文章编号:1001 - 9081(2009)07 - 1816 - 04

基于 LU 矩阵空间的随机对密钥预分配方案

徐巧娟, 郑燕飞, 陈克非, 朱 博
(上海交通大学 计算机科学与工程系, 上海 200240)
(xuqiaojuan@gmail.com)

摘 要:从安全性和效率等方面,提出基于对称矩阵 LU 分解的无线传感器网络对密钥预分配方案的几个问题,包括密钥信息分配不均、U 矩阵完全公开、系统规模扩大对执行效率的影响较大等;根据对这些问题的具体分析,提出一种新的解决方案。该方案利用构造矩阵空间的思想,结合了随机分配方案和 LU 矩阵分解方案的特点,其可行性和安全性也得到证明;另外,根据在 PC 和 SunSpot 节点上的时间测试结果,对两种方案进行性能比较,后者在很大程度上降低了存储量和计算量。

关键词:无线传感器网络;对密钥预分配;对称矩阵;LU 分解;矩阵空间;随机原理
中图分类号: TP309.7 **文献标志码**:A

Random pair-wise key pre-distribution scheme based on LU matrix space

XU Qiao-juan, ZHENG Yan-fei, CHEN Ke-fei, ZHU Bo
(*Department of Computer Science and Engineer, Shanghai Jiao Tong University, Shanghai* 200240, *China*)

Abstract: This paper gave a detail analysis of the pair-wise key pre-distribution scheme based on LU-decomposition in terms of security and efficiency, covering several security issues such as uneven distribution of key information, disclosure of U matrix and the fact that the size of system has great impact on efficiency. An improved scheme based on matrix space which combines random scheme and LU-decomposition scheme was proposed, and its feasibility and security were also verified. The results of time test on PC and SunSpot devices show the improved scheme reduces storage and computation compared to the original one.

Key words: Wireless Sensor Network (WSN); pair-wise key pre-distribution; symmetric matrix; LU-decomposition; matrix space; random theory

0 引言

无线传感器网络(Wireless Sensor Network, WSN)集成了传感器、计算机和通信三大技术,已被广泛地应用于军事、环境、家庭和其他商业领域等方面。随着应用的深入,其安全问题变得越来越重要。基于网络中节点的计算能力和存储能力小等特点,传统的公钥加密体制和第三方认证方案并不可行,通常采用对称加密体制和节点之间相互认证方案。而如何实现有效的密钥管理是其中最基础的服务,目前普遍认为可行的是采取密钥预分配方案(Key Pre-distribution Scheme, KPS),即把密钥信息预先装入传感器节点。目前 KPS 有多种实现方法。文献[1]提出了随机对密钥分配方案,该方案首先生成一个足够大的密钥池,所有的节点在被部署之前都被随机分配一个密钥环,在密钥协商阶段,节点之间相互交换各自的密钥环,寻找出共同的密钥作为加密密钥。基于随机方案,文献[2]提出了 q-composite 随机对密钥分配方案,该方案与前一种唯一的不同之处在于,想要通信的节点对之间在密钥协商阶段必须找到至少 q 个共同密钥,然后利用这 q 个共同密钥对密钥进行计算,得到的结果作为加密密钥。这种方案增强了系统的安全级别,因为敌手想要攻击系统需要捕获更多的节点。另一个较为新颖的方案是基于对称多项式的对密钥分配方案[3](也是文献[4]提出的对称矩阵方案的另一种描述)。该方案利用对称多项式的特点 $f(x,y) = f(y,x)$,每一个节点存储多项式 $f(i,y)$,其中 i 是该节点的信息。对任意两个节点 i 和 j,节点 i 通过令 y 值为 j 计算出 $f(i,j)$,同时节点 j 通过令 y 值为 i 计算出 $f(j,i)$。于是,$f(i,j) = f(j,i)$ 就是这两个节点的对密钥。该方案的存储量小,计算简单,并且在文献[3]中被证明是无条件安全和 t-collusion resistant。文献[5]结合基于对称多项式方案和随机对密钥分配方案,提出了基于多项式池的密钥预分配方案。这样,一定程度上增加了存储量,但增强了抵抗攻击的能力。另外,还有很多基于节点位置信息的密钥分配方案。

最近,文献[6]提出一种基于对称矩阵 LU 分解的对密钥分配方案:首先,产生一个足够大的密钥池,接着随机选取一个集合用于构造对称矩阵;第二阶段是将这个对称矩阵分解成一个下三角矩阵 $\boldsymbol{L}$ 和一个上三角矩阵 $\boldsymbol{U}$;在节点被部署之前,将 $\boldsymbol{L}$ 矩阵中的一行和 $\boldsymbol{U}$ 矩阵的一列随机分配给某一个节点,要求被分配给同一节点的列和行号一致。在对密钥生成阶段,每一个节点广播自己的列信息,然后通过将对方的列向量和自己的行向量相乘,得到了两个节点之间的公共密钥。显然,通过这个过程,任何想要通信的节点对之间都能找到对密钥。

收稿日期:2009 - 01 - 06;**修回日期**:2009 - 02 - 23。 **基金项目**:国家 863 计划项目(2009AA01Z418)。

作者简介:徐巧娟(1984 -),女,浙江建德人,硕士研究生,主要研究方向:无线传感器网络安全; 郑燕飞(1976 -),女,河南郑州人,助理研究员,博士,主要研究方向:无线传感器网络安全; 陈克非(1959 -),男,北京人,教授,博士生导师,博士,主要研究方向:密码学、信息安全; 朱博(1985 -):男,陕西咸阳人,硕士研究生,主要研究方向:无线传感器网络安全。

本文提出了 Choi-Youn 方案的几个实际问题,包括密钥信息分配不均、U 矩阵完全公开等;然后通过在 SunSpot 节点和普通 PC 设备上的时间测试结果对这个方案进行执行效率的分析;接着利用矩阵空间的思想对方案进行改进,该方案能以较高的概率保证通信范围内的节点之间直接建立对密钥,不但解决原始方案存在的问题,在效率方面也有了很大的改善。

1　Choi-Youn 方案及其分析

1.1　Choi-Youn 方案

定义 1　对称矩阵。对称矩阵是一种方阵,它的特点是:$\boldsymbol{K} = \boldsymbol{K}^{\mathrm{T}}$。也即该矩阵中的元素相对于对角线是对称的,$k_{ij} = k_{ji}$。

Choi-Youn 的方案包括以下 4 个过程:

1)生成一个密钥池,大小为 $2^{17} \sim 2^{20}$;

2)随机从密钥池中选取 $n(n-1)/2$ 个密钥构造 $\boldsymbol{L}$ 矩阵($\boldsymbol{L}$ 矩阵上三角全为0);接着采用文献[7]中的方案得到 $\boldsymbol{U}$ 矩阵(这里的 n 是最终会被部署到特定应用系统中的最大的节点数目);

3)将已经构造完成的矩阵中的各行各列随机分配给各个节点,唯一的要求是同一位置上的行和列指派给同一个节点,即 $\boldsymbol{L}_{ri}$($\boldsymbol{L}$ 矩阵的第 i 行)和 $\boldsymbol{U}_{ci}$($\boldsymbol{U}$ 矩阵的第 i 列)分配给同一节点;

以上 3 步都是在节点部署之前完成的。

4)最后一步是密钥协商阶段:假设节点 x 和 y 分别存储($\boldsymbol{L}_{ri}$,$\boldsymbol{U}_{ci}$)和(L_{rj},U_{cj})。首先它们相互交换列信息,然后做向量乘法。节点 x 得到 $\boldsymbol{L}_{ri} \times \boldsymbol{U}_{cj} = k_{ij}$,而节点 y 得到 $\boldsymbol{L}_{rj} \times \boldsymbol{U}_{ci} = k_{ji}$,于是 $k_{ij} = k_{ji}$ 就是它们的对密钥。

1.2　分析

Choi-Youn 方案利用对称矩阵的特点,计算方便,实现简单,而且任一节点对都可以找到它们之间的对密钥;但是仍然存在一系列问题。

1)密钥信息分配不均:注意到 $\boldsymbol{L}$ 和 $\boldsymbol{U}$ 矩阵中的前几行(列),很明显这些向量中的信息过于简单,例如:$\boldsymbol{L}$ 矩阵中的第一行 $\boldsymbol{L}_{r1}$ 和 $\boldsymbol{U}$ 矩阵的第一列 $\boldsymbol{U}_{c1}$ 只有一个有效数据,其余都为 0;而对于矩阵的后面部分,当系统规模庞大时,数据量太大,给存储造成了困难。

2)在这个方案中,列信息是被广播的。任何人包括敌手都能轻易地得到列向量甚至是每一个列向量的所有者。可以说,$\boldsymbol{U}$ 矩阵事实上是公开的。而从文献[9]中的分析可知,利用完整的 $\boldsymbol{U}$ 矩阵以及部分行向量信息可以将 $\boldsymbol{L}$ 矩阵完全地恢复出来,因此如何将这些广播的信息进行隐藏是关键。

3)使用该方案时,系统规模扩大对执行效率的影响较大。下面通过在 SunSpot 设备上的时间测试结果(见表 1),对矩阵扩展带来的额外计算量和存储量进行具体的分析。

LU 分解效率　本文将文献[7]中的过程以 Java 程序实现,以下是实现的公式:

$$\boldsymbol{U}_{ij} = \frac{\sum_{k=2}^{i} \boldsymbol{L}_{jk}\boldsymbol{U}_{ki} - \sum_{k=1}^{i} \boldsymbol{L}_{ik}\boldsymbol{U}_{kj}}{\boldsymbol{L}_{ii}} \tag{1}$$

在 SunSpot 基站上的测试结果如下:

从表中可以很明确地看到,当矩阵规模扩大到原来的两倍时,构造 LU 矩阵所耗费的时间增长到原来的 8 ~ 10 倍。虽然这一过程是离线的,但是从测试的结果可以看到,如果基站或者 PC 的内存有限,要构造较大的 LU 矩阵将是困难的,尤其是当系统本身的规模非常大时,时间增长非常快。

表 1　SunSpot 节点和 PC 上构造 LU 矩阵的时间

SunSpot			PC		
矩阵规模	构造 LU 矩阵时间/ms		矩阵规模	构造 LU 矩阵时间/ms	
n/B	单倍规模	双倍规模	n/B	单倍规模	双倍规模
10	0.001	0.009	50	0.000	0.016
30	0.028	0.219	200	0.032	0.235
40	0.064	0.548	500	0.500	4.671
50	0.125	1.122	800	2.250	21.802
100	1.122	10.259	1 000	4.671	55.797

存储量　当规模增大到原来的两倍时,总共增加的存储是 n^2,分配到各节点上就是 $n^2/2n = n/2$。这对单个节点的存储能力是一大挑战。

密钥协商时间　在密钥协商阶段,涉及到信息的实时传输以及向量乘积。本文采用文献[8]中的编码方案,将被传输的列向量分为两部分即非零部分和零部分,在做向量乘积时进行相应解码。

将 SunSpot 节点之间的测试结果显示在表 2 中(注:表中给出的是通信发起方 A 节点和通信接收方 B 节点获得一个通信密钥的平均时间,其中节点 A 的时间为从广播请求信息到获得密钥,节点 B 的时间为从收到节点 B 的请求信息到获得密钥)。

表 2　SunSpot 节点之间密钥协商时间　　ms

向量长度 /B	密钥协商时间	
	节点 A	节点 B
125	679.500	584.667
250	852.000	755.000
500	1 311.000	1 215.000

从表中可以看出,随着矩阵增大,密钥协商时间明显增加了,主要原因就是传输的数据量大。而系统的效率主要取决于这一阶段的时间,因此必须限制矩阵的大小。

2　基于 LU 矩阵空间的随机方案

由于无线传感器网络的规模一般非常庞大,普通对称矩阵方案虽然能够保证任意节点之间都能找到共同的密钥,但是在实际的网络中,传感器节点的通信范围有限,一个节点只能与它周围的节点通信,因此只要以较高的概率保证相邻节点之间能找到共同密钥即可;而利用随机图原理,只要保证图是连通的,不能直接通信的节点对,可以通过中间节点进行过渡。利用这个特点,本文结合随机密钥分配方案,利用文献[10]描述的矩阵空间的概念实现系统的密钥预分配,从而有效地解决了上面提出的问题。

2.1　具体方案

定义 2　矩阵空间。矩阵空间是一系列($\boldsymbol{L}_i$,$\boldsymbol{U}_i$)的集合,其中,$\boldsymbol{L}_i$ 是下三角矩阵,$\boldsymbol{U}_i$ 是对应的上三角矩阵,i 是其 *ID* 值(这里矩阵空间的大小用 t 表示)。

具体过程如下:

1)首先产生一个大密钥池,大小为 $2^{17} \sim 2^{20}$。

2)矩阵空间生成阶段:随机从该密钥池中选取 $t \times \frac{m(m-1)}{2}$($m \ll n$)($n$ 为最终会被部署到特定应用系统中的最大的节点数目,m 为所要构造的矩阵大小)个密钥构造 t 个下三角矩阵 $\boldsymbol{L}_i$,$i = 1,2,\cdots,t$;接着采用文献[6]中的方案得到对应的 $\boldsymbol{U}_i$,$i = 1,2,\cdots,t$。

3)密钥信息分配阶段:每个传感器节点在被部署之前,系统会从矩阵空间中随机选取 r 个元素,如 $(\boldsymbol{L}_{i_1},\boldsymbol{U}_{i_1})$,$(\boldsymbol{L}_{i_2},\boldsymbol{U}_{i_2})$,…,$(\boldsymbol{L}_{i_r},\boldsymbol{U}_{i_r})$,然后将每个元素中的下三角矩阵的任意一行和上三角矩阵中相对应的列信息(如 $(\boldsymbol{L}_{i_1},\boldsymbol{U}_{i_1})$ 中的 $(\boldsymbol{L}_{r_j i_1},\boldsymbol{U}_{c_j i_1})$,$r_j$ 表示矩阵 $\boldsymbol{L}_{i_1}$ 中的第 j 行,c_j 表示矩阵 $\boldsymbol{U}_{i_1}$ 中的第 j 列)分配给该节点,这样每个节点都存储 r 个行和列信息。注意到,对于规模为 m 的矩阵最多只能被分配给 m 个节点,因为每个矩阵的每一行(列)信息都只能被分配一次。

以上三步是在系统部署之前完成的。

4)节点之间建立对密钥阶段:假设两个节点 x,y 要建立对密钥,首先向对方广播自己存储的一系列 ID 值,假如这两个节点之间存在共同的 ID 值,设为 k,说明两个节点能直接建立对密钥;接着,节点 x,y 分别发送该 ID 对应的列向量信息 $\boldsymbol{U}_{c_i k}$ 和 $\boldsymbol{U}_{c_j k}$,通过将自身的行向量与对方的列向量做向量乘法,$\boldsymbol{L}_{r_i k}\times\boldsymbol{U}_{c_j k}=\boldsymbol{L}_{r_j k}\times\boldsymbol{U}_{c_i k}$,结果就是它们的共密钥。

5)假如两个节点之间没有发现共同的 ID 值,就需要通过中间节点作为过渡,具体过程如下:假设节点 x 要与节点 y 建立对密钥,节点 x 向它的邻居节点广播自己和节点 y 的 ID 值信息,各邻居节点判断是否与这两个节点都存在共同的 ID 值,如果存在就利用这个邻居节点作为中间节点。

2.2 性能分析

首先利用随机图的原理来分析网络的连通性:对于一个有 n 个节点的网络,要保证整个网络的连通性达到一定值 P_r,则需要每个节点都能与 d 个邻居节点直接通信。

$$d=\frac{n-1}{n}\times(\ln n-\ln\ln P_r) \tag{2}$$

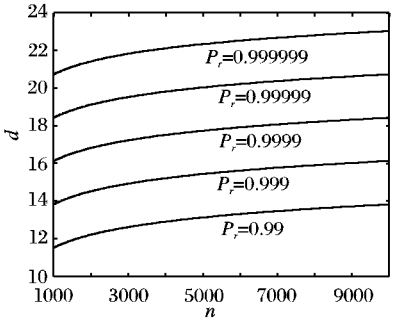

图1 d、P_r 以及 n 之间的关系曲线

可以看出,P_r 增大,节点度的增量很小;而且 n 越大,曲线越平缓,说明网络规模的增大对节点度的影响并不大。因此,只要能保证节点能与其邻居节点以一定的概率通信就能保证整个网络的连通。

现分析任意两个节点之间能直接建立对密钥的概率(同样也是邻居节点之间能直接建立对密钥的概率),设为 p,于是:

$$p=1-\frac{C_t^r C_{t-r}^r}{C_t^{2r}}=1-\frac{[(t-r)!]^2}{(t-2r)!t!} \tag{3}$$

由于相比 r,t 大得多,可以用 Stirling 近似式 $t!\approx\sqrt{2\pi t}(\frac{t}{e})^t$ 来简化式(3)得到:

$$p=1-\frac{(1-r/t)^{2(t-r+1/2)}}{(1-2r/t)^{(t-2r+1/2)}} \tag{4}$$

由图2容易看出,对于 $t=10000$ 的矩阵空间,只需要给每个节点分配75个元素就能保证节点能直接找到共同密钥的概率达到0.5,如果矩阵空间的规模增大到10倍,每个节点分配大约250个元素就能保证同样的概率。

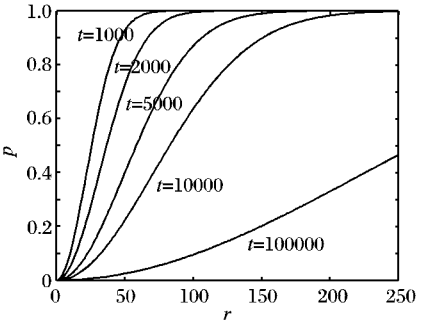

图2 两个节点之间存在共密钥的概率 p 与 t,r 的关系曲线

对于不能直接建立共密钥的节点之间,下面分析通过多跳方式通信的情况(这里仅给出经过一个中间节点的分析):假设节点 x 和 y,x 节点的邻居节点有 d' 个,这 d' 个节点中,存在能同时与 x,y 节点建立共密钥的概率为:

$$p'=1-(1-p)(1-p^2)^{d'} \tag{5}$$

另外,矩阵空间中的每一个元素,最多只能被分配 m 次,首先分析在给系统中所有节点随机分配密钥信息的过程中,矩阵空间中任一元素被分配了 m 次的概率:

$$P_m=C_n^m(\frac{r}{t})^m(1-\frac{r}{t})^{n-m} \tag{6}$$

因而任一元素最多只被分配 m 次的概率为:

$$P_{\leqslant m}=\sum_{0\leqslant i\leqslant m}P_i \tag{7}$$

图3显示了式(7)的曲线图($n=1000$),由图可知,在 n 固定的情况下,随着 m 的增大,要使 $P_{\leqslant m}$ 达到最大,r/t 也变大。在实际的网络中,可以根据式(7)和图3合理选取参数。一般情况下,要求 m 和 r 尽可能小,举例说明:$m=20$ 时,为了保证在随机分配的过程中任一元素不被选中超过 m 次,r/t 的值应在0.01左右合理选择;而在 r/t 确定的情况下,结合式(4)和图2,在满足 r 尽可能小的要求时确定 t。

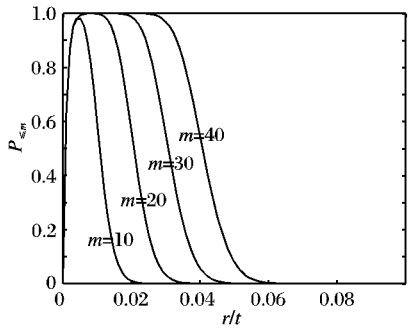

图3 式(7)的曲线

另外,要保证每个节点都能分配到 r 个元素,必须满足:

$$m\times t\geqslant n\times r\Rightarrow r/t\leqslant m/n \tag{8}$$

与前面的方案相比,本文的方案存在以下优势:

1)矩阵空间的生成耗费时间较少,因为每个矩阵的规模小得多,生成 t 个矩阵的时间大约为 $t\times m^3$,相比之前的 n^3 没有很大的变化,但是这一阶段是在节点被部署之前完成的,只要在合理的范围之内,对系统的效率影响不大。如果合理设置系统参数,能得到一定的改善。

2)每个节点存储的数据也较少,大约 $r\times(2m)\ll 2n$。

3)节点在通信过程中传输量小,因为列向量长度小得多,为 $m\ll n$,额外增加的也只是 ID 值信息。

4)做向量乘积的计算量也比原方案少得多($m\ll n$)。

2.3 安全性分析

该方案也解决了原始方案的几个安全问题。

1)首先该方案解决了第2部分提出的第一个问题即节点之间的密钥信息分配不均:每个节点都拥有 t 对行列信息,分配又具有随机性,这样所有节点所含的密钥信息量相对一致,不会出现过多或者过少的情况。

2)前面提到,文献[9]中利用 LU 矩阵的特点,通过 $\boldsymbol{U}$ 矩阵的行信息和 $\boldsymbol{L}$ 矩阵中部分信息还原出更多的 $\boldsymbol{L}$ 矩阵信息。本文的方案在很大程度上解决了这个问题,因为要还原出 $\boldsymbol{L}$ 矩阵的信息,必须要知道 $\boldsymbol{U}$ 矩阵,但在本文的方案中,即使攻击者截获了所有被广播的列信息,还是不知道该列信息对应矩阵的 ID 值;从另一个角度来看,攻击者想要获取某个矩阵完整的列信息是相当困难的,因为首先对于某一个矩阵,由于最多只能被选择 m 次,可能只有部分信息被分配给节点,其次即使该矩阵恰好被选择了 m 次,它们的分布也是未知的。

3 结语

密钥分配和管理关系到无线传感器网络的安全问题,一直是研究的热点问题之一。无线传感器网络不同于传统网络,考虑到其能量、计算能力、存储容量和通信带宽的限制,密钥分配机制有其自身的特点。近年来被广泛接受的基于对称矩阵 LU 分解的对密钥预分配方案,存在几个安全问题,如密钥信息分配不均、$\boldsymbol{U}$ 矩阵完全公开等,还有系统规模扩大对执行效率影响非常大的问题。本文提出的基于 LU 矩阵空间的随机方案,结合了随机分配方案和 LU 矩阵分解方案的特点,通过合理设置参数不但降低了矩阵规模使之能适应传感器的要求,也能以较高的概率保证邻居节点之间直接建立对密钥,同时也解决了原始方案中的安全问题。

参考文献:

[1] ESCHENAUER L, GLIGOR V D. A key management scheme for distributed sensor networks[C]// Proceedings of 9th ACM Conference on Computer and Communications Security. New York: ACM, 2002:41 - 47.

[2] CHAN H, PERRIG A, SONG D. Random key pre-distribution schemes for sensor networks[C]// Proceedings of 2003 IEEE Symposium on Research in Security and Privacy. Washington, DC: IEEE Computer Society, 2003:197 - 213.

[3] BLUNDO C, De SANTIS A, HERBERG A. Perfectly-secure key distribution for dynamic conferences[J]. Information and Computation, 1998, 146(1):1 - 23.

[4] BLOM R. An optimal class of symmetric key generation systems [C]// Proceedings of Euro-crypt 84, LNCS 0209. Berlin : Springer-Verlag, 1984:335 - 338.

[5] LIU D, NING P, Establishing pair-wise keys in distributed sensor networks[C]// Proceedings of the 10 th ACM Conference on Computer and Communication Secuity. New York: ACM, 2003: 27 - 31.

[6] CHIO S J, YOUN H Y. An efficient key pre-distribution scheme for secure distributed sensor networks[C]// The 2005 IFIP International Conference on Embedded and Ubiquitious Computing. Nagasaki: Springer, 2005:1088 - 1097.

[7] PARK C W, CHIO S J, YOUN H Y. A noble key pre-distribution scheme with LU matrix for secure wireless sensor networks[C]// Proceedings of International Conference on Computational Intelligence and Security. Berlin: Springer, 2005:487 - 499.

[8] DAI T T, PATHAN A K, HONG C S. A resource-optimal key pre-distribution scheme with enhanced security for wireless sensor networks[C]// Management of convergence networks and services, LNCS 4238, 2006:546 - 549.

[9] ZHU B, ZHENG Y, CHEN K, *et al*, Cryptanalysis of LU decomposition-based key pre-distribution schemes for wireless sensor networks[EB/OL]. [2008 - 11 - 20]. http://eprint. iacr. org/2008/411. pdf.

[10] DU W, DENG J, HAN Y S, *et al*. A pair-wise key pre-distribution scheme for wireless sensor networks[C]// Proceedings of the 10th ACM conference on Computer and Communicaiton Security. New York: ACM, 2003:27 - 30.

(上接第 1815 页)

[10] HWANG R J, LAI C H, SU F F. An efficient signcryption scheme with forward secrecy based on elliptic curve [J]. Applied Mathematics and Computation, 2005, 167(2):870 - 881.

[11] OLIVEIRA L B, DIEGO A, EDUARDO M, *et al*. TinyTate: Computing the tate pairing in resource-constrained sensor nodes [C]// Network Computing and Applications. New York: IEEE, 2007: 318 - 323.

[12] OLIVEIRA L B, MICHAEL S, JULIO L, *et al* . TinyPBC : Pairings for authenticated identity-based non-interactive key distribution in sensor networks [EB/OL]. [2008 - 10 - 20]. http:// eprint. iacr. org/2007/482. pdf.

[13] NIDHI V. Practical implementation and performance analysis on security of sensor networks[EB/OL]. [2008 - 10 - 20]. https:// ritdml. rit. edu/dspace/bitstream/1850/2893/1/NVermaThesis11-2006. pdf.

[14] MALAN D J, WELSH M, SMITH M D. A public-keyinfrastructure for key distribution in TinyOS based on elliptic curve cryptography [EB/OL]. [2008 - 10 - 20]. http://www. cs. harvard. edu/ ~ malan/publications/secon04. pdf.

[15] POTLAPALLY N R , RAVI S , RAGHUNATHAN A , *et al* . Analyzing the energy consumption of security protocols [C]// Proceedings of the 2003 International Symposium on Low Power Electronics and Design. New York: ACM, 2003:30 - 35.

[16] Tinyos[EB/OL]. [2008 - 10 - 20]. http://www. tinyos. net.

[17] AN L, PENG N. TinyECC: A Configurable Library for elliptic curve cryptography in wireless sensor networks[C]// Proceedings of the 7th International Conference on Information Processing in Sensor Networks. Washington, DC: IEEE Computer Society, 2007: 1 - 17.

[18] ZHENG Y. Digital signcryption or how to achieve Cost (Signature and Encryption) [C]// Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 1997: 165 - 179.

[19] ZHENG Y , IMAI H . How to construct efficient signcryption schemes on elliptic curves [J]. Information Processing Letters, 1998, 68(5):227 - 233.

[20] Signcryption Central [EB/OL]. [2008 - 10 - 21]. http://www. signcryption. net/publications.

[21] Cricket [EB/OL]. [2008 - 10 - 21]. http://www. xbow. jp/ mcskit410. pdf.

[22] Crossbow Technology[EB/OL]. [2008 - 10 - 21]. http://www. xbow. com.

[23] Crossbow[EB/OL]. [2008 - 10 - 21]. http://www. xbow. com/ Products/Product_pdf_files/Wireless_pdf/ MICA2_Datasheet. pdf.

[24] ELGAMAL. A public key cryptosystem and a signature scheme based on discrete logarithms[C]// Proceedings of CRYPTO 84 on Advances in Cryptology. New York: Springer-Verlag, 1985: 469 - 472.