基于 RNG 与 CBC 的异构传感器网络密钥管理方案*

胡运松, 单 洪
(电子工程学院, 合肥 230037)

摘 要: 为解决异构无线传感器网络密钥管理方案所需负载较大和大规模节点被俘获后的安全隐患问题,提出了一种新的密钥管理方案,采用随机数生成和分组链接技术建立会话密钥,通过在不同簇内广播不同的阶段标志来增加网络的安全性。理论分析和仿真实验表明,该方案能够利用较低的存储负载获得较高的密钥连通性,同时能够解决大规模节点被俘获而带来的安全问题。

关键词: 异构传感器网络; 随机数生成; 分组链接; 阶段标志; 密钥链
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1892-04
doi:10.3969/j.issn.1001-3695.2010.05.082

Key management scheme for heterogeneous wireless sensor network based on RNG and CBC

HU Yun-song, SHAN Hong
(*Electronic Engineering Institute*, *Hefei* 230037, *China*)

Abstract: For solving the issues of great storage payload and security trouble after mass nodes been compromised in heterogeneous wireless sensor network, this paper proposed a new key management scheme. The scheme took random number generation and cipher block chaining to build a session key. Meanwhile, added different phase signs in different clusters to increase security performance for the whole network. Theoretic studies and simulation experiments show that the scheme needs less storage payload to get more key connectivity and has the ability to solve the security problem after mass nodes been compromised.
Key words: heterogeneous wireless sensor network; random number generation; cipher block chaining; phase sign; key chain

0 引言

无线传感器网络(WSN)由部署在监测区域内的大量传感器节点组成,通过无线通信方式形成的一个多跳自组织的网络系统,其目的是协作地感知、采集和处理网络覆盖区域中感知对象的信息,并发送给观察者[1]。传感器节点可以根据感测能力、通信能力、计算能力和能量等不同而分为不同种类。根据网络中节点类型是否相同,无线传感器网络可以分为同构型和异构型。同构无线传感器网络是指由相同类型的传感器节点构成的网络,而异构无线传感器网络(HWSN)则是由不同类型的节点所组成的。

保障 WSN 的安全运行是无线传感器网络得以广泛运用的基础之一。WSN 的自身特点决定了其安全研究的复杂性和独特性:传感器节点规模大、资源有限、容易被捕获;无线通信方式容易被窃听和干扰;低成本的传感器节点被俘获后信息可能会泄露。这些特性使得解决 WSN 的安全问题成为一项富有挑战性的工作。以提供安全、可靠的保密通信为目标的密钥管理方案和协议的设计是 WSN 安全最为重要、最为基本的研究领域[2]。目前 WSN 密钥管理的研究主要集中于同构传感器网络[3~7],HWSN 密钥管理是近年来的研究热点[8~10]。本文在分析各种密钥管理方案后,针对 HWSN 的特点,提出一种基于随机数生成和分组链接技术的密钥管理方案,用于解决 HWSN 密钥管理方案所需负载较大和大规模节点被俘获后的安全问题。

1 相关研究

目前关于 WSN 的密钥管理方案主要分为三类,即可信任服务器方案、公开密钥方案和密钥预分发方案[11]。可信任服务器方案中,节点之间建立密钥依赖于一个可信任服务器,由于其大量的通信开销,该方案不适合应用于 WSN 中。公开密钥方案基于非对称加密并且通常需要公钥基础设施,对传感器节点的能力要求较高,也不适合在 WSN 中应用。密钥预分发方案在 WSN 部署之前将秘密信息存储于传感器节点中,解决了网络部署后密钥分配所带来的能量消耗问题,是目前 WSN 密钥管理方案的研究热点。

Perrig 等人[3] 于 2001 年提出 SPINS 安全协议,其中的 SNEP 协议假设网络中每个节点均与基站共享一对主密钥,其他密钥都从主密钥衍生,节点之间对偶密钥的建立需要通过基站来实现。Eschenauer 等人[4] 提出一种随机密钥预分配方案,部署服务器首先产生一个密钥总数为 P 的密钥池,节点在部署前从密钥池中随机选取 n 个密钥,邻居节点之间通过预分配的密钥建立通信的对偶密钥。在 Chan 等

收稿日期: 2009-08-11; **修回日期**: 2009-09-22 **基金项目**: 国家"863"计划资助项目
作者简介:胡运松(1982-),男,博士研究生,主要研究方向为传感器网络(purain@126.com);单洪(1965-),男,教授,博导,主要研究方向为网络安全等.

人[5]提出的 q-composite 随机密钥预分配方案中，节点从密钥总数为 $|S|$ 的密钥池里随机选取 m 个不同的密钥，部署后两个相邻节点至少需要共享 q 个密钥才能直接建立配对密钥。Liu 等人[6]提出了基于多项式池的对偶密钥预置框架，给出基于随机子集和超立方模型的密钥预置方案。文献[7]提出了一种基于地理位置的密钥管理方案，将目标区域划分为若干个大小相同的正方形区域，为每个区域分配一个二元多项式，节点预置本区域和相邻区域共五个二元多项式。

Du 等人[8]提出一种适用于 HWSN 的非对称密钥预置方案，该方案为资源充沛的高级节点预置更多的密钥，使得整个网络的安全性和生存期都有较大的提高。Lu 等人[9]构建了一种 HWSN 密钥管理方案的统一框架，基于随机密钥预分配和多项式密钥预分配，为现有的分布式密钥管理方案构建统一的框架。文献[10]证明在拥有少量资源充沛的高级节点的 HWSN 中采用基于概率的不均衡密钥分配方案能够提高整个网络安全性和抗俘获性。

上述各种密钥管理方案虽然有效地提高了 WSN 中节点之间通信的安全性，但是均存在一些缺陷，不太适合应用于安全需求较高的 HWSN 中。文献[3~7]提出的密钥管理方案主要针对同构 WSN，不能直接应用于 HWSN。文献[8,9]提出的方案所需存储负载较高且无法解决大规模节点被俘获所带来的安全问题。

2　网络模型

HWSN 由汇聚节点(sink)、高级节点(H-sensor)和普通节点(L-sensor)组成，节点依据不同的感知任务和地理位置划分为多个簇，H-sensor 因为具有较高的存储、计算和传输能力、能量大或者可以补充，所以选定其作为簇首，L-sensor 将监测数据通过 H-sensor 传输到 sink。网络模型如图 1 所示。

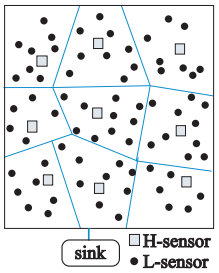


图1　HWSN网络模型

本文对 HWSN 的假设如下：

a) L-sensor 由于资源限制，不配置防俘获的硬件装置，即 L-sensor被俘获后，存储的内容(包括密钥、数据和代码等)都会泄露。

b) H-sensor 数目在整个网络中所占比例很小，如规模为 5 000个节点的网络中只有 20 个 H-sensor。

c) H-sensor 配置防俘获的硬件装置，即使被俘获，H-sensor 也不会泄露其存储的内容。因为 H-sensor 数目较少，为其配置更高级的装置对于整个网络的性能不会有影响，相反会明显提高网络的效率。

d) 每个节点都有惟一的 ID，都预置随机数生成与散列函数。

本文中常用的符号及其定义如表 1 所示。

表 1　常用符号及其定义

符号	说明
H_i	高级节点 H-sensor
L_i	普通节点 L-sensor
ID_i	节点 i 的 ID 号
N_i	节点 i 产生的 nonce 随机数
T_i	阶段标志
K_M	H-sensor 的预置主密钥
$K_{M,i}$	L-sensor 的预置认证密钥
ck_i	节点的密钥链生成值
id_i	共享密钥链生成值 ID 号
s	密钥链生成值的共享数目
q	密钥链生成值共享门限值
$n_{i,j}$	会话密钥生成时迭代次数
list	邻居节点列表
rand( )	伪随机生成函数
hash( )	散列函数
MAC	消息认证码

3　方案设计

本文中的密钥池由若干个密钥链构成，每个密钥链都通过散列函数和密钥链生成值迭代产生。为保证 HWSN 更加安全的运行，整个运行周期被分为多个阶段，在不同的阶段 H-sensor 广播一个阶段标志 T_i，不同 H-sensor 广播不同的 T_i，L-sensor 将 T_i 和 ID 号作为伪随机函数的输入，产生密钥链生成值，这是会话密钥建立的基础。H-sensor 经过判断后，向 L-sensor 发送密钥链生成值的 ID 和迭代次数，L-sensor 通过散列函数计算出与邻居节点的会话密钥。

3.1　密钥预分配阶段

首先选择密钥池的大小 P、密钥链的个数 M 和密钥链的长度 L。其中，$P = M \times L$，然后确定 L-sensor 和 H-sensor 的预置密钥链个数 r 和 $R(R >> r)$，随后为每个节点生成惟一的 ID。Sink 生成一个认证主密钥 K_M 用于节点间的相互认证，每个 H-sensor 都预置主密钥 K_M，L-sensor 也预置一个认证密钥 K_{M,L_i} ($K_{M,L_i} = \mathrm{hash}(K_M, id_{L_i})$)。

3.2　簇生成阶段

HWSN 簇生成过程如下：H-sensor 首先以最大功率广播 hello 消息，消息包括 H-sensor 的 ID 号和阶段标志 T_i，用 rand( )产生 R 个密钥链生成值 $ck_1, \cdots, ck_R = \mathrm{rand}(\mathrm{ID}_{H_a} \oplus T_i)$，密钥链生成值的 ID 号为 $id_i = ck_i \bmod M$。然后 L-sensor 从接收到的 H-sensor 中选择接收信号强度标志最好的一个 H-sensor 作为其簇首节点，并存储其 ID 和 T_i，随后用 rand( )产生 r 个密钥链生成值 $ck_1, \cdots, ck_r = \mathrm{rand}(\mathrm{ID}_{L_i} \oplus T_i)$，同时计算其 ID 号。簇生成阶段完成后，HWSN 形成以 H-sensor 为簇首的若干个小区域。

3.3　会话密钥建立阶段

本阶段包括两个部分，即 L-sensor 与 H-sensor 之间会话密钥的生成和 L-sensor 与 L-sensor 之间会话密钥的生成。L-sensor 与 H-sensor 之间会话密钥的生成过程为：L-sensor 首先向所属簇的簇首节点 H-sensor 发送确认消息，内容为 L-sensor 的 ID 号，nonce 值和用该节点认证密钥 K_{M,L_i} 计算的消息认证码。H-sensor 收到消息后先计算出 K_{M,L_i}，然后用 rand( )生成 L-sensor 的密钥链生成值，判断 L-sensor 与 H-sensor 的密钥链生成值的共享数目 s 与门限值 q 的关系，如果大于或等于，则 H-sensor 将前 q 个共享密钥链生成值的 ID 号 $id_i, \cdots, id_q$，迭代次数 n_i ($n_i \leqslant L$) 发送给 L-sensor，L-sensor 收到 H-sensor 发送的消息后，根据 $id_1, \cdots, id_q$ 和 n_i 计算出与 H-sensor 的会话密钥 K_{L_i,H_a}。如果 $s < q$，则 H-sensor 生成与 L-sensor 的会话密钥

K_{L_i,H_a}并通过 K_{M,L_i}发送给 L-sensor。通过 $id_1,\cdots,id_q$ 和 n_i 计算会话密钥的具体步骤及伪代码如图 2 所示。

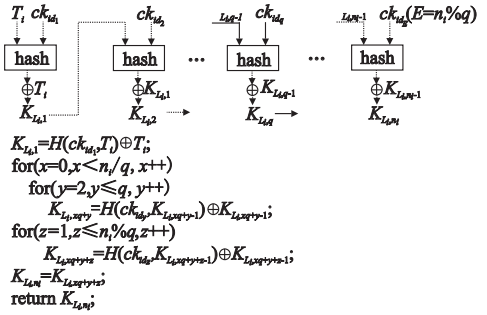


图2 会话密钥计算步骤与伪代码

L-sensor 与 L-sensor 之间会话密钥的生成过程为：L-sensor 首先发送广播消息来获得其邻居节点的 ID 号，然后向簇首节点 H-sensor 发送消息，内容为 L-sensor 的 ID 号，nonce 值，邻居节点的 ID 和用 K_{L_i,H_a} 计算的消息认证码。H-sensor 首先用 rand( )生成 L-sensor 及其邻居节点的密钥链生成值，然后判断 L-sensor 与其邻居节点的密钥链生成值的共享数目 s 与 q 的关系，如果大于或等于，则 H-sensor 将前 q 个共享密钥链生成值的 ID 号 $id_1,\cdots,id_q$，迭代次数 $n_{L_i,L_j}(n_{L_i,L_j}\leq L)$ 发送给 L-sensor，L-sensor 收到 H-sensor 发送的消息后，根据 $id_1,\cdots,id_q$ 和 n_{L_i,L_j} 计算出与各个邻居节点的会话密钥。如果 $s<q$，则 H-sensor 生成 L-sensor 间的会话密钥 K_{L_i,L_j} 并通过 K_{L_i,H_a} 和 K_{L_j,H_a} 发送给 L-sensor。

3.4 密钥更新阶段

密钥更新主要考虑三种情况，即网络一个阶段运行结束、节点被俘获和新节点加入。网络运行完一个阶段后，L-sensor 删除所有密钥信息，仅仅保留其 ID 号，在下一阶段重新建立会话密钥。当发现网络中有节点被俘获后，H-sensor 广播密钥撤回消息，L-sensor 收到该消息后删除与被俘获节点的会话密钥同时将其 ID 号从邻居节点列表中删除。HWSN 中有新节点加入时，首先确定属于哪个簇，然后向簇首 H-sensor 发送请求数据包，获得当前的阶段标志，随后计算与其他节点的会话密钥。

4 理论分析

4.1 密钥连通性分析

设 $p_{LH}(j)$ 为 L-sensor 与 H-sensor 之间共享 j 个密钥链生成值的概率，则

$$p_{LH}(j)=\binom{M}{j}\binom{M-j}{R+r-2j}\binom{R+r-2j}{r-j}\binom{M}{r}\binom{M}{R} \quad (1)$$

其中：$\binom{M}{j}$ 为从 M 个密钥链生成值中选取 j 个共享值；$\binom{M-j}{R+r-2j}$ 为从剩余的 $M-j$ 个中选取 $R+r-2j$ 个非共享值给 H-sensor 和 L-sensor；$\binom{R+r-2j}{r-j}$ 为 $R+r-2j$ 个值分配给 H-sensor和 L-sensor；$\binom{M}{r}$ 为从 M 个密钥链生成值中选取 r 个分配给 L-sensor；$\binom{M}{R}$ 为从 M 个密钥链生成值中选取 R 个分配给 H-sensor，则 L-sensor 与 H-sensor 之间能够直接建立对偶密钥的概率为

$$p_c=1-(p_{LH}(0)+p_{LH}(1)+\cdots+p_{LH}(q-1)) \quad (2)$$

图 3 给出在 $P=10\ 000$，$L=20$，$R=100$ 时 p_c 与 r 和 q 之间的关系。如图 3 所示，随着 L-sensor 预置的密钥链生成值 r 不断增加，其与 H-sensor 之间的密钥连通概率 p_c 也逐渐增大。当 L-sensor 预置相同数目密钥链生成值时，如果 q 不断增大，节点间需要共享更多的密钥链生成值，因此 p_c 值逐渐减小。

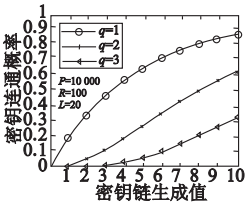


图3 密钥连通概率与门限值关系

4.2 节点的存储负载

本文在建立对偶密钥过程中使用密钥链技术，L-sensor 仅仅需要预置少量的密钥链生成值就可以与其他节点建立对偶密钥，与 AP(Du 等人[8] 提出的非对称密钥预置方案) 和 QC (Chan 等人[5] 提出的 q-composite 随机密钥预分配方案) 相比能够大大减少节点的存储负载。

图 4 给出密钥池大小为 10 000 的情况下，AP 与 QC 方案的密钥连通概率。其中，图 4(a) 为 AP 方案中 H-sensor 预置 $N=500$ 个密钥值时 L-sensor 预置密钥数目与密钥连通概率之间的关系；图 4(b) 为 QC 方案中每个节点的预置密钥数目与密钥连通概率之间的关系。比较图 3 与 4，可知本文提出的方案(下文简写为 RCP) 与 AP 和 QC 相比，仅仅需要 L-sensor 预置少量的密钥链生成值，就能够获得相同的密钥连通概率。例如，在网络规模为 1 000 个 L-sensor 和 20 个 H-sensor 时，取 $q=2$，$r=5$，$R=100$，AP 的 L-sensor 需要预置 20 个密钥，而 QC 需要在所有节点内预置 100 个密钥才能具有相同的密钥连通概率。这时 RCP 所需存储负载为 $1\ 000\times5+100\times20=7\ 000$，AP 所需存储负载为 $1\ 000\times20+500\times20=30\ 000$，而 QC 所需存储负载为 $1\ 020\times100=10\ 2000$。AP 所需存储负载是 RCP 的 4.3 倍，而同构传感器网络中的方案 QC 所需存储负载则远远大于 RCP。因此，理论分析表明本文提出的密钥管理方案能够在保证连通性的前提下，大大减少节点的存储负载，从而提高整个 HWSN 的性能。

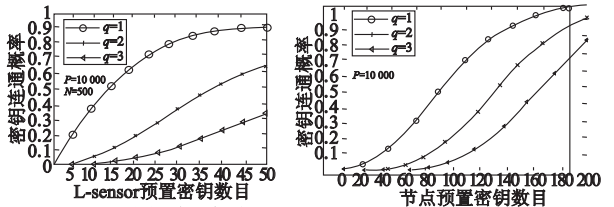


图4 密钥连通概率

4.3 安全性分析

HWSN 中的 L-sensor 不配置防俘获装置，决定了其被攻击后可能会泄露敏感信息，从而被攻击者利用来实施其他攻击活动。本节主要分析 L-sensor 被俘获后对网络中其他通信链路的影响。

由文献[8]可知，如果不考虑簇首发送的阶段标志，假设网络中有 c 个 L-sensor 被俘获，每个 L-sensor 预置 r 个密钥链生成值，则给定一个密钥链生成值 K，其未泄露的概率为 $(1-\frac{r}{M})^c$，泄露的概率为 $1-(1-\frac{r}{M})^c$。如果 L-sensor 之间需要 j 个密钥链生成值来计算会话密钥，则该会话密钥泄露的概率为 $(1-(1-\frac{r}{M})^c)^j$。建立安全会话密钥的概率为

$$p=p_{LH}(q)+p_{LH}(q+1)+\cdots+p_{LH}(r) \quad (3)$$

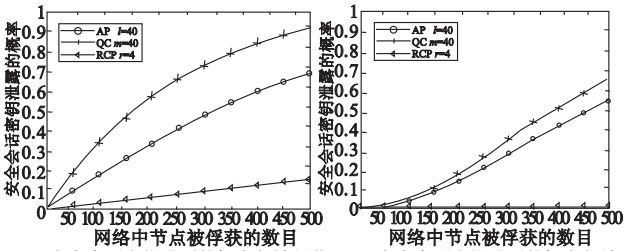
其中:$p_{LH}(j)$ 由公式(1)得到。因此,当 c 个 L-sensor 被俘获后,安全会话密钥泄露的概率为

$$C(r)=\sum_{j=q}^{r}\left(1-\left(1-\frac{r}{M}\right)^{c}\right)^{j}\frac{p_{LH}(j)}{p} \tag{4}$$

考虑到簇首节点 H-sensor 发送不同的阶段标志 T_i,然后 L-sensor通过 T_i 和 ID 计算密钥链生成值,由于每个簇的阶段标志不同,属于不同簇的 L-sensor 的密钥链生成值不同,一个簇内的 L-sensor 被俘获不会影响其他簇 L-sensor 之间会话密钥的建立。假设网络中有 W 个 H-sensor(即存在 W 个簇),被俘获的 L-sensor 均匀分布于 W 个簇中。如果有 x 个 L-sensor 被俘获,则每个簇有$\lceil\frac{x}{W}\rceil$个 L-sensor 被俘获,这时安全会话密钥泄露的概率为

$$C(r)=\sum_{j=q}^{r}\left(1-\left(1-\frac{r}{M}\right)^{\lceil\frac{x}{W}\rceil}\right)^{j}\frac{p_{LH}(j)}{p} \tag{5}$$

图 5(a)和(b)分别给出了密钥池大小为 $P=10\ 000$,H-sensor 数目为 $W=20$ 的 HWSN 中,取 $q=1$ 和 $q=3$ 时,AP、QC 和 RCP 三种密钥管理中安全会话密钥泄露的概率与被俘获节点数目之间的关系。由图 5 可知,如果网络中有相同数目的节点被俘获,RCP 方案中安全会话密钥泄露的概率最小;随着 q 增加,三种方案的安全会话密钥泄露的概率都会降低,RCP 方案中密钥泄露的概率降低幅度最大;当网络中节点被俘获的数目较小时,安全会话密钥泄露的概率也较小,随着网络中节点被俘获数目的逐渐增大,三种方案中安全会话密钥泄露的概率都随之增加,而 RCP 方案中密钥泄露的概率增加幅度要明显小于另外两种方案,尤其是在 $q=3$ 时更为明显。



(a)安全会话密钥泄露的概率与被俘获节点数目之间的关系(q=1)　(b)安全会话密钥泄露的概率与被俘获节点数目之间的关系(q=3)

图5　安全会话密钥泄露概率与俘获节点关系

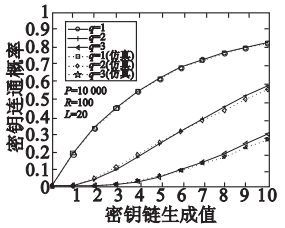


图6　密钥连通性理论分析与仿真实验结果的比较

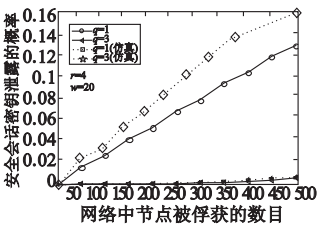


图7　网络安全性理论分析与仿真实验结果的比较

通过上述分析可以看出,AP 与 QC 方案中的所有节点都是从全局的密钥池中选取预置密钥,因此任何一个节点被俘获后都有可能影响到网络中其他会话密钥的建立,而在本文提出的方案中,每个簇都有不同的阶段标志,L-sensor 利用本簇的阶段标志与 ID 号产生密钥链生成值并计算会话密钥,因此某个簇内 L-sensor 被俘获并不会影响到其他簇内节点间会话密钥的建立,而是将安全会话密钥泄露的可能局限于本簇内,这就大大提高了整个网络的安全性。

5　仿真实验

本章采用 MATLAB 进行仿真实验,并与第 4 章的理论分析结果比较。在 1 000 m × 1 000 m 的范围内随机生成 5 000 个 L-sensor 节点,20 个 H-sensor 节点,H-sensor 预置 100 个密钥链生成值。图 6 给出了选取不同门限值时,密钥连通性理论分析与仿真实验结果的比较。如图 6 所示,当 $q=1$ 时,仿真实验与理论分析的结果几乎是相同的,而 $q=2$,$q=3$ 时,两者的结果也是基本吻合的。比较图 4 与 6 可知,本文提出的方案能够解决传统密钥管理方案负载需求较大的问题。

图 7 给出了 L-sensor 预置 4 个密钥链生成值,被俘获节点均匀分布于各个簇,取 $q=1$ 和 $q=3$ 时,网络安全性理论分析与仿真实验结果的比较。如图 7 所示,随着被俘获节点数目的不断增大,两者的安全会话密钥泄露的概率都随之增大,仿真实验结果的增加幅度要略微大于理论分析的结果,这主要是由于在仿真过程中某些簇的被俘获节点数目要大于平均值,同时簇内 L-sensor 节点的数目较大,节点被俘获后受到影响的节点数目也就相应会增加。比较图 5 与 7 可知,本文提出的方案能够解决大规模 L-sensor 被俘获而带来的安全问题。

6　结束语

本文分析了当前 HWSN 中密钥管理方案存在的问题,提出了一种适合 HWSN 的高效安全的密钥管理方案。该方案针对 HWSN 的特点,采用随机数生成和分组链接技术建立会话密钥,通过在不同簇内广播不同的阶段标志来提高整个网络的安全性。理论分析表明该方案能够在保证连通性的前提下大大减少节点的存储负载,即使网络中有大量 L-sensor 被俘获,安全会话密钥泄露的概率也很小,仿真实验验证了该方案的正确性与可行性。下一步工作将研究 HWSN 中组播通信的密钥管理方案。

参考文献:

[1] AKYILDIZ I, SU W, CAYIRCI E. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8):102-114.

[2] 苏忠,林闯. 无线传感器网络密钥管理的方案和协议[J]. 软件学报,2007,18(5):1218-1231

[3] PERRIG A, SZEWCZYK R, TYGAR J D. *et al*. SPINS: security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534

[4] ESCHENAUER L, GLIGOR V. A key management scheme for distributed sensor networks[C]//Proc of the 9th ACM Conf on Computer and Communications Security. New York: ACM Press, 2002: 41-47.

[5] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]//Proc of IEEE Symp on Security and Privacy. Washington: IEEE Computer Society, 2003, 197-213.

[6] LIU D, NING P, LI R. Establishing pairwise keys in distributed sensor networks[J]. ACM Trans on Information and System Security. 2005, 8(1):41-77.

[7] LIU D, NING P. Location-based pairwise key establishments for static sensor networks[C]//Proc of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks. New York: ACM Press, 2003: 72-82.

[8] DU X, XIAO Y, GUIZANI M, *et al*. An effective key management scheme for heterogeneous sensor networks[J]. Ad hoc Networks, 2007, 5(1):24-34.

[9] LU K, QIAN Y, HU J. A framework for distributed key management schemes in heterogeneous wireless sensor networks[J]. IEEE Trans on Wireless Communications, 2008, 7(2):639-647.

[10] TRAYNOR P, KUMAR R, HEESOOK C, *et al*. Efficient hybrid security mechanisms for heterogeneous sensor networks[J]. IEEE Trans on Mobile Computer, 2007, 6(6):663-677.

[11] DU W, DENG J, HAN Y S, *et al*. A pairwise key predistribution scheme for wireless sensor networks[J]. ACM Trans on Information and System Security, 2005, 8(1):41-47.