): 900-904.

[11] ABDELFATAH R I, ABDAL-GHAFOUR N M, NASR M E. Secure VANET authentication protocol (SVAP) using Chebyshev chaotic maps for emergency conditions[J]. IEEE Access, 2021(10): 1096-1115.

[12] LI C T, WU T Y, CHEN C M. A provably secure group key agreement scheme with privacy preservation for online social networks using extended chaotic maps[J]. IEEE Access, 2018(6): 66742-66753.

[13] ZHANG L. Cryptanalysis of the public key encryption based on multiple chaotic systems[J]. Chaos, Solitons & Fractals, 2008, 37(3): 669-674.

[14] VAN WAART O, THIJSSEN J. Traditional cryptography[EB]. 2015.

[15] ZHU H F. Using chaotic maps to construct anonymous multi-receiver scheme based on BAN logic[EB]. 2016.

[16] SUN Y, ZHU H F, FENG X S. A novel and concise multi-receiver protocol based on chaotic maps with privacy protection[J]. International Journal of Network Security, 2017(19): 371-382.

[17] ZHU H F, ZHANG Y. An efficient chaotic maps-based deniable authentication group key agreement protocol[J]. Wireless Personal Communications, 2017, 96(1): 217-229.

[18] ZHENG X L, HUANG C T, MATTHEWS M. Chinese remainder theorem based group key management[C]//Proceedings of the 45th annual southeast regional conference. New York: ACM Press, 2007: 266-271.

[19] 常相茂, 占俊, 王志伟. 低开销的 NB-IoT 节点群组身份安全认证协议[J]. 通信学报, 2021, 42(12): 152-162.
CHANG X M, ZHAN J, WANG Z W. Low-cost group-based identity security authentication protocol for NB-IoT nodes[J]. Journal on Communications, 2021, 42(12): 152-162.

[20] DHARMINDER D, GUPTA P. Security analysis and application of Chebyshev chaotic map in the authentication protocols[J]. International Journal of Computers and Applications, 2019: 1-9.

[21] DHARMINDER D, KUNDU N, MISHRA D. Construction of a chaotic map-based authentication protocol for TMIS[J]. Journal of Medical Systems, 2021, 45(8): 1-10.

[22] DHARMINDER D, KUMAR U, GUPTA P. A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services[J]. Complex & Intelligent Systems, 2021, 7(5): 2531-2542.

[23] ZHANG L P, ZHU Y, REN W, et al. An energy-efficient authentication scheme based on Chebyshev chaotic map for smart grid environments[J]. IEEE Internet of Things Journal, 2021, 8(23): 17120-17130.

[24] ZHOU J, OU Y H. Key tree and Chinese remainder theorem based group key distribution scheme[C]//International Conference on Algorithms and Architectures for Parallel Processing. Berlin, Heidelberg: Springer, 2009: 254-265.

[25] VIJAYAKUMAR P, BOSE S D, KANNAN A. Chinese remainder theorem based centralised group key management for secure multicast communication[J]. IET Information Security, 2014, 8(3): 179-187.

[26] NEUMAN B C, TS'O T. Kerberos: an authentication service for computer networks[J]. IEEE Communications Magazine, 1994, 32(9): 33-38.

[27] 曹阳. 基于扩展混沌映射的动态身份认证密钥协商协议[J]. 成都理工大学学报(自然科学版), 2021, 48(4): 505-512.
CAO Y. Dynamic identity authentication key agreement protocol based on extended chaos mapping[J]. Journal of Chengdu University of Technology (Science & Technology Edition), 2021, 48(4): 505-512.

[28] 张昱, 孙光民, 翟鹏, 等. 一种基于切比雪夫混沌映射的可证明安全的溯源认证协议[J]. 信息网络安全, 2022(12): 25-33.
ZHANG Y, SUN G M, ZHAI P, et al. A provably secure traceability authentication protocol based on Chebyshev chaotic map[J]. Netinfo Security, 2022(12): 25-33.

[29] HOLDEN A V. Chaos[M]. Course Book. Princeton, NJ: Princeton University Press, 2014.

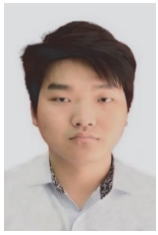
[30] 王振宇, 郭阳, 李少青, 等. 面向轻量级物联网设备的高效匿名身份认证协议设计[J]. 通信学报, 2022, 43(7): 49-61.
WANG Z Y, GUO Y, LI S Q, et al. Design of efficient anonymous identity authentication protocol for lightweight IoT devices[J]. Journal on Communications, 2022, 43(7): 49-61.

[作者简介]

廖伟（1999– ），男，云南大学信息学院硕士生，主要研究方向为物联网安全、嵌入式系统开发。

何乐生（1977– ），男，博士，云南大学信息学院副教授，主要研究方向为嵌入式系统及物联网应用、微弱信号采集和处理及其在生物电信号和射电天文信号处理等方面的应用。

尹恒（1999– ），男，云南大学信息学院硕士生，主要研究方向为嵌入式系统开发、物联网安全。



余圣涛（1997– ），男，云南大学信息学院硕士生，主要研究方向为图像加密、物联网安全。

权家锐（1999– ），男，云南大学信息学院硕士生，主要研究方向为多模态目标跟踪、神经网络。