面向ZigBee网络节点安全定位的消息签名方案

黄一才 李森森* 鲍博武 郁 滨
(信息工程大学 郑州 450001)

摘 要：针对ZigBee网络节点定位中消息的安全性问题，该文提出一种带隐私保护的消息签名方案。方案基于椭圆曲线(ECC)上的无双线性对运算，设计了带身份隐私保护的定位请求消息签名算法和坐标隐私保护的定位参照消息签名算法。理论证明了所提方案可抵御伪造攻击、重放攻击等多种外部攻击，同时具备隐私保护、身份追踪等功能。性能分析结果表明，与同类方案相比，所提方案计算开销和通信开销均具有优势。

关键词：安全定位；ZigBee；消息签名；外部攻击；接收信号强度指示
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2019)03-0702-07
DOI: 10.11999/JEIT180064

Message Signature Scheme for ZigBee Network Security Positioning

HUANG Yicai LI Sensen BAO Bowu YU Bin
(*PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: In view of the security of message in ZigBee network node location, a message signature scheme with privacy protection is proposed. The proposed scheme is based on Elliptic Curve Cryptosystem (ECC) without bilinear pairing, and location request message signature algorithm with identity privacy protection and location reference message signature algorithm with coordinate privacy protection are put forward. It is proved theoretically that the proposed scheme can not only resist the various external attacks, such as forgery attack, replay attack, etc., but also has the function of privacy protection and identity tracking. Performance analysis shows that the proposed scheme has the advantages of computing overhead and communication overhead over similar schemes.

Key words: Secure location; ZigBee; Message signature; External attack; Received Signal Strength Indicator (RSSI)

1 引言

节点定位技术是当前ZigBee技术领域的一个研究热点，节点位置信息在工业控制、战场环境监测、智能家居及医疗等领域具有重要意义[1]。ZigBee网络节点定位可以分为基于距离的(rang-based)和距离无关的(rang-free)定位方法。基于距离的定位方法常见的有TOA[2], DTOA[3], AOA[4]和RSSI[5]等；距离无关的定位方法主要有DV-Hop[6], APIT[7], Fingerprinting[8]等。其中，基于RSSI的定位方法因不需要增加额外的硬件设施，被广泛应用于无线定位。

外部攻击是一种常见的定位攻击，其主要特征是无需获得网络的信任参数，直接对定位过程实施攻击。外部攻击普遍存在于基于RSSI的定位网络中，比较常见的外部攻击方式包括：(1)在物理层和链路层采用反射、阻挡和削弱等手段破坏RSSI的准确性[9]；(2)在网络层使用伪造、重放、虫洞等攻击手段制造错误的参考坐标或RSSI[10]。外部攻击对基于RSSI的ZigBee网络造成两个显著的安全威胁。一方面，外部攻击者将恶意数据包发送给网络中的合法节点，若合法节点不具备对数据包合法性的验证能力，将这些数据包携带的信息存储下来，并运用于下一步的位置计算过程中，不仅会估算出错误的位置结果，甚至还可能无法完成定位。另一方面，外部攻击者向网络发送干扰电磁信号，迫使信号传播损耗模型失效，合法节点无法通过RSSI值推算出正确的信号传播距离，导致定位失败。

时间限制、空间限制、安全编码等非密码技术早已被用于解决外部攻击带来的安全威胁，但非密码技术对网络假设条件和节点配置要求都较高。例如，Capkun等人[11]提出的VM算法要求节点具备纳

收稿日期：2018-01-17；改回日期：2018-11-29；网络出版：2018-12-07
*通信作者： 李森森 lss589@163.com
基金项目：信息保障技术重点实验室开放基金(KJ-15-104)
Foundation Item: The Key Laboratory of Information Assurance Technology Open Fund (KJ-15-104)

秒级数据处理能力，SeRLoc[12]要求信标节点配置测量精确的定向天线，SeRLA[9]要求网络中所有节点具备频移键控调制能力。ZigBee的低功耗低成本要求使得节点的计算能力和配置都十分有限，如CC2430，因此非密码技术方案的前提条件是ZigBee网络难以满足的。

基于密码技术的方案主要采用加密、认证等手段来保证节点身份的合法性。文献[10]采用了对称加密算法，依据是否能够正常解密RSSI值密文，识别非法节点，进而达到安全定位的效果。但方案中先采集RSSI值再进行验证的方式使得方案的效率较低。文献[13]针对伪装攻击，提出一种基于对称密码算法进行节点身份合法性识别的认证方案，但是方案无法抵御复制攻击和重放攻击，并且该方案所需的计算开销较大。文献[14]提出一种基于哈希函数的节点双向身份认证方案，但方案的认证过程需要可信第三方的参与，并不适用于两层网络结构的ZigBee定位网络。文献[15]针对定位系统整体的安全性问题，提出一种适用于节点对的身份认证方案，但方案基于双线性对的椭圆曲线算法，计算复杂度比较高，不适用于低功耗要求的ZigBee网络。文献[16]提出了一种无证书签名方案，方案无需使用高计算复杂度的双线性对运算，但该方案无法提供匿名性、可追踪性和隐私保护功能，且无法抵御重放攻击。文献[17]针对车联网身份认证问题，提出了一种基于椭圆曲线的消息认证方案，但该方案无法提供隐私保护功能。

针对ZigBee网络节点定位中消息的安全性问题，本文提出基于无双线性对运算的消息签名方案。方案考虑盲节点和信标节点的不同安全需求，分别设计了带身份隐私保护的定位请求消息签名与验签算法和坐标隐私保护的定位参照消息签名与验签算法。在随机预言机模型下证明方案的安全性，并对方案的性能进行分析。

2　系统模型

本文方案的系统模型如图1所示。模型中主要包含4种角色，分别是可信中心、信标节点、盲节点和攻击节点，其中攻击节点根据实施手段的不同，分为I类攻击节点、II类攻击节点和III类攻击节点。

(1)可信中心：网络的中心节点，负责组建网络，是网络中信标节点和盲节点的父节点，并且计算系统参数和分配节点私钥。

(2)信标节点：网络部署前已预置坐标，作为定位参照消息的提供者，使用私钥对定位参照消息进行签名传输至盲节点。

(3)盲节点：网络中的待定位节点，通过向信标节点广播定位请求消息开启网络定位功能，并且利用私钥进行匿名性的定位请求消息签名。

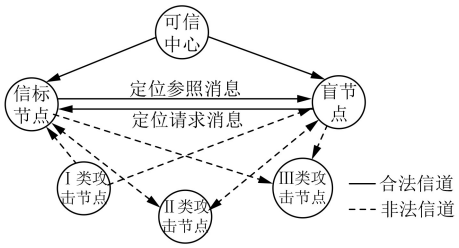

图 1 系统模型图

(4)I类攻击节点：通过伪造、随机插入等手段，将非法数据包发送给信标节点和盲节点。

(5)II类攻击节点：通过截获信标节点或盲节点发送的数据包，解析并更改数据包的内容和格式，然后使用更大或更小的功率重新发送非法数据包。

(6)III类攻击节点：截获定位消息数据包，窃取其中的隐私数据。

模型假设：

(1)网络中所有节点保持双向通信，且可信中心具备较强的计算能力和充足的能量供应；

(2)盲节点的邻居信标节点数目均满足定位要求(即数目大于3)；

(3)信标节点和盲节点间保证时间同步。

3　消息签名方案

本文消息签名方案流程如图2所示。方案包含3个部分，分别是系统初始化、节点注册和消息签名与验签。系统初始化中可信中心生成并公布系统参数；节点注册部分完成盲节点和信标节点私钥的分配；消息签名与验签部分中盲节点广播定位请求消息，信标节点向盲节点发送定位参照消息。

3.1　系统初始化

C选取有限域F_p上的一条椭圆曲线E/F_p，群$E(F_p)$中的一个点P，P的阶q和由P生成的加法群G，其中p为一个大素数，$E(F_p)$为椭圆曲线E/F_p上的点和无穷远点构成的群，q足够大；然后随机选择系统私钥$s \in Z_q^*$，计算系统公钥$P_u = sP$；接着选择3个散列函数：$H_1 : G \to Z_q^*, H_2 : \{0,1\}^* \times G \to Z_q^*, H_3 : G \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \to Z_q^*$

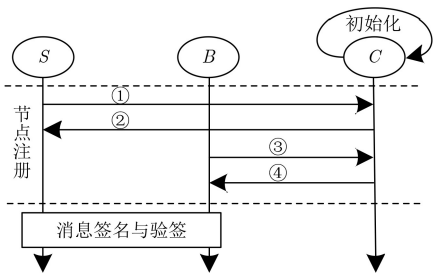

图 2 消息签名方案流程图

$\to Z_q^*$；最后公布系统参数$\langle E/F_p, q, G, P, P_u, H_1, H_2, H_3\rangle$。

3.2 节点注册

(1)S获取身份标识ID_i，随机选取$D_i \in Z_q^*$作为秘密值，通过安全信道将(ID_i, D_i)传递给可信中心C；

(2)C计算$R_i = D_i \cdot P$，$\mathrm{PD}_i = D_i \cdot P_u$，$h_{\mathrm{ci}} = \mathrm{ID}_i \oplus H_2(\mathrm{PD}_i, R_i)$，$x_i = D_i + h_{\mathrm{ci}} s \bmod q$，其中$(R_i, x_i)$作为盲节点$\mathrm{ID}_i$的私钥，通过安全信道将私钥传递给$S$；

(3)B获取身份标识ID_j，通过安全信道传递至可信中心C；

(4)C随机选取$r_j \in Z_q^*$，然后计算$R_j = r_j \cdot P$，$h_{cj} = H_2(\mathrm{ID}_j, R_j)$，$x_j = r_j + h_{cj} s \bmod q$，其中，$(R_j, x_j)$作为信标节点$\mathrm{ID}_j$的私钥，并通过安全信道将私钥和$\mathrm{PD}_i$传递给$B$。至此，$S$和$B$均注册完成，分别获得$(R_i, x_i)$和$(R_j, x_j, \mathrm{PD}_i)$。

3.3 消息签名与验签

消息签名与验签部分具体消息流如图3所示，包括定位请求消息签名、定位请求消息验签、定位参照消息签名和定位参照消息验签。

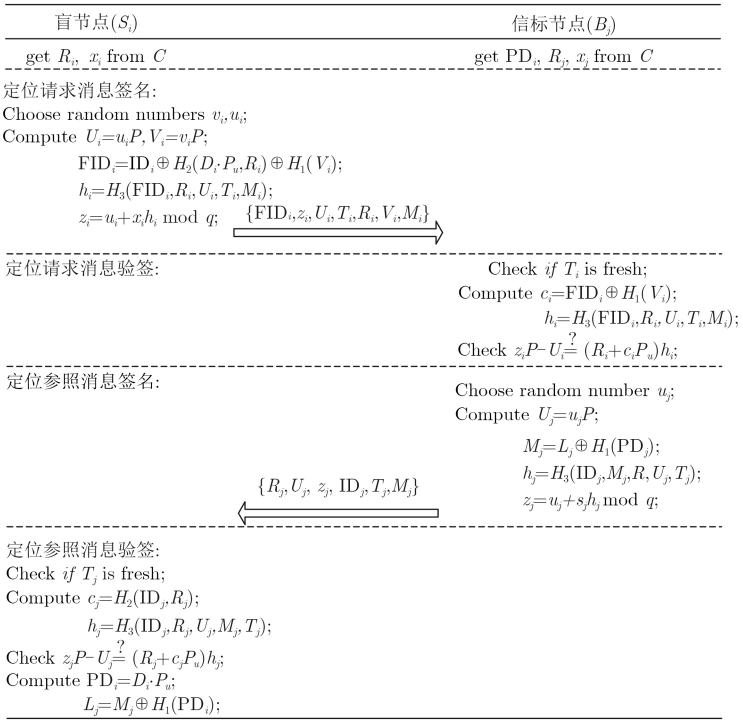

图 3 消息签名与验签消息流

(1)定位请求消息签名：S随机产生$v_i, u_i \in Z_q^*$和时间戳T_i，然后计算$V_i = v_iP$，$U_i = u_iP$，$\mathrm{FID}_i = \mathrm{ID}_i \oplus H_2(D_i \cdot P_u, R_i) \oplus H_1(V_i)$，接着计算定位请求消息$M_i$的摘要值$h_i = H_3(\mathrm{FID}_i, R_i, U_i, T_i, M_i)$，再使用自己的私钥进行签名$z_i = u_i + x_ih_i \bmod q$，最后广播签名后的数据包$\{\mathrm{FID}_i, z_i, U_i, R_i, T_i, V_i, M_i\}$。

(2)定位请求消息验签：B当收到信息$\{\mathrm{FID}_i, z_i, U_i, R_i, T_i, V_i, M_i\}$后，首先判断时间戳$T_i$是否新鲜，若不新鲜则判定验签不通过，否则计算$c_i = \mathrm{FID}_i \oplus H_1(V_i)$，$h_i = H_3(\mathrm{FID}_i, R_i, U_i, T_i, M_i)$，然后验签等式$z_iP - U_i = (R_i + c_iP_u)h_i$是否成立，若成立则验签成功，进入定位参照消息签名阶段；否则拒绝定位请求。

(3)定位参照消息签名：B提取自己的坐标L_j，随机选择$u_j \in Z_q^*$，计算$U_j = u_j \cdot P$，$M_j = L_j \oplus H_1(\mathrm{PD}_i)$，然后计算定位参照坐标数据的摘要值$h_j = H_3(\mathrm{ID}_j, M_j, U_j, R_j, T_j)$，再使用自己的私钥进行签名$z_j = u_j + x_jh_j \bmod q$，最后通过安全信道向$S$单播签名后的消息$\{R_j, U_j, z_j, \mathrm{ID}_j, T_j, M_j\}$。

(4)定位参照消息验签：S获得签名消息$\{R_j, U_j, z_j, \mathrm{ID}_j, T_j, M_j\}$，然后判断时间戳$T_j$是否新鲜，若不新鲜则验签不通过，否则计算$c_j = H_2(\mathrm{ID}_j, R_j)$和$h_j = H_3(\mathrm{ID}_j, R_j, U_j, L_j, T_j)$，验签等式$z_jP - U_j = (R_j + c_jP_u)h_j$是否成立，若成立则验签通过，计算$\mathrm{PD}_i = D_i \cdot P_u$，$L_j = M_j \oplus H_1(\mathrm{PD}_i)$，存储定位参照坐标$L_j$；否则拒绝该定位参照消息。

4 安全性分析

引理1[18] (分叉引理) 设Γ是一个概率多项式时间图灵机，即在多项式时间内能以概率型图灵机

解决某个复杂问题。如果Γ能以不可忽略的概率找到一个有效签名，那么输入不同的随机预言机，它可以以同样不可忽略的概率找到两个有效签名，并且两者不一样。

定理 1　本文定位请求消息签名算法能够抵抗伪造攻击。

证明　假定攻击者A可以在多项式间内以不可忽略的优势解决ECDLP困难问题。攻击者A输入挑战游戏的系统公钥$P_u=\varphi P$，其目标是计算出私密保存的私钥φ。A利用程序B充当解决ECDLP困难问题的游戏挑战者，A调用B进行以下游戏。

系统初始化。挑战者B定义系统公钥$P_u=\varphi P$，秘密保存系统私钥φ，生成系统参数：$\langle E/F_p, q, G, P, P_u, H_1, H_2, H_3, H_4\rangle$并发送给攻击者A。挑战者B维护列表$l_1, l_2, l_3, l_{\rm sk}, l_{\rm ssig}$，用以跟踪攻击者A对预言机$H_1, H_2, H_3$、盲节点私钥和盲节点签名的查询。每个列表初始设置为空。

(1)H_1预言机查询：列表l_1的格式是$\langle V_i, h_1\rangle$。当A以消息$\{V_i\}$查询时，若列表l_1中存在相应的记录$\{V_i, h_1\}$，则将h_1返回给A。否则，B随机产生$h_1\in Z_q^*$，将记录$\{V_i, h_1\}$插入列表l_1中，并返回h_1给A。

(2)H_2预言机查询：列表l_2的格式是$\langle {\rm PD}, R, h_2\rangle$。当A以消息$\{D_i\}$查询时，计算$R_i=D_i\cdot P, {\rm PD}_i=D_i\cdot P_u$，若列表$l_2$中存在相应的记录$\langle {\rm PD}_i, R_i, h_2\rangle$，则将$h_2$返回给A。否则，B随机产生$h_2\in Z_q^*$，将记录$\langle {\rm PD}_i, R_i, h_2\rangle$插入列表$l_2$中，并返回$h_2$给A。

(3)H_3预言机查询：列表l_3的格式是$\langle {\rm FID}, R, U, T, h_3\rangle$。当A以消息$\{{\rm FID}_i, R_i, U_i, T_i\}$查询列表$l_3$时，若存在相应的记录$\{{\rm FID}_i, R_i, U_i, T_i, h_3\}$，则将$h_3$返回给A。否则，B随机产生$h_3\in Z_q^*$，将记录$\{{\rm FID}_i, R_i, U_i, T_i, h_3\}$插入列表$l_3$中，并返回$h_3$给A。

(4)私钥查询：列表$l_{\rm sk}$的格式为$\langle {\rm ID}, s_{\rm sk}\rangle$，A对给定身份${\rm ID}_i$查询其私钥时，有如下情况：

(a)当${\rm ID}_i={\rm ID}_I$(其中${\rm ID}_I$代表游戏挑战次数达到最大次数)时，挑战结束，退出游戏；

(b)当${\rm ID}_i\neq{\rm ID}_I$时，B随机产生$D_i, h_2\in Z_q^*$，计算$h_{\rm ci}={\rm ID}_i\oplus h_2, s_{\rm sk}=D_i+\varphi h_{\rm ci} \bmod q$，将$\langle {\rm ID}_i, s_{\rm sk}\rangle$添加到列表$l_{\rm sk}$中，同时将$s_{\rm sk}$返回给A。

(5)盲节点签名查询：攻击者A用$\{{\rm FID}_i, T_i\}$查询时，B随机选取$D_i, u_i, v_i\in Z_q^*$，则可以依据消息$\{V_i\}$进行H_1预言机查询得到h_1，依据消息$\{D_i\}$进行H_2预言机查询得到h_2，根据$\{{\rm FID}_i, R_i, U_i, T_i\}$进行$H_3$预言机查询得到$h_3$，根据身份$\{{\rm FID}_i\}$进行私钥查询得到$s_{\rm sk}$，则得到签名消息$z_i=u_i+s_{\rm sk}h_3 \bmod q$，并返回$\{{\rm FID}_i, U_i, T_i, V_i, z_i\}$给A。

根据引理1，攻击者A产生不同的h_1'，在多项式时间内重新获得另一个有效的签名消息$\{{\rm FID}_i, U_i, T_i, V_i, z_i'\}$。则两个签名消息满足

$$z_iP=U_i+(D_i\cdot P+{\rm FID}_i\oplus h_1\cdot\varphi\cdot P)h_3 \tag{1}$$

$$z_i'P=U_i+(D_i\cdot P+{\rm FID}_i\oplus h_1'\cdot\varphi\cdot P)h_3 \tag{2}$$

根据式(1)和式(2)可得$(z_i-z_i')\cdot P=({\rm FID}_i\oplus h_1-{\rm FID}_i\oplus h_1')\cdot h_3\cdot\varphi\cdot P$。

令$A=(z_i-z_i'), B=({\rm FID}_i\oplus h_1-{\rm FID}_i\oplus h_1')\cdot h_3$，则A得到$\varphi=AB^{-1} \bmod q$作为求解上述输入的ECDLP困难问题。由于在多项式时间内无法解决ECDLP困难问题，所以在这个游戏中攻击者是无法获胜的。假设不成立，命题得证。

定理 2　本文定位参照消息签名算法能够抵抗伪造攻击。

证明　给定一个ECDLP困难问题实例$P_u=\varphi P$，攻击者A的目标是计算出φ。同定理1的证明，A利用程序B充当解决ECDLP困难问题的游戏挑战者，A调用B进行挑战游戏。

系统初始化。挑战者B生成系统参数：$\langle E/F_p, q, G, P, P_u, H_1, H_2, H_3, H_4\rangle$并发送给攻击者A。挑战者B维护列表$l_2, l_4, l_{\rm bk}, l_{\rm bsig}$，用以跟踪攻击者A对预言机$H_2$, H_4，信标节点私钥和信标节点消息签名的查询。每个列表初始设置为空。

在此挑战游戏中，A进行H_2预言机查询与定理1证明过程中的一致。

(1)H_4预言机查询：列表l_4的格式是$\langle {\rm ID}, M, R, U, T, h_4\rangle$。当A以消息$\{{\rm ID}_i, L_i, R_i, U_i, T_i\}$查询列表$l_4$时，若存在相应的记录$\{{\rm ID}_i, M_i, R_i, U_i, T_i, h_4\}$，则将$h_4$返回给A。否则，B随机产生$h_4\in Z_q^*$，将记录$\{{\rm ID}_i, M_i, R_i, U_i, T_i, h_4\}$插入列表$l_4$中，并返回$h_4$给A。

(2)私钥查询：信标节点私钥列表$l_{\rm bk}$的格式为$\langle {\rm ID}, s_{\rm bk}\rangle$，给定身份$\{{\rm ID}_j\}$查询私钥时，有如下情况：(a)当${\rm ID}_j={\rm ID}_J$(其中${\rm ID}_J$代表游戏挑战次数达到最大次数)时，挑战结束，退出游戏。(b)当${\rm ID}_j\neq{\rm ID}_J$时，B随机产生$r_i, h_2\in Z_q^*$，计算$s_{\rm bk}=r_i+\varphi h_2 \bmod q$，将$\langle {\rm ID}_i, s_{\rm bk}\rangle$添加到列表$l_{\rm bk}$中，同时将$s_{\rm bk}$返回给A。

(3)信标节点签名查询：当A以$\{{\rm ID}_j, T_j, M_j\}$查询时，B随机产生$r_j, u_j\in Z_q^*$，则$R_j=r_j\cdot P, U_j=u_j\cdot P$，进行相应预言机查询获得$h_2, h_4, s_{\rm bk}$，得到签名信息$\{{\rm ID}_j, T_j, M_j, R_j, U_j, z_j\}$返回给A。

同定理1证明过程，依据引理1, A在多项式时间内再次产生不同的h_2'，从而产生两个签名信息。

$$z_jP=U_j+(r_j\cdot P+h_2\cdot\varphi\cdot P)h_4 \tag{3}$$

$$z'_jP = U_j + (r_j \cdot P + h'_2 \cdot \varphi \cdot P)h_4 \tag{4}$$

根据式(3)和式(4)，得到$\varphi = \dfrac{z_j - z'_j}{(h_2 - h'_2)h_4} \bmod q$。同理，在多项式时间内无法解决ECDLP困难问题，假设不成立，命题得证。

推论 1 本文方案可抵抗伪造攻击、篡改攻击和重放攻击等外部攻击。

证明 采用反证法。假设攻击者能够实现伪造攻击，因而必须伪造满足验签等式$z_iP - U_i = (R_i + c_iP_u)h_i$的签名信息(盲节点与信标节点均适用)。在随机预言机模型下，攻击者要伪造一个签名信息必须解决一个ECDLP问题，与定理1和定理2矛盾，因此方案可抵抗伪造攻击。

若攻击者将签名信息$\{\mathrm{FID}_i, z_i, U_i, T_i, V_i\}$或$\{\mathrm{ID}_j, T_j, M_j, R_j, U_j, z_j\}$进行篡改，使得验证等式$z_iP - U_i = (R_i + c_iP_u)h_i$或$z_jP - U_j = (R_j + c_jP_u)h_j$成立。在攻击者不知道系统私钥$s$的情况下，攻击者无法计算出正确的盲节点或信标节点私钥，即无法使得验证等式成立。因此，本文方案可以抵抗篡改攻击。

方案中增加了时间戳T，验签时首先需要签证消息的新鲜性。若不新鲜，即拒绝消息。因此，方案可抵抗重放攻击。 证毕

推论 2 本文方案具备盲节点身份隐私保护和身份追踪功能。

证明 盲节点签名使用了假身份FID_i，假身份是由私密值D_i和随机数v_i产生的。$R_i = D_i \cdot P$，$V_i = v_iP$，$\mathrm{FID}_i = \mathrm{ID}_i \oplus H_2(D_i \cdot P_u, R_i) \oplus H_1(V_i)$，由于$v_i$是随机产生的，每次假身份$\mathrm{FID}_i$及签名信息是不相同的，前后并不关联。若攻击者想从假名$\mathrm{FID}_i = \mathrm{ID}_i \oplus H_2(D_i \cdot P_u, R_i) \oplus H_1(V_i)$中获取身份信息，则必须求解出$\mathrm{PD}_i$和$R_i$。依据定理1和定理2可知，由于攻击者在不知道系统私钥s的情况下，在多项式时间内无法完成解决ECDLP困难问题。因此，本文方案可提供身份隐私保护。

当可信中心C需要追踪发送定位请求信息的盲节点真实身份时，可根据$\mathrm{ID}_i = \mathrm{FID}_i \oplus H_1(V_i) \oplus H_2(s \cdot R_i, R_i)$得到盲节点真实身份。因此，本文方案可实现身份追踪功能。 证毕

推论 3 本文方案具备信标节点坐标隐私保护功能。

证明 可信中心为信标节点分配$\mathrm{PD}_i = D_i \cdot P_u$，其中包含盲节点的私密值$D_i$。信标节点计算$M_j = L_j \oplus H_1(\mathrm{PD}_i)$，从而对坐标$L_j$进行保护。在不知道盲节点私密值的情况下，基于单向散列函数的抗原像性和抗碰撞性，以及ECDLP困难问题，攻击者无法从M_j复原出坐标L_j。因此，方案提供信标节点坐标隐私保护功能。 证毕

表1是文献[16]、文献[17]的方案与本文方案在安全性方面的对比结果。文献[16]无法提供匿名性、可追踪性和隐私保护功能，并且无法抵御重放攻击。文献[17]的方案无法提供隐私保护功能。本文方案能够提供多种安全性功能，满足ZigBee定位网络的多种安全需求。

表 1 安全性能对比表

安全定位方案	可认证性	匿名性	身份追踪	抗伪造攻击	抗篡改攻击	抗重放攻击	隐私保护
文献[16]方案	√	×	×	√	√	×	×
文献[17]方案	√	√	√	√	√	√	×
本文方案	√	√	√	√	√	√	√

5 实验与性能分析

本节依据设计的消息签名方案在ZigBee CC2530硬件平台上进行定位仿真实验，对方案的计算开销和通信开销进行分析，并与文献[16]和文献[17]的方案进行对比。本文方案面向的是信标节点和盲节点所组成的节点对，因此性能分析过程中，均以节点对为分析对象。假定所有方案中加解密算法一样，分析过程不考虑加解密算法的计算开销。

实验仿真得到各节点进行定位时，签名验签的总时间如图4。可知，本文方案在时间开销上要优于文献[16]方案和文献[17]方案。

计算开销。表2是3种方案中ECC标量乘法运算T_{em}, ECC标量加法运算T_{ea}和单向散列运算次数的统计表。在文献[17]方案中，完成消息签名需要3次T_{em}和4次T_h；消息验签过程中主要包含3次ECC标量加法运算T_{ea}，3次T_{em}和3次T_h，以节点对为对

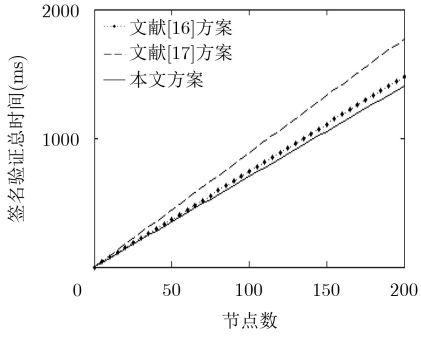

图 4 消息签名验签仿真曲线

表 2　复杂计算次数统计表

方案	签名过程	验签过程
文献[16]方案	$2\times(T_{\rm em}+T_h)$	$2\times(4T_{\rm em}+4T_{\rm ea}+T_h)$
文献[17]方案	$2\times(3T_{\rm em}+4T_h)$	$2\times(3T_{\rm em}+3T_{\rm ea}+3T_h)$
本文方案	$4T_{\rm em}+4T_h$	$2\times(3T_{\rm em}+2T_{\rm ea}+2T_h)$

象，因此总共有12次$T_{\rm em}$, 6次$T_{\rm ea}$和14次T_h。用同样的方法对文献[16]的方案进行分析，其总共有10次$T_{\rm ea}$, 8次$T_{\rm em}$和4次T_h。本文消息签名算法中，定位请求消息签名过程中有3次$T_{\rm em}$和3次T_h，验签过程中有3次$T_{\rm em}$, 2次$T_{\rm ea}$和2次T_h，定位参照消息签名过程中有1次$T_{\rm em}$和1次T_h，验签过程中有3次$T_{\rm em}$, 2次$T_{\rm ea}$和2次T_h，总共为10次$T_{\rm em}$, 4次$T_{\rm ea}$和8次T_h。

通信开销。设群G中元素所占字节数为40 Byte，时间戳T_i所占字节数为4 Byte，身份ID所占字节数为20 Byte，单向散列值字节数为20 Byte。在本文消息签名算法中，盲节点发送消息为$\{{\rm FID}_i, z_i, U_i, T_i, V_i, M_i\}$，其中，$U_i, V_i\in G$, ${\rm FID}_i, z_i\in z_q^*$和$T_i$是增加的通信开销，总量为$40\times2+20+20+4=124$ Byte。信标节点使用AES加密传输消息，AES是按128 Byte进行加密运算的，因此不考虑通信开销的额外增加量。依照同样的分析方法，文献[16]的方案增加的通信开销为100 Byte，文献[17]的方案增加的通信开销为124 Byte。

3种方案的性能分析结果如表3所示。从表3可知，与文献[16]方案相比，ECC的标量乘法运算持平，ECC的标量加法运算减少了50%，单向散列运算增加了75%，通信开销增加量高15%；与文献[17]方案相比，ECC的标量乘法运算和ECC的标量加法运算均下降2次，单向散列运算减少了50%，通信开销增加量两者一样。根据MIRACL库[19]中各种密码运算的执行时间统计结果，$T_{\rm em}=0.7358$ ms, $T_{\rm ea}=0.0040$ ms, $T_h=0.0002$ ms，因此本文方案中消息签名算法的计算开销更具有优势，通信开销与文献[17]相当，更适用于资源受限的ZigBee网络。

表 3　性能分析结果表

方案	ECC的标量乘法运算(次)	ECC的标量加法运算(次)	单向散列运算(次)	通信开销增加量(Byte)
文献[16]方案	10	8	4	100
文献[17]方案	12	6	14	124
本文方案	10	4	8	124

6　结束语

本文针对ZigBee网络定位过程中消息合法性验证问题，提出了一种无双线性对运算的消息签名方案。方案基于椭圆曲线离散对数问题，设计了带身份隐私保护的定位请求消息签名算法和坐标隐私保护的定位参照消息签名算法。安全性分析证明了方案能够抵御伪造、篡改、重放等外部攻击，满足ZigBee网络定位的安全需求。性能分析结果表明，方案在计算开销和通信开销比同类方案均具有一定的优势。

参 考 文 献

[1] 张扬勇. 基于ZigBee无线传感器网络RSSI定位算法[D]. [博士论文], 广东工业大学, 2015. doi: 10.7666/d.Y2795470.
ZHANG Yangyong. RSSI position algorithm in wireless sensor network based on Zigbee[D]. [Ph.D. dissertation], Guangdong University of Technology, 2015. doi: 10.7666/d.Y2795470.

[2] PAK J M, AHN C K, PENG S, *et al*. Distributed hybrid particle/FIR filtering for mitigating NLOS effects in TOA based localization using wireless sensor networks[J]. *IEEE Transactions on Industrial Electronics*, 2016, 64(6): 5182–5191. doi: 10.1109/TIE.2016.2608897.

[3] DIAZ S E, MARTIN A D C, and SALAS J G. HALO4: Horizontal angle localization and orientation system with 4 receivers and based on ultrasounds[J]. *Journal of Intelligent & Robotic Systems*, 2016, 82(3): 1–13. doi: 10.1007/s10846-015-0283-2.

[4] JUNG Y J, JEON M H, AHN J K, *et al*. Location estimation algorithm based on AOA using a RSSI difference in indoor environment[J]. *Journal of Advanced Navigation Technology*, 2015, 19(6): 558–563. doi: 10.12673/jant.2015.19.6.558.

[5] JIN Rencheng, CHE Zhiping, XU Hao, *et al*. An RSSI-based localization algorithm for outliers suppression in wireless sensor networks[J]. *Wireless Networks*, 2015, 21(8): 2561–2569. doi: 10.1007/s11276-015-0936-x.

[6] LI Yuanyuan. Improved DV-HOP location algorithm based on local estimating and dynamic correction in location for wireless sensor networks[J]. *International Journal of Digital Content Technology & Its Applications*, 2011, 5(8): 196–202.

[7] CHENG Wenhau, LI Jia, and LI Huaizhong. An improved APIT Location Algorithm for Wireless Sensor Networks[M]. Berlin: Springer, 2012: 113–119.

[8] 李华亮, 钱志鸿, 田洪亮. 基于核函数特征提取的室内定位算法研究[J]. 通信学报, 2017, 38(1): 158–167. doi: 10.11959/

j.issn1000-436x.2017018.

LI Hualiang, QIAN Zhihong, and TIAN Hongliang. Research on indoor localization algorithm based on kernel principal component analysis[J]. *Journal on Communications*, 2017, 38(1): 158–167. doi: 10.11959/j.issn1000-436x.2017018.

[9] 叶阿勇, 许力, 林晖. 基于RSSI的传感器网络节点安全定位机制[J]. 通信学报, 2012, 33(7): 135–142. doi: 10.3969/j.issn.1000-436X.2012.07.017.

YE Ayong, XU Li, and LIN Hui. Secure RSSI-based node position mechanism for wireless sensor networks[J]. *Journal on Communications*, 2012, 33(7): 135–142. doi: 10.3969/j.issn.1000-436X.2012.07.017.

[10] 詹杰, 刘宏立, 刘大为, 等. 无线传感器网络中DPC安全定位算法研究[J]. 通信学报, 2011, 32(12): 8–17. doi: 10.3769/j.issn.1000-436x.2011.12.002.

ZHAN Jie, LIU Hongli, LIU Dawei, *et al*. Research on secure DPC localization algorithm of WSN[J]. *Journal on Communications*, 2011, 32(12): 8–17. doi: 10.3769/j.issn.1000-436x.2011.12.002.

[11] CAPKUN S and HUBAUX J P. Secure positioning in wireless networks[J]. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): 221–232. doi: 10.1109/JSAC.2005.861380.

[12] LAZOS L and POOVENDRAN R. SeRLoc: Robust localization for wireless sensor networks[J]. *ACM Transactions on Sensor Networks*, 2005, 1(1): 73–100. doi: 10.1145/1077391.1077395.

[13] 靖刚, 吴俊敏, 徐宏力, 等. 基于对称密码的无线传感器网络安全定位[J]. 计算机工程, 2009, 35(12): 117–119. doi: 10.3969/j.issn.1000-3428.2009.12.041.

JING Gang, WU Junmin, XU Hongli, *et al*. Secure localization based on symmetric cryptography in wireless sensor networks[J]. *Computer Engineering*, 2009, 35(12): 117–119. doi: 10.3969/j.issn.1000-3428.2009.12.041.

[14] 李鹏, 王晓艳, 王汝传, 等. 一种基于哈希双向认证的无线传感网络定位安全方法[P]. 中国专利, CN104507082A, 2015.

LI Peng, WANG Xiaoyan, WANG Ruchuan, *et al*. Secure localization based on bidirectional hash authentication in wireless sensor networks[P]. China Patent, CN104507082A, 2015.

[15] 黄晓, 程宏兵, 杨庚. 基于身份的无线传感器网络定位认证方案[J]. 通信学报, 2010, 31(3): 115–122. doi: 10.3969/j.issn.1000-436x.2010.03.017.

HUANG Xiao, CHENG Hongbing, and YANG Geng. Identity-based authentication localization scheme for wireless sensor network[J]. *Journal on Communications*, 2010, 31(3): 115–122. doi: 10.3969/j.issn.1000-436x.2010.03.017.

[16] 王圣宝, 刘文浩, 谢琪. 无双线性配对的无证书签名方案[J]. 通信学报, 2012, 33(4): 93–98. doi: 10.3969/j.issn.1000-436X.2012.04.013.

WANG Shengbao, LIU Wenhao, and XIE Qi. Certificateless signature scheme without bilinear pairings[J]. *Journal on Communications*, 2012, 33(4): 93–98. doi: 10.3969/j.issn.1000-436X.2012.04.013.

[17] 吴黎兵, 谢永, 张宇波. 面向车联网高效安全的消息认证方案[J]. 通信学报, 2016, 37(11): 1–10. doi: 10.11959/j.issn.1000-436x.2016211.

WU Libing, XIE Yong, and ZHANG Yubo. Efficient and secure message authentication scheme for VANET[J]. *Journal on Communications*, 2016, 37(11): 1–10. doi: 10.11959/j.issn.1000-436x.2016211.

[18] POINTCHEVAL D and STERN J. Security proofs for signature schemes[C]. Advances in Cryptology — EUROCRYPT'96, Berlin, Germany, 1996: 387–398.

[19] MIRACL library on Certivox.com[OL]. https://www.certivox.com/miracl, 2018.

黄一才：男，1985年生，讲师，研究方向为无线网络安全.

李森森：男，1993年生，助教，研究方向为无线网络安全和蓝牙技术.

鲍博武：男，1994年生，硕士生，研究方向为无线网络安全和蓝牙技术.

郁 滨：男，1964年生，教授，博士生导师，研究方向为无线网络安全和视觉密码.