一种新的基于双线性配对的无线传感网络密钥协商方案

陈 浩 郭亚军
(华中师范大学计算机科学系 武汉 430079)

摘 要 针对无线传感器网络密钥协商中安全性不足的问题,提出了一种适合无线传感器网络的密钥协商方案KASBP。该方案首先运用基于双线性配对的运算预置网络系统参数并通过计算获得节点的相关参数;然后节点向邻居节点广播,并利用Diffie-Hellman密钥交换技术,使节点间能够共享密钥。理论分析结果表明,KASBP方案的执行效率不仅优先于LZC和Shim-Woo的密钥协议方案,同时也符合"已知密钥安全""完美前向安全""密钥泄露安全""未知共享密钥安全""密钥支配安全"等安全需求。

关键词 密钥协商,双线性配对,密钥交换,密钥管理
中图法分类号 TP393.08 **文献标识码** A

Key Agreement Scheme Based on Bilinear Pairing for Wireless Sensor Network

CHEN Hao GUO Ya-jun
(Department of Computer Science, Hua Zhong Normal University, Wuhan 430079, China)

Abstract Considering the problem of inadequate security in wireless sensor networks, the paper proposed a key agreement scheme based on bilinear pairing for wireless sensor network. Firstly, the proposed scheme pre-distributed network system parameters using ID-based encryption algorithm and computed nodes' parameters on bilinear pairings. Then it broadcasted to networks and exchanged parameters between nodes and computed nodes' key using Diffie-Hellman key exchange technology. Analysis results show that the proposed scheme is not only more efficient than the previous LZC scheme and Shim-Woo scheme, but also satisfies all the required security attributes: implicit key authentication, known-key security, perfect forward secrecy, key-compromise impersonation resilience and unknown key-share resilience.

Keywords Key agreement, Bilinear pairing, Key exchange, Key management

1 引言

集成了传感器技术、微机电系统(Micro-electro-mechanical systems)技术、无线通信技术和分布式信息处理技术的无线传感器网络(Wireless Sensor Network,以下简称WSN),如图1所示,是当前信息技术的前沿之一,是当今的研究热点,受到了广泛的关注[1]。为保证传感器网络安全运行,防止恶意窃听网络通信,假冒合法节点向网络注入恶意信息,传感器节点间的通信信息应该加密,重要的网络数据必须经过有效认证。而要达到此目的,首先必须解决密钥分配问题,在相互通信的节点间建立会话密钥。由于传感器节点在能量、计算能力和通信带宽方面的限制,不宜采用一般意义上的公钥密码。寻找一种适合WSN的密钥协商方案是目前安全研究的热点,包括适合WSN的密钥协议的建立、存储、分配等相关问题。

对于无线传感器网络密钥协商的问题,尤其是在Boneh和Franklin提出双线性配对函数可以应用于以身份标识为基础的加密系统后[2],相关研究就迅速发展起来。

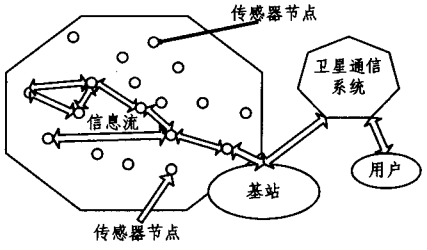

图1 一个典型无线传感器网络体系结构

在Joux第一次发表三方密钥协商之后,许多密钥协商方案就以此作为主要研究方向[3],但该协商方案面临中间攻击者的威胁。Al-Riyami和Paterson随后提出了基于个体身份标识的三方密钥协商方案[4]。Liu,Zhang和Chen三位学者在基于身份标识的基础上,提出了一套具有身份鉴别能力的三方密钥协商方案(以下简称LZC方案)[5]。而随后Shim和Woo两位学者指出,LZC方案无法抵挡未知共享密钥的攻击,并且针对此提出了一套更安全的密钥协商方案(以下简称Shim-Woo方案)[6]。

基于上述讨论,提出了一种在WSN中使用的密钥协商

到稿日期:2009-07-15 返修日期:2009-09-30 本文受国家自然科学基金项目(60773008),湖北省教育厅科研项目(B20094002),武汉市教育局科研项目(2008k075),华中师范大学"银桂计划"资助。

陈 浩(1982—),男,硕士生,主要研究方向为网络信息安全、无线网络信息安全等,E-mail:chenhao_1982@163.com;郭亚军(1966—),男,教授,主要研究方向为网络信息安全、P2P网络的可信计算等。

方案 KASBP，包括密钥协议及其建立、存储、分配及加、解密等具体步骤。第 2 节是相关研究，给出节定义以及说明；第 3 节是具体方案；第 4 节给出了与其他方案在复杂性、有效性和安全性方面的理论分析、比较；最后对全文进行了总结。

2 相关研究

2.1 双线性配对概念

定义 1（双线性配对）[3,5,9] 指两个循环群之间相对应的线性映射关系。其相关参数与符号如下：G_1 是阶数为大质数 q 的循环加法群，G_2 是阶数为大质数 q 的循环乘法群。双线性配对函数表示方式为 $\hat{e}:G_1\times G_1\to G_2$，且对于 $\forall P,Q\in G_1$ 与 $\forall a,b\in Z_p^*$，q 等参数满足下列特性：

- 双线性（Bilinearity）

$$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$$

$$\hat{e}(P_1+P_2,Q)=\hat{e}(P_1,Q)\,\hat{e}(P_2,Q)$$

$$\hat{e}(P,Q_1+Q_2)=\hat{e}(P,Q_1)\,\hat{e}(P,Q_2)$$

- 非退化性（Non-degeneracy）

若 P 是 G_1 的生成元，则 $\hat{e}(P,P)$ 也会是 G_2 的生成元，即 $\hat{e}(P,P)\neq 1$。

- 可计算性（Computability）

对于 $\forall P,Q\in G_1$ 而言，恒有一有效率的算法可在多项式时间内计算 $\hat{e}(P,Q)$。

2.2 难题假设

以下是针对本文中所要用的数学难题的详细定义和说明。

定义 2（离散对数难题，Discrete Logarithm Problem，简称 DLP） 令 $b\in Z_q^*$ 为未知数，给定一个大质数 n 和生成元 g，要求 $0\leqslant x\leqslant q-2$ 且满足 $g^x\equiv(b \bmod n)$，Z_q^* 代表基数为 q 的所有质数的集合。

定义 3（Diffie-Hellman 的求解计算难题，Computational Diffie-Hellman Problem，简称 CDHP） 令 $a,b\in Z_q^*$ 为未知数，给定 $P,aP,bP\in G_1$，要求 ab 且满足 $abP\in G_1$。

定义 4（Diffie-Hellman 计算平方难题，Square Computational Diffie-Hellman Problem，简称 SCDHP） 令 $a\in Z_q^*$ 为未知数，给定 $P,aP\in G_1$，要求 a^2 且满足 $a^2P\in G_1$。

对于以上数学难题，Bao 等学者已经证明，在求解上述难题的过程中，其困难程度是同样的[7]。

2.3 安全假设

国内外经过研究发现，一个密钥协商协系统必须符合下面 5 大安全特性[8]。

1）已知密钥安全

指当某一次的通信过程中，会话密钥泄漏，其它次所产生的会话密钥并不会因此而同时泄漏。已知密钥安全主要是将会话密钥泄漏所产生的安全危害局限在当次的通讯过程内。

2）完美前向安全

指即使一个或多个使用生命周期较长的会话密钥泄漏，但在此次泄漏之前所产生的会话密钥不会因此而连带泄漏。系统对于过去所有已被加密的数据具有保护功能，使攻击者无法因为此泄漏情况而推导出先前所产生的会话密钥。

3）密钥泄露安全

指当节点 A 的会话密钥不小心泄漏给了攻击节点。在攻击节点得到此会话密钥的情形之下，攻击节点只能模仿自己是节点 A 来欺骗其它节点，并无法模仿其它节点欺骗节点 A。

4）未知共享密钥安全

指当完成密钥协商后，节点 A 相信自己与节点 B 共享会话密钥，但节点 B 却和另一攻击节点建立了会话密钥。最后造成在节点 A 不知情的情况下与攻击节点也分享了此次会话密钥。因此，任何节点不可能在节点 A 不知道的情况下，而得到关于节点 A 的会话密钥。

5）密钥支配安全

指任何一次的会话密钥建立过程中，会话密钥的产生方式必须由节点之间共同合作建立。密钥控制安全主要是保护会话密钥的产生方式不能为单独一方所决定，以达到安全及公平的原则。

2.4 相关方案分析

从 Diffie 和 Hellman 发表第一个密钥交换方式以后，该协议就是广大学者研究的方向之一[11,12]。该密钥交换的方法虽然一直被改进，但还是容易遭受中间人攻击。假设 Alice 与Bob 进行密钥交换，而 Eva 作为攻击者，充当中间人的角色，Eva 选择一个随机数 z 对 Alice 的参数进行调换，然后传送给 Bob。而 Bob 无法识别从中间人传来的参数是否合法，同样的 Alice 也受到这样的欺骗，最后密钥被攻击。其过程如图 2 所示。

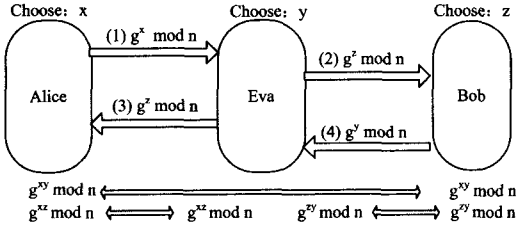

图 2 Diffie-Hellman 密钥协商中遭受中间人攻击

随后的发展中，密钥协议由之前的双方协商改为三方同时参与协商。2000 年，法国学者 Joux 提出仅一次信息交换就可完成三方密钥协商的方案。该方法将双线性配对函数与密码学紧密地结合起来，以完善密钥协商系统。但是，该方法因为不具备身份标识的能力，容易遭受攻击者的伪装攻击。针对此缺点，可以通过签证或者认证来增加系统的安全性。随后，Al-Riyami 和 Paterson 等学者又发表了进一步的改进方法[4,10,13]。

Liu，Zhang 和 Chen 三位学者在以基于身份的密码系统中，采用单项抗碰撞函数来对节点的身份标识进行加密，在一次通讯量的情况下，让三方完成协议，并且同时建立多把共享的会话密钥（简称 LZC 方案）。该方法融合了身份签证的设计概念，以达到对节点身份的鉴别，若攻击节点企图伪造一个合法的身份，对其它节点进行欺骗，将面临求解 Diffie-Hellman 计算问题的数学难题。

韩国学者 Shim 和 Woo 发表论文指出，LZC 方案无法抵挡未知密钥攻击。文章指出，在 LZC 方案中，攻击节点可以通过网络分别截取节点间公布的消息，然后利用自己的身份来冒充合法节点，躲过身份的鉴别而产生欺骗。因此提出了安全和效率都更好的 Shim-Woo 方案。而整个系统在最后的

认证阶段，采用的是 Diffie-Hellman 平方计算问题的假设。另一方面，LZC 协议没有采用单项抗碰撞函数运算，减少了计算量，却没有使安全性受到影响。

3 密钥协商

基于以上的讨论，提出了在 WSN 中使用的密钥协商方案 KASBP(a Key Agreement Scheme Based on Bilinear Pairing for Wireless Sensor Network)。下面给出方案的具体描述。

以下是本协商方案中使用到的系统参数定义：

KGC 为密钥产生中心

G_1 为循环加法群

G_2 为循环乘法群

q 为大质子数

P 为 G_1 的生成元

s 为 KGC 的私钥，$s\in Z_p^*$

P_{pub} 为 KGC 的公钥，$P_{pub}=sP$

H_1 为单项抗碰撞函数，$H_1:\{0,1\}^*\rightarrow G_1$

$\hat{e}$ 为双线性配对函数，$\hat{e}:G_1\times G_1\rightarrow G_2$

ID_i 为节点 i 的标识

Q_{ID} 为节点 i 的公钥，$Q_i=H_1(ID_i)$

S_{ID} 为节点 i 的私钥，$S_i=sQ_i$

A,B,C 为参与密钥协商的 3 个节点

$\{a,a'\},\{b,b'\},\{c,c'\}$ 为 A,B,C 所选择的随机安全参数

P_A,P_A',T_A 为 A 所广播的信息，其中，$P_A=aP,P_A'=a'P$，$T_A=S_A+aa'P_{pub}$

P_B,P_B',T_B 为 B 所广播的信息，其中，$P_B=bP,P_B'=b'P$，$T_B=S_B+bb'P_{pub}$

P_C,P_C',T_C 为 C 所广播的信息，其中，$P_C=cP,P_C'=c'P$，$T_C=S_c+cc'P_{pub}$

Step1 KGC 初始化

KGC 选择随机的安全参数 s，计算得出 $P_{pub}=sP$。此时，系统初始化完成，$\{s,P_{pub}\}$ 为 KGC 的密钥对。KGC 将所有参数广播$\langle G_1,G_2,P,P_{pub},q,H_1\rangle$。而安全参数 s 作为 KGC 的私钥保存。

Step2 节点注册

所有节点必须以自己的身份到 KGC 注册，才能产生其本身的一对密钥。首先，节点 i 将自己的身份标识 ID_i 发送给 KGC，KGC 产生$\{S_{ID},Q_{ID}\}$。其中，$Q_i=H_1(ID_i)$为节点 i 的公钥，$S_i=sQ_i$ 为节点 i 的私钥。KGC 会广播所有的公开密钥 Q_i。

Step 3 节点初始化

使用的 3 个节点分别用 A,B,C 来表示。其中，节点 A 的公钥为 $Q_A=H_1(ID_A)$；密钥为 $S_A=sQ_A$。节点 B 的公钥为 $Q_B=H_1(ID_B)$；密钥为 $S_B=sQ_B$。节点 C 的公钥为 $Q_C=H_1(ID_C)$；密钥为 $S_C=sQ_C$。3 个节点分别选择两个随机安全参数，分别表示为$\{a,a'\},\{b,b'\},\{c,c'\}$。

节点 A 计算出 $P_A=aP,P_A'=a'P,T_A=S_A+aa'P_{pub}$

节点 B 计算出 $P_B=bP,P_B'=bP,T_B=S_B+bb'P_{pub}$

节点 A 计算出 $P_C=cP,P_C'=c'P,T_C=S_C+cc'P_{pub}$

Step 4 节点间密钥协商

在节点 A,B,C 初始化完成以后，节点 A 向节点 B 和节点 C 公开(P_A,P_A',T_A)信息，同样地，节点 B,C 也分别对其它节点公布$(P_B,P_B',T_B),(P_C,P_C',T_C)$。用如下表达式表达：

$A->B,C\ (P_A,P_A',T_A)$

$B->A,C\ (P_B,P_B',T_B)$

$C->A,B\ (P_C,P_C',T_C)$

Step 5 验证密钥阶段

由于节点之间的关系是对等关系，取其中的 A 分析，即节点 A 在接受到 B,C 两个节点传来的信息后，就进行身份的验证[14]，即验证以下等式是否成立：

$$\hat{e}(T_B+T_C,P)=?=\hat{e}(Q_B+bb'P+Q_C+cc'P,P_{pub})$$

$$\hat{e}(T_A+T_C,P)=?=\hat{e}(Q_A+aa'P+Q_C+cc'P,P_{pub})$$

$$\hat{e}(T_A+T_B,P)=?=\hat{e}(Q_A+aa'P+Q_B+bb'P,P_{pub})$$

看上面的等式是否成立，具体验证过程如下：

$$\begin{aligned}\hat{e}(T_B+T_C,P)&=\hat{e}(TB,P)\,\hat{e}(TC,P)\\&=\hat{e}(S_B+bb'P_{pub},P)\,\hat{e}(S_C+cc'P_{pub},P)\\&=\hat{e}(sQ_B+sbb'P,P)\,\hat{e}(sQ_C+scc'P,P)\\&=\hat{e}(Q_B+bb'P,P)^s\,\hat{e}(Q_C+cc'P,P)^s\\&=\hat{e}(Q_B+bb'P,sP)\,\hat{e}(Q_C+cc'P,sP)\\&=\hat{e}(Q_B+bb'P,P_{pub})\,\hat{e}(Q_C+cc'P,P_{pub})\\&=\hat{e}(Q_B+bb'P+Q_C+cc'P,P_{pub})\end{aligned}$$

若发现上述等式成立，则标识验证通过，与节点 B 和节点 C 完成密钥协商，并计算出 8 把共享密钥，如下所示：

$K_{A1}=\hat{e}(P_B,P_C)^a$，$K_{A2}=\hat{e}(P_B,P_C')^a$，$K_{A3}=\hat{e}(P_B',P_C)^a$，$K_{A4}=\hat{e}(P_B',P_C')^a$，$K_{A5}=\hat{e}(P_B,P_C)^{a'}$，$K_{A6}=\hat{e}(P_B,P_C')^{a'}$，$K_{A7}=\hat{e}(P_B',P_C)^{a'}$，$K_{A8}=\hat{e}(P_B',P_C')^{a'}$。

同样地，节点 B 和节点 C 经过同样的计算，彼此之间也会有 8 把共享密钥，分别如下所示：

B 节点：

$K_{B1}=\hat{e}(P_A,P_C)^b$，$K_{B2}=\hat{e}(P_A,P_C')^b$，$K_{B3}=\hat{e}(P_A',P_C)^b$，$K_{B4}=\hat{e}(P_A',P_C')^b$，$K_{B5}=\hat{e}(P_A,P_C)^{b'}$，$K_{B6}=\hat{e}(P_A,P_C')^{b'}$，$K_{B7}=\hat{e}(P_A',P_C)^{b'}$，$K_{B8}=\hat{e}(P_A',P_C')^{b'}$，

C 节点：

$K_{C1}=\hat{e}(P_A,P_B)^c$，$K_{C2}=\hat{e}(P_A,P_B')^c$，$K_{C3}=\hat{e}(P_A',P_B)^c$，$K_{C4}=\hat{e}(P_A',P_B')^c$，$K_{C5}=\hat{e}(P_A,P_B)^{c'}$，$K_{C6}=\hat{e}(P_A,P_B')^{c'}$，$K_{C7}=\hat{e}(P_A',P_B)^{c'}$，$K_{C8}=\hat{e}(P_A',P_B')^{c'}$。

4 安全性与效率分析

针对之前 LZC 密钥协商与 Shim-Woo 密钥协商的两种方案，作一个综合的比较。

4.1 安全性的分析

针对每个系统必须符合的安全特性，分析过程如下：

1)针对已知密钥安全，证明过程如下：

每一次共享密钥产生的方式，都是由节点所选择的暂时随机安全参数$\{a,a'\},\{b,b'\},\{c,c'\}$来决定的。因此，即便是攻击者能以网络流量的方式监测到共享密钥，但要从密钥 $K_{A1}=\hat{e}$

$(P_B,P_C)^a$，$K_{A2}=\hat{e}(P_B,P_C)^a$ 中破解$\{a,a`\}$，将使攻击者面临求解 Diffie-Hellman 计算问题的困难。所以，即使是丢失先前的共享密钥，其影响范围也仅仅针对该次的通讯记录，不会对后续的通信产生任何安全影响。

2)针对完美前向安全，证明过程如下：

共享密钥的产生与节点密钥，两者之间没有直接的关系。所以，攻击者必须先解出节点所选取的随机安全参数，才可以破解共享密钥。比如，攻击者万一得到了节点 A 的密钥 S_A。A 传送出去的信息$(P_A,P_A`,T_A)$中，攻击者可以计算出 $T_A-S_A$，得到 $aaP_{pub}$，但攻击者无法计算出相对应的安全参数$\{a,a`\}$，仍然面临求解 Diffie-Hellman 计算问题的困难。因此，本方案满足完美前向安全。

3)针对密钥泄露安全，证明过程如下：

假设，攻击节点 E 得到了节点 A 的密钥，想冒充节点 B 与节点 A，C 进行欺骗通信。节点 E 只能透过先前从网络上截获的信息$(P_B,P_B`,T_B)$，伪装成节点 $B$ 发送信息给节点 $A$，$C$。但节点 $E$ 无法得知节点 $B$ 的私钥 $S_B$，而且，试图计算出节点 $B$ 的安全参数$\{b,b`\}$，面临求解 Diffie-Hellman 计算问题的困难，同样是不可能的。因此，本方案满足密钥泄露安全。

4)针对未知共享密钥安全，证明过程如下：

在 LZC 的密钥协商中，攻击者可以在不知道安全参数$\{a\}$的情况下，产生一个伪装但合法的身份，而遭受未知共享密钥的攻击。问题在于，安全参数在只有一个$\{a\}$的情况下，可以通过自身的假设得到共享密钥。本方案中，随机安全参数为$\{a,a`\}$，除非攻击节点同时拥有，否则，将无法破解共享密钥。

5)针对密钥支配安全，证明过程如下：

在每一次的密钥协商过程当中，每一个共享密钥，都必须经过节点 A,B,C 三者的所有$\{a,a`\}$，$\{b,b`\}$，$\{c,c`\}$安全参数，才能够产生。共享密钥的产生不会受到某一个单一节点的控制。

总结对比结果如表 1 所列。

表 1　LZC,Shim-Woo,KASBP 3 种方案安全性对比

	LZC	Shim-Woo	KASBP
已知密钥安全	√	√	√
完美前向安全	√	√	√
密钥泄露安全	√	√	√
未知共享密钥安全	×	√	√
密钥支配安全	√	√	√

从表 1 可以看出，KASBP 方案与 Shim-Woo 方案处于同一个安全级别，而 LZC 则无法通过未知共享密钥安全。

4.2　效率分析

首先，在 LZC 密钥协商中，$T_A=H(P_A,P_A`)S_A+a\,P_A`$，采用的是单项抗碰撞函数，一个随机参数 a，要经过 4 次乘法运算，4 次双线性配对运算。

$$A->B,C:P_A=aP,P_A`=a`P,T_A=H(P_A,P_A`)S_A+aP_A`\hat{e}(T_B+T_C,P)=\hat{e}(H(P_A,P_B`)Q_B+H(P_C,P_C`)Q_C,P_{pub})\hat{e}(P_B,P_B`)\hat{e}(P_C,P_C`)\quad\text{(LZC 方案)}$$

但此方法容易遭受未知密钥的攻击。假设攻击节点 E 截获了节点 A 所发出的信息$(P_A,P_A`,T_A)$，然后将信息调换如下：$P_E=P_A$，$P_E`=a`P$($a`$为节点 E 自选的参数)，然后 E 再伪造自己身份 $T_E=H(P_E,P_E`)S_E+aa`P$，将信息篡改为$(P_E,P_E`,T_E)$重新传给节点 B 和节点 C 进行蒙骗。

$$E->B,C:P_E=P_A,P_A`=a`P,T_E=H(P_E,P_E`)S_E+aa`P\quad(1)$$

由式(1)可知，即使在不知道 A 所选取的安全参数$\{a\}$的情况下，攻击节点还是可以进行伪装攻击的。

而 Shim-Woo 的方案中，经过了 2 次乘法运算，4 次双线性配对运算。

$$A->B,C:P_A=aP,P_A`=a`P,T_A=S_A+a^2P+a`P_{pub}\hat{e}(T_B+T_C`,P)=\hat{e}(Q_B+Q_C+P_B`+P_C`)\hat{e}(P_B,P_B`)\hat{e}(P_C,P_C`)\quad\text{(Shim-Woo 方案)}$$

该方法很好地避免了 LZC 方案所面对的问题，即攻击者除非同时拥有$\{a,a`\}$才能进行伪装、欺骗。而提出的新的方案，在安全性一致的前提下，经过 2 次乘法运算，2 次双线性配对运算就可以达到要求。

$$A->B,C:P_A=aP,P_A`=a`P,T_A=S_A+aa`P_{pub}\hat{e}(T_B+T_C,P)=\hat{e}(Q_B+bbP+Q_C+cc`P,P_{pub})\quad\text{(KASBP 方案)}$$

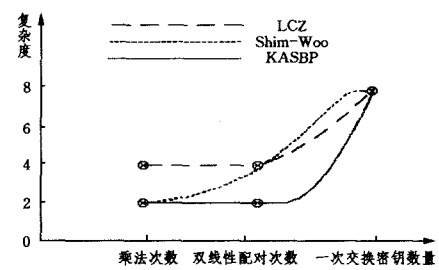

图 3　LZC,Shim-Woo,KASBP 3 种方案效率线比较图

由图 3 可以看出，在相同的安全性、所产生共享密钥数量相同的条件下，KASBP 方案计算所使用的计算方法次数、双线性配对次数都明显少于其他两种方案。

最后将比较的结果进行总结，如表 2 所列。

表 2　LZC,Shim-Woo,KASBP 3 种方案效率对比

	LZC	Shim-Woo	KASBP
乘法次数	4	2	2
双线性配对次数	4	4	2
单向抗碰撞函数的使用	Y	N	N
一次密钥交换量	8	8	8

结束语　针对 WSN 中节点间传递信息安全性不足的特点，研究并提出了一种适合 WSN 的密钥协商方案 KASBP。将 LZC 密钥协商与 Shim-Woo 密钥协商进行了理论分析和比较，结果表明，KASBP 在省去单项碰撞函数运算，乘法运算只使用 2 次，双线性配对函数只进行 2 次配对的情况下，达到 Shim-Woo 密钥协商方案的安全级别。如何处理网络带宽上的问题，并采用更高效、更安全的密钥协商方案将是今后的主要研究方向之一。

参 考 文 献

[1] Akyildiz I F, Su W, Sankarasubramaniam Y. Wireless Sensor Networks: A Survey [J]. Computer Networks, 2002, 38(4): 393-422

[2] Boneh D, Franklin M. Identity-based Encryption from the Weil pairing[J]. SIAM journal of Computing, 2003, 32(3): 586-615

(下转第 117 页)

替换代理提供的函数地址表中相应位置的函数，或者设置多至32个预先处理函数以及32个后续处理函数后，当实际接口调用对应函数时，其实是调用替换的函数，这样来获取软件系统的适应性。本文提出的机制显然更加灵活。

另外，SOA(面向服务体系结构)也能用于在线动态更换服务，但主要是粗粒度的，需重写整个服务。FOEM能针对类中的方法进行替换，从而变更整个类，主要是细粒度的，但利于系统变更时尽可能复用不变的代码，提高软件的复用性，这对于资源依赖强烈的嵌入式系统有一定的优势[9]。

从FOEM的设计可知，集中调度是整个系统的瓶颈，但我们可以相关调度策略来进行优化，这方面的研究很多，也不是本文研究的重点，因此没有详细展开。另外，由于通过方法的调用请求和方法的具体执行分开机制，在获得演化的灵活性的同时也带来一定的性能影响。但FOEM只对存在需求可变化的类才采用该机制，并且FOEM的主要开销是类的加载。从演化的技术来看，运行时单次加载所带来的性能开销是可接受的。表1是FOEM与OpenORB和ACE的具体相关比较(其中Load表示装载演化，Runtime表示运行时演化，AF表示抽象工厂模式，FM表示工厂方法模式)。

表1 相关比较

	动态演化粒度	运行时演化	动态配置	设计模式	演化类别	反射
FOEM	函数/类/对象	支持	支持	Command	Load/Runtime	不支持
Open-ORB	函数	不支持	不支持	Proxy	Load	支持
ACE	组件	支持	支持	AF/Proxy/FM	Load/runtime	不支持

结束语 随着计算环境的变化，给软件设计开发提出了新的挑战，尤其是如何快速地适应环境和需求的变化。而自适应演化软件正是解决该类问题的方案之一。当前对于自适应演化软件的研究从各方面展开，但主要是在理论研究方面，比如服务组合以及组合后的验证、动态体系结构语言的描述、动态体系结构的建模等。而关于在具体应用中如何实现自适应，特别是在线的软件自适应演化方面的实现研究却不多。本文基于设计模式中的命令模式，通过隔离方法的调用请求和方法的具体执行，提出一种灵活的在线演化机制，并通过初步的实现验证本机制的有效性。下一步对其性能进行改进，使之适合对系统性能要求高但资源严格受限的实时嵌入式环境。

参考文献

[1] 杨芙清，梅宏，吕建，等. 浅论软件技术发展[J]. 电子学报，2002，30(12A)：1901-1906

[2] 吕建，马晓星，陶先平，等. 网构软件的研究与进展[J]. 中国科学(E辑)：信息科学，2006，36(10)：1037-1080

[3] 余萍，马晓星，吕建，等. 一种面向动态软件体系结构的在线演化方法[J]. 软件学报，2006，17(6)：1360-1371

[4] Kephart J，Chess D. The Vision of Autonomic Computing[J]. IEEE Computer，January 2003：41-51

[5] 陈磊，李三立. 网格数据复本管理的动态自适应软件体系结构[J]. 软件学报，2006，17(6)：1436-1447

[6] Oreizy P，Gorlick M M，Taylor R N，et al. An architecture-based approach to self-adaptive software[C]// IEEE Intelligent System，1999，14(3)：54-62

[7] Garlan D，Schmerl B. Using architectural models at runtime：research challenges[C]// Oquendo F，Warboys B，Morrison R，eds. Proc. of the 1st European Workshop on Software Architectures. LNCS 3047，St. Andrews：Springer-Verlag，2004：200-205

[8] 王晓鹏，王千祥，梅宏. 一种面向构件化软件的在线演化方法[J]. 计算机学报，2005，28(11)：1890-1897

[9] Vandewoude Y，Berbers Y. Run-time Evolution for Embedded Component-oriented Systems[C]// Proceedings of the International Conference on Software Maintenance (ICSM'02)

[10] Gamma E，Helm R，Johnson R，et al. 设计模式-可复用面向对象软件的基础[M]. 李英军，等译. 机械工业出版社，2007

[11] Blair G S，Coulson G，Andersen A，et al. The design and implementation of open ORB 2[EB/OL]. IEEE Distributed Systems Online，2001，2(6). http://dsonline. computer. ogr/0106/features/bla0106-print. html.

(上接第90页)

[3] Joux A. A One Round Protocol for Tripartite Diffie-Hellman[C]// ANTS 4，LNCS 1838. Springer-Verlag，2000：385-394

[4] Al-Riyami S S，Paterson K G. Tripartite Authenticated Key Agreement Protocols form Pairings[C]// IMA Conference of Cryptography and Coding 2003，LNCS 2898. 2003：332-359

[5] Liu S，Zhang F，Chen K. ID-Based Tripartite key agreement protocol with pairing[C]//2003 IEEE International Symposium on Information Thory. 2003：136-143

[6] Shim K，Woo S. Weakness in ID-based One Round Authenticated Tripartite Multiple-Key Agreement Protocol with Pairings[J]. Applied Mathematics and Computation，2005，166：523-530

[7] Bao F，Deng R，Zhu R. Variations of Diffie-Hellman problem[M]. Springer-Verlag，2003：301-312

[8] Shim K. Efficient ID-Based Authenticated Key Agreement Protocol Based on the Weil Pairing[J]. Eectronic Letters，2003，39(8)：653-654

[9] Juang W-S，Wei-Ken Nien W-K. Efficient Password Authenticated Key Agreement Using Bilinear Pairings，Mathematical and Computer Modelling[M]. New York：Pergamon- Press，2008

[10] Chien H Y，Lin R Y. Identity-based key agreement protocol for mobile ad-hoc networks using bilinear pairing[C]//IEEE International Conference of Sensor Networks，Ubiquitous，and Trustworthy Computing. vol. 1，June 2006：520-529

[11] Chung H R，Ku W C. Impersonation attacks on a simple three-party key exchange protocol[C]// 17th Information Security Conference. June 2007

[12] Lee N Y，Wu C N，Wang P C. Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings[J]. Computers and Electrical Engineering，2008，34(1)：12-20

[13] Chien H Y. Highly Efficient ID-based Ring Signature from Pairings[C]// 2008 IEEE Asia-Pacific Services Computing Conference，IEEE APSCC 2008. Yilan，December 2008

[14] Guo Y J，Yu Z Q. Trust architecture in dynamic systems[C]// International Symposium on Advances in Computer and Sensor Networks and Systems. 2008：69-74