一种混合轻量型无线传感器网络公钥密码方案

郭 萍[1,2] 张 宏[1] 傅德胜[2] 周 未[1,3]
(南京理工大学计算机科学与技术学院 南京 210094)[1]
(南京信息工程大学计算机与软件学院 南京 210044)[2]
(中国人民解放军驻南京大桥机器厂 南京 211104)[3]

摘 要 将基于身份的公钥机制与轻量级CA(Certificate Authority)思想相结合,构建了一个基于身份及轻量级CA混合模型的传感器网络密码方案。该方案既克服了基于身份公钥机制中的第三方密钥托管问题,又简化了基于传统证书机制中产生、验证及管理公钥的复杂性。分析表明,方案可使公钥产生轻量化,公钥验证轻量化,密钥管理无需证书,且安全性高,可抵御无线环境下易于实施的多种攻击,适用于保障资源受限的无线网络中数据的机密性、完整性和不可否认性。

关键词 无线网络安全,无线传感器网络(WSN),基于身份,轻量级CA
中图法分类号 TP393 **文献标识码** A

Hybrid and Lightweight Cryptography for Wireless Sensor Network

GUO Ping[1,2] ZHANG Hong[1] FU De-sheng[2] ZHOU Wei[1,3]
(School of Computer Science & Technology, Nanjing University of Science & Technology, Nanjing 210094, China)[1]
(School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing 210044, China)[2]
(Machinery Plant Stationed in Nanjing Daqiao, People's Liberation Army of China, Nanjing 211104, China)[3]

Abstract Combined identity-based system with the idea of lite-CA(Certificate Authority), a scheme of identity-based and lightweight CA-based cryptography for wireless sensor network was proposed. The scheme not only avoids the drawback of private key escrow in the identity-based system, but also gains the advantage of simplifying complication of producing and verifying public key in traditional certificate-based CA system. Analysis shows that the scheme equips with characteristics of lite-producing public key, lite-verifying public key, certificate less, and high security which can defense some attacks easily carrying into wireless environment. It is applicable to be used in wireless network to gain data confidentiality, integrity, and non-refutation.

Keywords Wireless network security, Wireless sensor network(WSN), Identity-based, Lite-CA

无线网络的开放性、移动性、易受攻击性导致其安全性很难保障,因此认证、签名及加密等技术的运用非常重要。公钥密码在密钥分发、管理等方面有着秘密密码无与伦比的优越性,近年来公钥密码在无线环境中的应用得到广泛研究[1-9]。

公钥密码系统的实现主要有以下4种方式。(1)公钥证书密码系统[1,2]。用户通过CA(Certification Authority)产生一对公/私钥,CA颁发经其签名的公钥证书,将公钥和相应私钥的拥有者信息绑定在一起。CA负责管理该域内所有实体的公钥证书,包括证书的申请、发布、更新、撤销、存储等。CA的复杂性,往往成为制约PKI(Public Key Infrastructure)高效实现的瓶颈。(2)基于身份的(Identity-based)密码系统[3-5]。即用户的公钥,也是用户的身份,它可以是任何标识该用户的身份信息,例如IP地址、E-mail信息等;用户的私钥由一可信私钥生成中心(PKGC, Private Key Generator Center)产生,通过秘密通道给用户,这个过程相当于PKGC对用户的身份进行签名。因此,在基于身份的方案中没有证书,也不需要CA。PKGC默认拥有所有用户的私钥,即用户私钥被强制托管。(3)无证书(certificateless)密码系统[6,7]。在这种系统中,用户的私钥由两部分构成,一部分类似于基于身份方案中用户私钥的构成,由PKGC根据用户身份来产生;另外一部分则由用户自己选择。相应地,用户的公钥也由两部分构成,一部分是用户的身份,跟基于身份方案中公钥的构成一样;另外一部分是有关用户所选择的那部分私钥的一个零知识证明,这部分类似基于证书CA系统中用户的公钥,所不同的是此部分公钥不需要CA签名来绑定。无论是公钥还是私钥的产生均无需CA签名来绑定,所以这种系统能够贴上"无证书"标签。但是无证书系统中的第二部分公钥没有经过CA的签名来绑定,也使得所谓的"替换公钥"攻击成为可能,因此其顽健性较差。(4)轻量级CA(lite-CA based)公钥密码系统[8,9]。私钥完全由用户自己选择,但是其公钥分为两部

到稿日期:2011-05-15 返修日期:2011-07-28 本文受国家自然科学基金青年基金(60903027)资助。
郭 萍(1973-),女,博士生,讲师,主要研究方向为无线网络安全、无线网络加密认证技术,E-mail:ziyyou@yeah.net;张 宏(1956-),男,教授,博士生导师,主要研究方向为数据挖掘、无线网络安全;傅德胜(1951-),男,教授,博士生导师,主要研究方向为信息安全、网络安全。

分，一部分是其私钥的某个单向变换，另外一部分是可信第三方 CA 对用户身份和第一部分公钥的签名。此设想跟基于证书 CA 系统的联系和区别是[9]：第二部分公钥类似于传统 CA 系统中的证书，但是对证书的管理不是集中式的，而是分散式的，即由各个用户自己负责，因此也无需 CA，这正是轻量级 CA 名称的由来。轻量级 CA 密码系统与无证书密码系统的共同点是：二者均避免了强制密钥托管问题，也都不是基于身份的方案。二者的区别是：前者的证书（即第二部分公钥）是显式的，可以抵抗“替换公钥”攻击；而后者的证书是隐式的，不能抵抗“替换公钥”攻击。

本研究工作将基于身份的公钥体制与基于轻量级 CA 公钥体制相结合，构建一种基于身份及轻量级 CA（Lite-CA）混合结构的公钥体制密码方案。该方案既有基于身份公钥体制下产生公钥的灵活方便，又克服了第三方私钥强制托管问题；既有轻量级 CA 对公钥与用户身份的绑定性，又避免了传统基于证书 CA 公钥体制下繁重的证书管理问题。该方案特别适用于资源受限、安全性脆弱的无线环境。现以无线传感器网络为例，详述本方案的具体算法步骤。

本文第 1 节介绍轻量级 CA 公钥密码系统的一般模型；第 2 节提出基于身份及轻量级 CA 混合结构无线传感器网络密码方案；第 3 节分析所提方案的性能及安全性；最后总结全文。

1 轻量级 CA 密码系统一般模型

采用文献[10]的模型，无需证书管理的轻量级 CA 加密系统是一个五元组 $\Pi=(G_i,E_P,S_P,E,D)$，其定义如下。

1. 产生 LCA 公/私钥算法 G_i：G_i 是由 LCA 执行的 G_{LCA} 算法，输入系统安全参数集 K，输出 LCA 的公/私钥对 (PK_{LCA},SK_{LCA})。

2. 产生用户主公钥及私钥算法 G_i：G_i 是由用户执行的 G_U 算法，输入系统安全参数集 K，输出用户的主公钥/私钥对 $(PK_U^{\{Master\}},SK_U)$，其中 $PK_U^{\{Master\}}$ 为主公钥。

3. LCA 产生用户辅公钥算法 E_P：E_P 是由 LCA 执行的算法，输入系统安全参数集 K，SK_{LCA}，及 $PK_U^{\{Master\}}$，ID_U，输出用户的辅公钥 $PK_U^{\{Slavery\}}$。

4. 产生全部公钥算法 S_P：S_P 是由用户执行的算法，输入系统安全参数集 K，SK_{LCA}，$PK_U^{\{Master\}}$，$PK_U^{\{Slavery\}}$，ID_U，输出用户最终公钥对 $(PK_U^{\{Master\}},PK_U^{\{Slavery\}})$，当且仅当 $(PK_U^{\{Master\}},ID_U)$ 经 LCA 合法签名。

5. 加密算法 E：E 是一个由任何想发送信息的发送者执行的加密算法，输入明文 $m\in M$，PK_{LCA}，$(PK_U^{\{Master\}},PK_U^{\{Slavery\}})$，得到输出密文 $c\in C$，当且仅当 $(PK_U^{\{Master\}},PK_U^{\{Slavery\}})$ 经验证是合法的，其中 $(PK_U^{\{Master\}},PK_U^{\{Slavery\}})$ 是接收方的公钥对。

6. 解密算法 D：D 是一个由接收方执行的解密算法，输入密文 $c\in C$ 及 SK_U，得到输出明文 $m\in M$，其中 SK_U 是接收方的私钥。

2 基于身份及轻量级 CA 混合结构传感器网络密码方案

有一类无线传感器网络（WSN）会长期部署在某处进行监控，以传回现场信息。如人体传感器网络（Body Sensor Network）如同穿在患者身上的衣服，实时收集患者的心率、脉搏、血压、体温等信息。假设这类传感器网络一直处于工作状态，收集现场数据，需要和有线网络交互以传输保存收集到的数据或对访问用户进行身份认证，只有授权用户才可以随时访问 WSN 以获得实时信息。本文把这类无线传感器网络称为监控无线传感器网络（MWSN）。在这种场景下，对权限的控制及隐私的保护具有严格的要求。同时，考虑到传感器的有限容量，这些信息应该能够定时传送到一个存储数据库中保存。

2.1 监控无线传感器网络（MWSN）中角色描述

1. LCA（Lite-CA，轻量级 CA）：基于证书模型下的可信权威中心，根据约定的语义检查用户的身份并为用户颁发部分公钥（即辅公钥）。在整个系统中负责对用户进行身份认证，以及为用户产生辅公钥，并将由用户自己产生的主公钥与由 LCA 产生的辅公钥绑定签名，既避免了基于身份公钥系统中私钥对被强制托管的缺陷，也避免了无证书系统中公钥与用户身份不能绑定而易受到公钥替换攻击。

2. 用户：用户可能要多次访问监控传感器网络，以获取相关数据进行分析。但是他只能访问他当班时 MWSN 的信息，其它时间无权访问。因此，方案改变基于身份公钥体制中公钥产生的依据——IP 地址或 email 信息，取而代之的是一串与时间及用户身份有关的字符串，如 $str_{user}=(Time_{date}\mid ID_{user})$。这样做的目的是，方便更换用户的公钥及与之相对应的私钥，因为 IP 地址或 email 信息可能是长期的信息；且私钥可以不和公钥同时生成，公钥主要用于身份认证，私钥只在需要时才根据相同的语义生成，这一切都由用户自己操作，避免了基于身份公钥体制中第三方私钥强制托管缺陷。

3. 传感器节点：设 SN_i（$i=1,2,\cdots,n$）代表传感器节点，当传感器节点之间需要通信时，根据语义 $str_{S_i}=(Time_{date}\mid ID_{SN_i})$ 执行相关算法产生一对公/私钥。公钥可以发布，传感器网络用 LCA 公钥对数据进行加密，并将其发送至存储数据库；传感器节点的公/私钥用于它们间及与用户间的通信交互及认证。

4. 存储数据库：考虑到传感器节点有限的存储能力，历史数据需要保存在存储数据库中。当有用户需要访问历史数据时，首先要经过 LCA 严格认证，经 LCA 将数据解密后，用其公钥对数据重新加密后传输给用户。因此存储点与 LCA 需要有线网络的支持，以保证强大的运算能力、存储能力，及实施有线网络中强大的安全措施，如防火墙、入侵检测、高级加密运算等。

由上所述，监控传感器网络系统结构如图 1 所示。

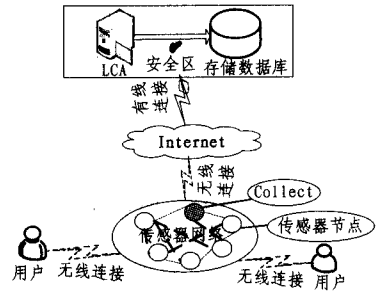

图 1 监控传感器网络结构图

2.2 系统参数说明及初始化

改进文献[11]中传感器网络公钥密码方案。LCA 初始

化系统的过程如下。

1. LCA 选取椭圆曲线群 $GF(p)$ 上的曲线 E，p 是大素数，P 是 E 的基点，而 q 也是一个大素数并且是 P 的生成元。

2. LCA 产生 n 个私钥 $x_1, x_2, \cdots, x_n \in GF(q)$，从而生成系统主私钥。$X=(x_1, x_2, \cdots, x_n)$。

3. 与之相对应，产生 n 个公钥组成系统主公钥 $Y=(y_1, y_2, \cdots, y_n)$，其中 $y_i=x_iP$，$1 \leqslant i < n$。

4. 最后，LCA 选择碰撞避免的单向哈希函数 $h:\{0,1\}^* \rightarrow \{0,1\}^n$，发布系统公共参数集 K 为 $\{Y,P,p,q,h(\cdot)\}$。

5. LCA 运行 G_{LCA} 算法，输入系统参数 $\{Y,P,p,q,h(\cdot)\}$，输出 LCA 的公/私钥对 (PK_{LCA}, SK_{LCA})。其中 $SK_{LCA}=\sum_{i=1}^{n} h_i(str_{LCA})x_i$，$str_{LCA}$ 是产生 LCA 公/私钥对的语义，$h_i(str_{LCA})$ 是 $h(str_{LCA})$ 的第 i 个比特；$PK_{LCA}=SK_{LCA}P=\sum_{i=1}^{n} h_i(str_{LCA})y_i$。

6. 用户执行 G_U 算法，输入系统安全参数集 $\{Y,P,p,q,h(\cdot)\}$，输出用户的主公钥/私钥对 $(PK_U^{(Master)}, SK_U)$。其中 $SK_U=\sum_{i=1}^{n} h_i(str_U)x_i$，$str_U$ 是产生用户主公钥/私钥对的语义，$h_i(str_U)$ 是 $h(str_U)$ 的第 i 个比特；$PK_U^{(Master)}=SK_UP=\sum_{i=1}^{n} h_i(str_U)y_i$。

7. 传感器节点执行 G_{SN_i} 算法，输入系统安全参数集 $\{Y,P,p,q,h(\cdot)\}$，输出传感器结点的主公钥/私钥对 $(PK_{SN_i}^{(Master)}, SK_{SN_i})$。其中 $SK_{SN_i}=\sum_{i=1}^{n} h_i(str_{SN_i})x_i$，$str_{SN_i}$ 是产生传感器结点的主公钥/私钥对的语义，$h_i(str_{SN_i})$ 是 $h(str_{SN_i})$ 的第 i 个比特；$PK_{SN_i}^{(Master)}=SK_{SN_i}P=\sum_{i=1}^{n} h_i(str_{SN_i})y_i$。

2.3 LCA 生成辅公钥并签名，得到全部公钥阶段

1. E_P 是由 LCA 执行的算法，输入系统安全参数集 $\{Y,P,p,q,h(\cdot)\}$，及 SK_{LCA}，$PK_U^{(Master)}$，ID_U，输出用户辅公钥 $PK_U^{(Slavery)}$。其中 $PK_U^{(Slavery)}=Sign_{SK_{LCA}}(ID_U \mid PK_U^{(Master)})$，即 LCA 对用户的主公钥及身份签名从而产生用户的辅公钥。

2. S_P 是由用户执行的算法，输入系统安全参数集 $\{Y,P,p,q,h(\cdot)\}$，及 PK_{LCA}，$PK_U^{(Master)}$，$PK_U^{(Slavery)}$，输出用户最终公钥 $(PK_U^{(Master)}, PK_U^{(Slavery)})$，当且仅当 $(PK_U^{(Master)}, ID_U)$ 经 LCA 合法签名。同理，根据以上二步，可以得到传感器节点的最终公钥 $(PK_{SN_i}^{(Master)}, PK_{SN_i}^{(Slavery)})$。

3. 用户通过零知识证明[12]向 LCA 表明拥有与 $PK_U^{(Master)}$ 相对应的私钥 SK_U。

经过以上 3 步，用户发布自己的公钥 $(ID_U, PK_U^{(Master)}, PK_U^{(Slavery)})$，同时保密其私钥 SK_U。

2.4 加密算法

1. 根据语义提取产生传感器节点 i 的辅公钥的任意串 str_{SN_i}，并产生随机数 n。

2. 根据 2.3 节所述步骤，传感器节点产生公钥对 $(ID_{SN_i}, PK_{SN_i}^{(Master)}, PK_{SN_i}^{(Slavery)})$，并发布公钥信息。

3. 传感器节点 i（数据源）计算 $m_1=(ID_{SN_i} \mid Time \mid n)$，其中 $Time$ 是加密数据的时间。与随机数 n 不同的是，$Time$ 可以是一个整点时间，为减少传感器与存储数据库之间的数据量，传输不是实时的，而是累积到一定的数据元组后才进行一次传输，例如早上九点十分与九点二十五分可能是一个 $Time$。

4. 传感器节点 i 计算 $m_2=(d \mid n)$，其中 d 是待加密数据。

5. 传感器节点 i（数据源）通过公告栏查询到邻居节点 j 的公钥对 $(ID_{SN_j}, PK_{SN_j}^{(Master)}, PK_{SN_j}^{(Slavery)})$，验证其公钥是否合法，检查 $PK_{SN_j}^{(Slavery)}$ 是否是 LCA 的合法签名，即 $PK_{SN_j}^{(Slavery)}=Sign_{SK_{LCA}}(ID_{SN_j} \mid PK_{SN_j}^{(Master)})$，用 LCA 的公钥对其进行解密得到 $(ID_{SN_j}, PK_{SN_j}^{(Master)})$，与传感器节点 j 的公开参数进行比对。

6. 节点 i 产生随机数 n'，用节点 j 的主公钥加密挑战消息 $(ID_{SN_i} \mid n')$，即 $M=(ID_{SN_i} \mid n')_{PK_{SN_j}^{(Master)}}$ 发送给节点 j；节点 j 收到消息后，同步骤 5 首先验证节点 i 的公钥是否合法。

7. 节点 i 计算 $c_1=E_{ECC}(m_1, PK_{LCA})$，计算 $c_2=E_{ECC}(m_2, PK_{LCA})$，其中 E_{ECC} 是椭圆曲线加密算法，即 LCA 的公钥对明文 (m_1, m_2) 加密得到密文 (c_1, c_2)；将元组 (c_1, c_2) 暂存在传感器内存中，同时将数据包 $SN_i \rightarrow SN_j$，如图 2 所示：$\{(c_1, c_2), SN_i, SN_j, Sig_{PK_{SN_j}^{(Master)}}((c_1, c_2) \parallel SN_i \parallel SN_j)\}$ 传输给邻居节点 j，$PK_{SN_j}^{(Master)}$ 是节点 j 的主公钥，节点 j 首先检验数据的完整性及节点 i 的合法性；再以同样方法与其邻居节点互相认证传递数据包，直到将数据包 $SN_{n-1} \rightarrow SN_{collector}$，如图 2 所示，传输到收集节点 $SN_{collector}$，其中 SN_{n-1} 是最后将数据传递给收集节点 $SN_{collector}$ 的节点。

8. 收集节点 $SN_{collector}$ 先验证数据包的完整性及对节点 SN_{n-1} 进行认证，收集节点定期将数据传输到存储数据库中进行长久保存，假设产生 t 个元组时，收集节点与存储数据库间进行一次数据传输 $\{(c_{11}^1, c_{21}^1), (c_{11}^2, c_{21}^2), \cdots, (c_{11}^t, c_{21}^t)\}$。

加密数据包传输过程如图 2 所示。

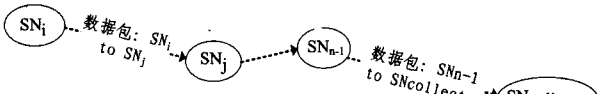

图 2 监控传感器网络加密数据包传输示意图

2.5 解密算法

2.5.1 用户直接向传感器节点请求实时数据

1. 假设用户已经过 LCA 的严格认证（认证过程如 2.3 节所述，即对用户主公钥签名过程）。

2. 用户请求当前实时传感器节点 SN_i 的监控信息，根据 2.3 节所述步骤，用户产生公钥对 $(ID_U, PK_U^{(Master)}, PK_U^{(Slavery)})$，并将其公开或直接传输给节点 i。

3. 双方经过如 2.4 节中第 5 步的认证，互相确认身份后，节点 i 使用用户的主公钥对 (m_1, m_2) 进行加密，其中 $m_{11}=(ID_U \mid Time \mid n')$，$n'$ 是节点 i 新产生的随机数，以防重放攻击，$c_{11}^i=E_{ECC}(m_{11}, PK_U^{(Master)})$；$m_{21}=(d \mid n')$，$c_{21}^i=E_{ECC}(m_{21}, PK_U^{(Master)})$。将新数据包 $\{(c_{11}^i, c_{21}^i), SN_i, SN_j, Sig_{PK_{SN_j}^{(Master)}}((c_{11}^i, c_{21}^i) \parallel SN_i \parallel SN_j)\}$ 传输给节点 i 的邻居节点 j。以此类推，最后由收集节点 $SN_{collector}$ 将数据包 $\{(c_{11}^i, c_{21}^i), SN_{collector}, ID_U, Sig_{PK_U^{(Master)}}((c_{11}^i, c_{21}^i) \parallel SN_{collector} \parallel ID_U)\}$ 传输给用户。

4. 用户首先通过 LCA 对收集节点 $SN_{collector}$ 的辅公钥的签名检查其是否合法，如果合法，则验证数据包完整性，并用自己的私钥进行解密：$m_{11}=D_{ECC}(c_{11}^i, SK_U)$，如果 $m_{11}=(ID_{SN_i} \mid Time \mid n')$ 中的节点信息及时间与用户所请求匹配，则继续解密 $m_{21}=D_{ECC}(c_{21}^i, SK_{SN_i})$，并检验 n' 与 m_{11} 中的 n' 是否一致。

通过以上 4 步，用户得到了所需要传感器节点的实时数据。

2.5.2 用户向存储数据库请求历史数据

1. 假设用户已经过 LCA 的严格认证。

2. 用户请求传感器节点 ID_{SN_i} 的历史监控信息，根据 2.3 节所述步骤，用户产生自己的公钥对（ID_U，$PK_U^{\{Master\}}$，$PK_U^{\{Slavery\}}$）并公开。

3. 对于(c_{11}^i, c_{21}^i)，$i \in t$，存储数据库传输给 LCA，LCA 用自己的私钥进行解密，即 $m_1 = D_{ECC}(c_{11}^i, SK_{LCA})$，如果 $m_1 = (ID_{SN_i} | Time | n)$中的节点信息及时间与用户所请求的相匹配，则 LCA 继续解密 $m_2 = D_{ECC}(c_{21}^i, SK_{LCA})$，并检验 n 与 m_1 中的 n 是否一致。

4. LCA 将使用用户的主公钥重新对(m_1, m_2)加密后传输给用户，同 2.5.1 步骤 3。

5. 同 2.5.1 节步骤 4。

通过以上 5 步，用户得到所需传感器节点的历史数据。

3 方案分析

3.1 方案特点

1. 基于身份产生公钥的轻量化

方案中私钥及主公钥由用户根据特定语义串产生，而基于身份公钥方案是以 Email、IP 地址等作为用户身份信息，这些信息通常不变，一旦生成公钥，就不许用户在同一组织内再申请公钥。方案中的特定语义串，如 $str = (Time_{date} | ID_{user})$，其含义是身份为 ID 的用户可以根据这个串变换时间产生主公钥，并且私钥可与主公钥不同时产生，而只在需要时根据生成主公钥的语义串及相关算法匹配产生。这比基于身份的方案更灵活，更简化，可认为是个轻量型基于身份的方法；同时该方案避免了传统基于证书公钥方案中证书管理的繁杂；本方案私钥及主公钥全部由用户产生，由 LCA 予以签名与用户身份绑定，解决了通常基于身份公钥方案中第三方密钥强制托管的问题。

2. 权威中心 CA 的轻量化

本方案中的用户及传感器节点的私钥及主公钥均由它们自己产生，为了避免主公钥遭到恶意第三方的替换攻击，同时也保证用户申明的公钥即是该用户的公钥而不是第三方未授权恶意攻击者的公钥，方案设计了一个轻量型的 LCA，对主公钥进行签名，产生一个与其主公钥相对应的辅公钥，即辅公钥是 LCA 对用户身份及主公钥的签名。可以通过验证 LCA 的签名来验证主公钥确实是申明者的公钥，同时又可以防止未授权第三方对主公钥的替换攻击，解决了无证书公钥方案中易遭受“替换公钥”攻击的缺陷。

3. 明文对及密文对的运用

明文成对出现，例如 $m_1 = (ID_U | Time | n)$，$m_2 = (d | n)$（参数示意详见 2.4 节），与之相对应，密文也成对出现。这样做的目的是，考虑到存储数据库可能是一个公共存储点，同时保存较多数据，即使是来自同一传感器网络的数据，由于连续采集现场信息，一段时间后数据量也非常大。当用户想提取保存在数据库中的数据时，发来的是一对密文(c_{11}, c_{21})，用户先解密 c_{11}，以判定（根据请求的节点及时间）是否是自己想要的数据，再决定是否解密数据量更大的 c_{21}。这里 c_{11} 相当于 c_{21} 的引擎，为 c_{21} 做个标记，以节约解密 c_{21} 的大计算量，同时随机数 n 能初步判定这对密文是否已遭到破坏。

3.2 性能分析

1. 优越性分析

本方案与文献[10,11]方案在公/私钥产生、管理等方面的对比分析结果如表 1 所列。

表 1 公/私钥产生及管理等方面的比较

	文献[10]方案	文献[11]方案	本方案
生成私钥方	用户	CA	用户
生成公钥方	用户和 CA	CA	用户和 CA
公钥维护模式	分布式	集中式	分布式
公钥认证模式	隐式	显式	隐式
公钥产生方式	基于证书方式	轻量型基于身份方式	轻量型基于身份方式
用户在同一组织内拥有公钥数量	不能很多	根据特定语义产生，理论上可很多	根据特定语义产生，理论上可很多
是否需要证书	否	是	否

表 1 显示本方案结合了文献[10]及文献[11]在公/私钥的产生、维护、分配、管理等方面的优点，既有传统基于证书模式下公钥与用户身份的绑定性，又避免了管理证书的繁杂；既有基于身份模式下公钥产生的轻量、方便，又避免了第三方密钥强制托管。

2. 计算性能分析

传感器节点的计算能力有限，算法的效率主要用算法执行过程中节点和用户所完成的各种计算来衡量。本方案中根据系统主公钥 $Y = (y_1, \cdots, y_n)$，进而产生用户主公钥 $PK_U^{\{Master\}}$ 的时间复杂度为 $O(n)$，用这个公钥执行加密操作的时间复杂度为 $O(1)$；同样，解密所需产生私钥的时间复杂度为 $O(n)$，用这个私钥执行解密算法的时间复杂度为 $O(1)$。文献[10]采用的是 RSA 加密方法，研究结果表明，椭圆曲线类型的算法在复杂性和安全性方面有一定的优势。密钥长度分别为 160bit 和 224bit 的椭圆曲线算法，与 RSA 1024bit 和 2048bit 的安全性相当[13]。因此，椭圆曲线类型的算法比通常的非对称密钥系统的计算成本要低。文献[11]虽然在产生公钥及加、解密的时间复杂度上与本方案一致，但是文献[11]采用传统基于证书的 CA 实现，系统的主公钥/私钥、用户的公钥/私钥、传感器节点的公钥/私钥都由 CA 产生，CA 是整个系统的单失效点，也是整个系统的瓶颈，极大影响了系统的安全性及效率。本方案 LCA 只负责对主公钥签名产生辅公钥，以便将用户或节点的主公钥与其身份绑定，辅公钥并不参与加解密，LCA 的重要性及工作复杂度比 CA 要小得多。

3.3 仿真实验分析

本节主要对基于混合模型的无线传感器网络密钥对的生成、签名、认证等进行仿真实验。计算机实验环境配置为 IBM 笔记本，主频 2.2 GHZ。仿真平台为 Tiny OS[14]，这是由美国加州大学开发的、目前国际上较为流行的无线传感器网络仿真平台，它基于组件的架构方式，能够快速实现无线传感器网络的仿真，可以实时监测网络状况，提供运行时的配置和调试。文献[10]采用 1024 bits RSA 算法，本方案采用 160 bits ECC 算法，实验结果如表 2 所列。

表 2 仿真实验比对

功能	文献[10]	本方案
公/私钥对生成	4708.3ms	33.8ms
签名	228.4ms	3.0ms
认证	12.8ms	10.7ms

文献[11]与本方案均采用 ECC 算法，不做单独比较；文献[10]与本方案加解密数据包及次数不一致，故只进行计算

（下转第 81 页）

[12] Lee J H, Song J S. TCP Aware Link Layer Agent for Seamless Vertical Handoff in the Cellular/WLAN Integrated Network [J]. Communications Letters, 2010, 14(11): 1017-1019

[13] Nkansah-Gyekye Y, Agbinya J I. Vertical Handoff Decision Algorithm for UMTS-WLAN[J]. Wireless Broadband and Ultra Wideband Communications, 2007: 37-37

[14] Zhang W, Wang J L. A Vertical Soft Handoff Scheme Based on SIP in the Ubiquitous Wireless Network [J]. Computer Sciences and Convergence Information Technology, 2009: 794-799

[15] Tao M, Yu H W. A smooth handoff scheme based on mSCTP for speed-aware application in mobile IPV6 [J]. Broadband Network & Multimedia Technology, 2009: 586-591

[16] Chen Y S, Chiu K L, Hwang R H. SmSCTP: SIP-based MSCTP Scheme for Session Mobility over WLAN/3G Heterogeneous Networks [C] // Proc. Wireless Communications and Networking Conference. 2007: 3307-3312

(上接第 72 页)

复杂度分析(见 3.2 节),不进行具体加、解密时间比对。

3.4 安全性分析

1. 窃听攻击:在这种攻击中,对手企图窃听在传感器与存储数据库间传输的元组(c_1, c_2)。因为所有数据都经过加密,所以对手无法获悉明文。

2. 跟踪攻击:对手通过跟踪获取用户隐私,如果已知元组(c_1, c_2),对手仅能知道来自同一传感器网络,无法获悉更多元组间的关系,因为每个密文中都有随机数 n,即使是由同一个公钥加密的两个元组的密文,它们之间也无法有确定的关系。

3. 替换攻击:如果攻击者想替换用户及传感器节点的主公钥,这是不可行的,因为主公钥经过 LCA 签名产生辅公钥,通信双方通过检查 LCA 签名来判定主公钥是否合法,且与相应辅公钥绑定。

4. 攻陷传感器:假如对手攻陷一个或多个传感器节点,即使它可以获取存储在传感器上的所有数据,对手也不能获取明文。因为这些数据是经用户或传感器的主公钥加密,除非对手可以破解椭圆曲线加密算法,并且知道用户与 LCA 间的零知识证明,才能破译(c_1, c_2),由椭圆曲线加密算法的难解性可知,这是不可行的。

5. 欺骗攻击:攻击者可以伪造($ID_{attacker}$, $PK_{attacker}^{(Master)}$, $PK_{attacker}^{(Slavery)}$),声称自己是合法用户,向用户或传感器节点要求数据。但是攻击者的 $PK_{attacker}^{(Slavery)}$ 没有经过 *LCA* 签名,即用 *LCA* 的公钥解密 $PK_{attacker}^{(Slavery)}$ 无法得到($ID_{attacker} \mid PK_{attacker}^{(Master)}$),因此很容易判定攻击者不是经 LCA 认证的合法用户。

6. 匹配攻击:攻击者可能也会使用不同的串组合,按照相同语义产生主公钥,但这个公钥没有经过 LCA 签名,因此无法拥有辅公钥;经用户或传感器节点的主公钥加密的元组(c_1, c_2),因为随机数 n 的存在,攻击者无法通过截获大量密文而用伪造的公钥试图用匹配法找出它们之间的关联。

结束语 无线传感器网络由于与固定网络和一般无线网络不同,有其自身的特征,因此为网络通信和信息安全提出新的挑战。本文结合基于身份的公钥机制及基于轻量级 CA 思想给出了一种应用于无线传感器网络的密钥建立、分配和加密签名一体化方法,并对其特点、计算复杂性和安全性进行了分析。理论及实验分析表明,方案具有产生公钥轻量化、公钥验证轻量化、密钥管理无需证书、安全性高,可抵御无线环境下易于实施的多种攻击,适用于资源受限的无线环境,为该类型的网络安全提供了新的解决方案。

参 考 文 献

[1] Malan D J, Welsh M, Smith M D. A public-key infrastructure for key distribution in TimyOS based on elliptic curve cryptography [A]// Proceedings of the 1st IEEE International Conference on Sensor and Ad hoc Communications and Networks[C]. 2004: 71-80

[2] Kohnfelder L M. Towards a practical public key cryptosystem [D]. Boston, MIT Department of Electrical Engineering, 1978

[3] Shamir A. Identity-based cryptosystems and signature schemes [A] // Advances in Cryptology-CRYPTO'84 [C]. Springer, 1985: 47-53

[4] Dang Lan-jun, Kou Wei-dong, Zhang Jun, et al. Improvement of mobile IP registration using self-certified public keys[J]. IEEE Transactions on Mobile Computing, 2007, 1(4): 167-173

[5] 杨庚,王江涛,程宏兵,等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报,2007,35(1):180-185

[6] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[A] // Advances in Cryptology-AsiaCrypt'03[C]. Springer, 2003: 452-473

[7] Jiang Yi-lin, Lin Chuang, Shen Xue-min, et al. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks[J]. IEEE Transactions on Wireless Communications, 2006, 5(9): 2569-2577

[8] Dong Xiao-lei, Wang Li-heng, Cao Zhen-fu. New public key cryptosystems with lite certification authority[EB/OL]. http://ePrint. iacr. org/2006/154, 2006

[9] 潘耘,王励成,曹珍富,等. 基于轻量级 CA 的无线传感器网络密钥分配方案[J]. 通信学报,2009,30(3):130-134

[10] Dong Xiao-lei, Wei Li-fei, Zhu Hao-jin, et al. EP²DF: An efficient privacy-preserving date-forwarding scheme for service-oriented vehicular Ad Hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(2): 580-591

[11] Tan Cu C, Wang Hao-dong, Zhong Sheng, et al. IBE-Lite: A lightweight identity-based cryptography for body sensor networks[J]. IEEE Transactions on Information Technology in Biomedicine, 2009, 13(6): 926-932

[12] Feige U, Flat A, Shamir A. Zero knowledge proofs of identity [J]. Journal of Cryptology, 1988, 1(2): 77-94

[13] Lauter K. The advantages of elliptic curve cryptography for wireless security[J]. IEEE Wireless Communications, 2004, 11(1): 62-67

[14] Watro R, Kong D, Cut I S, et al. TinyPK: securing sensor networks with public key technology[A] // Proceedings of the 2nd ACM work shop on Security of Ad hoc and Sensor Networks SASN'04[C]. New York, ACM Press, 2004: 59-64