基于可信基站的 SPINS 协议研究与改进

朱 磊, 吴 灏, 王清贤
(解放军信息工程大学 信息工程学院, 郑州 450002)

摘 要: SPINS 安全协议基于可信基站, 为无线传感器网络数据传输提供了一套安全的解决方案。通过分析 SPINS 协议, 指出其中存在的不足, 并对其进行了三方面的改进, 即引入全局密钥、支持网络扩展和加入密钥更新机制。分析表明, 改进的方案具有较好的扩展性, 能有效支持路由信息的认证, 新的密钥更新机制在一定程度上增加了安全性。

关键词: 无线传感器网络; 安全; SPINS 协议; 网络扩展; 密钥更新
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2010)06-2331-04
doi:10.3969/j.issn.1001-3695.2010.06.096

Security research and improvement of SPINS protocol

ZHU Lei, WU Hao, WANG Qing-xian
(*School of Information Engineering, PLA Information Engineering University, Zhengzhou* 450002, *China*)

Abstract: SPINS security protocol, which is based on the trusted base station, provides a solution for wireless sensor networks security. By analyzing the SPINS, this paper pointed out some existing shortages, and gave three improvements: the global key, network expansion, key update. The following analysis shows that, the improvement scheme has good scalability and effectively supports the authentication of routing messages. The new mechanism of key update increases the security level of WSNs to a certain extent.

Key words: wireless sensor networks(WSNs); security; SPINS protocol; network expansion; key update

无线传感器网络[1~3](WSNs)是一种由大量低成本、资源受限的传感器节点通过无线传输介质连接构成的无线网络, 通过节点间的协同工作采集和处理网络覆盖区域中的目标信息。WSNs 通常配置在无人值守或不可控制的地区, 部署前网络拓扑无法预知, 部署后也经常变化。其通信环境是开放的, 传感器节点部署后需要持续工作, 容易遭受破坏和干扰, 暴露的节点缺乏专门维护, 其安全性将受到严重的挑战; 同时, 传感器节点在存储、计算、能量和通信带宽方面的有限性[4], 使得其中的安全问题更加难以解决。近些年来, 随着无线传感器网络技术的发展以及应用领域的不断扩大, WSNs 的安全性问题越来越受到重视[5], 尤其是一些部署在危险环境中的 WSNs 应用, 如战场指挥、商业安全监控等。在这些应用中, 需要对传输的数据进行加密和认证保护。

通常传感器网络由节点和基站构成。连接传感网与外部网络的基站, 与普通节点相比具有较大的存储空间以及充足的能量供应, 并且能够保证足够的安全性, 不易受到破坏, 存储其中的秘密也不会泄露, 因此可以认为基站是可信的。基于可信基站, Perrig 等人[6]提出了无线传感器网络上的安全协议(security protocols for sensor network, SPINS); LEAP[7]面向大规模分布式的 WSNs, 支持网内数据处理; TinyPK[8]是 LEAP 的一个替代品, 用非对称密码机制实现 WSNs 的安全; ZigBee[9]是目前业界流行的一套协议, 为 WSNs 提供了高安全性, 但是能耗较高; 此外, TinySec[10]、SenSec[11]、MiniSec[12]和 FlexiSec[13]在链路层上提出了各自的安全方案。在以上这些协议中, SPINS 安全框架适用于各种无线传感器网络, 许多相关研究工作以 SPINS 作为基础展开, 但是 SPINS 设计上存在着缺乏密钥的更新机制、不支持网络拓展等一些不足[14,15]。针对 SPINS 出现的缺陷, 本文提出了一些改进, 在一定程度上提高了协议的安全性。本文会用到以下八个符号:

A, B 表示安全对象, 也就是节点;

ID_A 表示节点 A 的 id 号;

N_A 表示节点 A 产生的一个 nonce 随机数;

$M_1 | M_2$ 表示消息 M_1 和 M_2 的链接;

K_{AB} 表示节点 A、B 之间共享的密钥;

IV 表示初始向量;

$\{M\}(K_{AB}, IV)$ 表示使用密钥 K_{AB} 和初始向量 IV 在某种加密模式下加密所得的密文, 加密模式有分组链接(CBC)、输出反馈(OFB)或计数器(CTR)模式等;

$MAC(K_{AB}, M)$ 表示由密钥 K_{AB} 生成的消息 M 的消息认证码。

1 SPINS 协议

SPINS[6]是 Perrig 等人提出的一套针对无线传感器网络的安全解决方案。考虑到传感器网络资源受限的特点以及安全机制带来的负载, SPINS 把自己建立在对称密钥体系上, 通过两大组成部分, 即 SNEP(secure network encryption protocol)和 μTESLA(micro timed efficient stream loss-tolerant authentication), 在 WSNs 中实现了网络中数据的机密性、完整性、真实性

收稿日期: 2009-10-16; **修回日期**: 2009-11-25

作者简介: 朱磊(1982-), 男, 江苏南通人, 硕士研究生, 主要研究方向为网络信息安全(zlintact@gmail.com); 吴灏(1965-), 男, 江苏无锡人, 教授, 主要研究方向为网络信息安全; 王清贤(1960-), 男, 河南新乡人, 教授, 主要研究方向为网络信息安全.

和新鲜性。

SPINS 协议采用节点和可信基站之间预共享主密钥的模型,网络部署前每个节点都与基站初始化一个共享的主密钥。预共享的一系列主密钥作为传感器网络中可信计算基的一部分,确保了整个 SPINS 协议的安全。

在 SNEP 中,为了达到双向认证、数据机密性、完整性和新鲜性,使用了计数器(counter,CTR)模式的加密机制和消息验证码(message authentication code,MAC)。A 发送到 B 的完整消息是:

$$A\rightarrow B:\{D\}(K_{enc},C),\mathrm{MAC}(K_{mac},C|\{D\}(K_{enc},C))$$

其中:D 表示加密前的消息;K_{enc} 和 K_{mac} 分别表示加密密钥和 MAC 密钥;C 表示计数器的值。在加密时,C 和计数器链接模式提供了加密的语义安全;在 MAC 时,C 与密文数据一起链接计算,提供了重放保护和弱新鲜性。SNEP 协议要实现强新鲜性,则还需要引入 nonce 随机数。

μTESLA 利用散列函数的单向特性,将秘密延迟发布,实现了对广播报文的认证。基站首先使用单向散列函数 H 生成一个单向密钥链 $\{K_0,K_1,\cdots,K_n\}$。其中 $K_i=H(K_{i+1})$,由 K_{i+1} 容易计算得到 K_i,而由 K_i 则无法计算得到 K_{i+1}。将网络生存时间分为若干个时间片,在每一时间片对应密钥链中的一个密钥。在第 i 个时间片内,基站发送认证数据包,然后延迟一个时间 δ 后公布密钥 K_i。节点接收到该数据包后首先保存在缓冲区中,等待接收到最新公布的密钥 K_i,然后使用其目前保存的密钥 K_j,并使用 $K_j=H^{i-j}(K_i)$ 来验证密钥 K_i 是否合法。若合法,则使用 K_i 认证缓冲区中的数据包。使用 μTESLA,攻击者很难获取或伪造认证密钥,发布合法的广播报文。

SPINS 协议实现简单,具有较小的负载,而且各个节点与基站间使用的密钥不相关,抗毁性好,但是 SPINS 也存在一些不足[5,14,15]:基站存储与网络中所有节点对应的主密钥,需要有较大的存储空间;SPINS 没有考虑到网络扩展,部署后不能加入新节点;没有密钥更新,SNEP 中的加密密钥和 MAC 密钥不会改变;不能抵御 DoS 攻击。

2 改进的方案

2.1 引入全局密钥

在无线传感器网络中,节点参与路由选择与消息转发。开放的无线网络环境中传输的路由信息容易被恶意节点截获、窜改、重放甚至伪造。廉价的节点部署容易受到敌人的物理捕获,敌人进而可以发起各种形式的攻击,威胁整个网络的安全。Karlof 等人[16]详细阐述了 WSNs 中安全路由面对的威胁。

在 WSNs 中,实现路由安全的一种简单方法就是提供对路由消息的验证。SPINS 协议利用 μTESLA 机制来解决路由安全,有两种方法:a)节点将加密的路由消息传给基站,基站再用 μTESLA 机制广播认证的路由消息;b)节点用 μTESLA 机制广播认证的路由消息。前者依赖基站转发路由消息,通信开销较高,同时加重了基站的负载;后者需要在网络中初始化节点的 μTESLA 初始密钥,这是通过点到点的单播加密传输完成的,对于节点数为 n 的网络初始化通信开销为 $O(n^2)$。

通过引入网络共享的全局密钥 K_g,验证路由消息,可以避免使用 μTESLA 机制降低网络负载。可验证的路由消息格式为 DATA,MAC(K_{tg},DATA),K_{tg} 由 K_g 临时生成。全局密钥能够抵抗非法节点对路由的破坏,但对内部被捕获妥协节点的攻击则无能为力。对这种情况,发现捕获节点以后,网络密钥 K_g 立即更新,新的网络密钥对捕获节点保密。

1)网络密钥 K_g 的生成

a)每个节点部署时都存有初始网络密钥 K_{g0}。节点加入时由基站判断当前 K_g 是否为 K_{g0},如果不是,基站向新节点发送加密的 K_g。

b)待发的路由消息在发送方用临时网络密钥 K_{tg} 计算出 MAC 码,在接收方用 K_{tg} 进行验证。构造路由报文时,在报文中添加一个由发方提供的随机数 ctr,取目的地址 dest、源地址 src、报文长度 len 连同 ctr 组成新的随机数 R,R = dest|src|len|ctr。K_{tg} 由 K_g 和随机数 R 临时生成 $K_{tg}=F_{Kg}(R)$。

2)网络密钥 K_g 的更新

K_g 在网络中出现节点妥协情况下需要进行更新。此时,基站随机生成一个新的 K_g,并将其加密单播传送给各个可信节点。

2.2 支持网络扩展

SPINS 中基站与新节点间没有共享密钥,也没有秘密渠道使两者协商产生密钥,因此 SPINS 不支持网络扩展,一旦部署后新节点不能加入网络。为了支持网络扩展,修改了原协议的密钥预共享机制,使之支持新进节点的加入,然后设计了节点加入的具体流程。

2.2.1 密钥预共享机制

SPINS 中基站与网络中各个节点的主密钥是事先预置在基站和各节点中的,密钥间有很强的不相关性,某个密钥的泄露对其他密钥没有影响。但是 SPINS 的预共享机制不支持网络扩展,而且基站需要存储大量的节点密钥。借鉴 LEAP[7]中预主密钥生成主密钥的方法,改进原协议中的预共享机制,具体机制如下:

基站中只需预存一个预主密钥 K_{pm}。普通节点部署时根据预主密钥 K_{pm} 和节点的 id 号生成初始网络密钥 K_{g0} 和节点的主密钥 K_i,将这两个密钥存入节点中。计算方法采用一个单向的伪随机函数 $F_x(y)$。为了节省节点的存储资源,在这里用 MAC-CBC 实现 $F_x(y)$,便于代码重用。$F_x(y)$ 可表示为 MAC(x,y)。

$$K_{g0}=F_{Kpm}(0)=\mathrm{MAC}(K_{pm},0)$$
$$K_i=F_{Kpm}(i)=\mathrm{MAC}(K_{pm},i)$$
$$IV_{i0}=F_{Ki}(0)=\mathrm{MAC}(K_i,0)$$

其中:K_i 表示节点 i 与基站共享的主密钥;i 表示节点的 id 号;IV_{i0} 表示节点 i 初始的 IV。

基站需要节点的主密钥时,可以根据预存的 K_{pm} 和节点的 id 号直接计算出来。新节点的部署也很容易,只需计算它的主密钥然后存入节点,无须对基站进行处理。改进的预共享机制支持网络扩展,同时保持了 SPINS 原有节点间主密钥的不相关性,也为基站节省了存储空间。

2.2.2 节点加入流程

新节点加入网络时,需要对其进行可信验证,即新节点需要向网络出示可信任的凭据。如果验证成功,则该节点可以加入网络,这时要进一步配置网络参数,使其加入后能正常工作。如果验证失败,则将其看做非法节点,拒绝其访问。在本方案中,节点可信的凭据为通过预置在节点中的主密钥 K_i 计算而得的节点 MAC 密钥 K_{i-mac},必备的网络参数有节点与基站的

加密密钥 K_{enc}、密钥 K_{mac}、网络密钥 K_g 等。具体流程(图 1)如下:

a)新节点 S 寻找网络,查找它的邻居节点。

b)邻居节点 N 向新节点 S 回应,返回它的 id。

c)新节点 S 向邻居节点 N 发送入网认证请求。

$$S\rightarrow N:\text{data}_1,\text{MAC}(K_{s\text{-mac}},IV_{s0}|\text{data}_1)$$

其中:data_1 是请求标志;IV_{s0} 为节点 S 与基站 B 共享初始向量的初始值,$IV_{s0}=\text{MAC}(K_s,0)$;$K_{s\text{-mac}}$ 是 S 与 B 共享的 MAC 密钥,可由 K_s 和 IV_s 计算得到,具体方法见 2.3 节。

d)邻居节点 N 向基站 B 发送新节点 S 的请求消息

$$N\rightarrow B:s,\text{data}_1,\text{MAC}(K_{s\text{-mac}},IV_{s0}|\text{data}_1),\text{MAC}(K_{n\text{-mac}},IV_{ni}|s|\text{data}_1|\text{MAC}(K_{s\text{-mac}},IV_{s0}|\text{data1}))$$

其中:$K_{n\text{-mac}}$ 为邻居节点 N 与基站 B 共享的 MAC 密钥,IV_{ni} 为当前节点 N 与基站 B 的 IV。

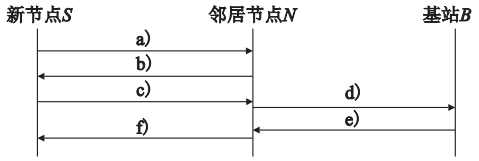

图1　节点加入

e)基站 B 收到新节点 S 的入网消息后,通过提取节点 S、N 的节点标志 s、n,与基站中的黑名单(已妥协或失效节点)对比。如果 n 在黑名单中,则丢弃该消息;如果 s 在黑名单中,则判断 s 为非法节点;如果均不在黑名单中,则计算出节点 S、N 的当前 MAC 密钥 $K_{s\text{-mac}}$、$K_{n\text{-mac}}$。利用这两个密钥对收到的消息进行验证,如果验证成功,则可判定新节点 S 为合法节点;否则,判断 S 为非法节点,拒绝该节点接入网络,然后向节点 N 发送验证消息。

这里消息有两种形式:

(a)如果节点 S 非法,则发送

$$B\rightarrow N:\text{data}_2,\text{MAC}(K_{n\text{-mac}},IV_{nj}|\text{data}_2)$$

其中:data_2 是非法标志,IV_{nj} 为当前 N、B 共享的 IV。

(b)如果节点 S 合法,则发送

$$B\rightarrow N:\text{data}_2,s,n,|K_g|(K_{s\text{-enc}},IV_{sj}),\text{MAC}(K_{s\text{-mac}},IV_{sj}|n|\{K_g\}(K_{s\text{-enc}},IV_{sj})),\text{MAC}(K_{n\text{-mac}},IV_{nk}|\text{data}_2|s|n|\{K_g\}(K_{s\text{-enc}},IV_{sj})|\text{MAC}(K_{s\text{-mac}},IV_{sj}|n|\{K_g\}(K_{s\text{-enc}},IV_{sj})))$$

其中:data_2 是合法标志;s 为节点 S 的 id;K_g 为当前的网络密钥。报文中 $\{K_g\}(K_{s\text{-enc}},IV_{sj})$ 以及 MAC 中相应的部分是只有当前的 K_g 不为 K_{g0} 时才出现,若 $K_g=K_{g0}$,报文格式为 data_2,s,n,$\text{MAC}(K_{n\text{-mac}},IV_{nk}|\text{data}_2|s|n)$。

f)消息到达节点 N,节点 N 对消息验证。如果消息为步骤 e)中的(a)形式且验证成功,则表示新节点 S 不合法,邻居节点 N 拒绝新节点 S 入网,并且之后不会向节点 S 发送任何消息。

如果消息为步骤 e)中的(b)形式且验证成功,则表示节点 S 可信,允许其加入网络,这时节点 N 向 S 发送入网消息,如图 1 阶段 f)。

如果消息步骤 e)的(b)中包含 K_g,$N\rightarrow S:n,\{K_g\}(K_{s\text{-enc}},IV_{sj}),\text{MAC}(K_{s\text{-mac}},IV_{sj}|n|\{K_g\}(K_{s\text{-enc}},IV_{sj}))$;否则,$N\rightarrow S:n$。其中:$n$ 为邻居节点 N 的 id。

新节点 S 收到该消息后即加入网络,进一步得到当前网络密钥 K_g。节点 S 根据 μTESLA 协议,从基站 B 取得广播密钥链当前密钥、μTESLA 时间段间隔等一些初始 μTESLA 参数,之后便可以验证基站的 μTESLA 广播报文。

2.3　密钥更新机制

SPINS 没有提供密钥更新机制,节点部署后网络中的密钥,尤其是关键的加密密钥、MAC 密钥并不改变。采用密钥协商生成新密钥的方式会产生大量的通信开销以及时延,不适合于 WSNs。这里采用的是基于共享变量的密钥自更新机制,SPINS 中,节点 i 与基站通信的消息描述如下:

$$i\rightarrow B:\{\text{data}\}(K_{enc},IV),\text{MAC}(K_{mac},IV|\{\text{data}\}(K_{enc},IV))$$

发送的数据以计数器模式(CTR)加密,K_{enc} 为双方的加密密钥,K_{mac} 为双方的 MAC 密钥。IV 为双方共享的初始向量,每次发送方发送一个消息/接收方收到一个消息,各自存储的 IV 都加 1。SPINS 中,K_{enc}、K_{mac} 分别由 $K_e=\text{MAC}(K_i,1)$ 和 $K_m=\text{MAC}(K_i,2)$ 计算得来,在整个网络生存期内不会改变。

为了抵抗密码分析,在原有的 SPINS 基础上加入密钥更新机制,使得每次发送/接收所对应的密钥都不同。由于 WSNs 资源有限,网络中进行密钥交换,需要消耗一定的能量,带来一定的延时,并不适合 WSNs 的应用。降低网络负载的一个较好的办法是用双方共享的一个可变数值与原有的密钥 k 混合,得出一个共享的新密钥 k'。新的加密密钥、MAC 密钥可以通过以下公式计算出来:

$$K_{enc}=\text{MAC}(K_e,IV),\ K_{mac}=\text{MAC}(K_m,IV)$$

IV 初始值为 $F_{Ki}(0)=\text{MAC}(K_i,0)$,其值随每个消息而自加 1。因此,每次对消息加密和 MAC 验证时所用的密钥不同,实现了密钥的一次一密,一定程度上增加了 SPINS 的安全性。发送方在发送方向与接收方在接收方向上共享一个 IV,并且保持同步,在收发双方之间应该有两对相互独立的 IV。

要保证一次一密,IV 必须不能重复,同时,由于采用计数器模式加密,也要求 IV 不能重复,为此采用 4 Byte(32 bit)作为 IV 的长度。可以证明 4 Byte 的 IV 不会出现重复。32 bit 的 IV 可以表示 2^{32} 个消息报文,假设每个报文长度为 30 bit,网络传输速率为 250 kbps(这是目前 WSNs 常用的速率),那么节点连续不停地发送数据最少可以发 $(2^{32}\times 30)/(250\times 2^{10}\times 60\times 60\times 24)\approx 5.8$ d。这个数字对无线传感器网络已经足够了,在网络的生存期内可以保证 IV 不会重复。

3　性能分析

3.1　安全性能

1)支持网络扩展没有改变 SPINS 的安全性　新节点能够加入网络,是由于节点中预置了与基站共享的主密钥,而基站通过存储的预主密钥和新节点 id 可以计算出相同的节点主密钥。假设基站可信,存储在其中的预主密钥不会泄露,因此改进的方案具有与原方案相同的安全性。

2)加入的密钥更新机制实现了一次一密　每个报文使用的密钥均不相同。与原协议不变的加密、MAC 密钥相比,改进的方案在安全性上有一定程度的加强。

3)使用全局网络密钥验证路由信息的安全　敌人发动的窜改、伪造攻击容易被基站和应用程序发现。由于 K_{tg} 生成时加入了随机数,敌人对数据进行重放攻击或选择性转发攻击也会被发现。如果敌人利用非法节点发动拒绝服务攻击(DoS)或洪泛攻击(HELLO flood),由于恶意数据不能被认证,容易被基站或应用程序发现,并通过访问控制机制进行隔离。

当节点被俘而未被发现时,全局密钥机制的安全性要稍弱些。SPINS 协议使用 μTESLA 认证,如果某个节点被捕获而妥协,敌人只知道该节点的 μTESLA 广播密钥链,只能伪造该节点发布的广播路由消息。对于修改的方案,一个节点被俘,敌人可以根据泄露的全局密钥伪造出任意的路由消息,而一旦发现被俘节点,两种方案都能将其从网络可信节点中剔除出去,恢复路由安全。

表 1 为协议修改前后安全性能基本比较,可以看出修改后的方案对网络中的各种攻击是十分健壮的。

表 1 方案路由安全性比较

安全方案	窜改	伪造	重放攻击	选择性转发	DoS 攻击	HELLO flood
原协议	抵御	抵御	不抵御	不抵御	不抵御	抵御
修改后	抵御	抵御	抵御	抵御	部分抵御	抵御

3.2 负载分析

在系统中,节点 id 为 2 Byte,随机数、*IV* 为 4 Byte,预主密钥、主密钥、加密密钥、认证密钥为 8 Byte。

3.2.1 存储开销

修改后的方案在网络部署时基站只存一个预主密钥 8 Byte,普通节点存储主密钥和全局密钥,共 16 Byte。原协议基站需要存储 8n Byte(n 为网络中节点数目),普通节点中存储开销为 8 Byte。

3.2.2 计算开销

基站与节点通信事先要通过预主密钥生成主密钥、*IV*、K_e、K_m,节点要通过主密钥生成 *IV*、K_e、K_m。通信时,要临时计算加密密钥、MAC 密钥或临时网络密钥,然后用计算得来的密钥加密、认证数据。计算开销最多为一个加密操作和三个 MAC 操作。

3.2.3 通信开销

在路由安全方面,SPINS 利用 μTESLA 广播认证的路由消息,如果节点本身不广播认证路由,通过将路由信息加密传给基站,利用基站广播,那么通信开销为一个单播消息和一个广播消息;如果节点自己广播认证路由消息,通信开销为一个广播消息,但是节点在之前必须将自己的 μTESLA 初始密钥通过基站发到其他节点中,通信开销为 n 个单播消息。改进后的方案节点发送认证路由消息的通信开销为一个广播消息。

为了支持网络扩展,新节点加入网络需要的通信开销为四个单播消息。

3.2.4 可扩展性

如果传感器节点数目增加,传感器节点需要存储的密钥数量几乎保持不变。对传感器节点计算能力、通信负荷要求也是确定的,因此修改方案是可扩展的。

表 2 为两种方案负载的基本比较。通信开销的单位为一个加密消息长度。修改的方案扩展性好,对基站的存储需求降低,而且计算和通信开销没有明显增加。

表 2 方案负载比较

安全方案	存储开销	计算开销	通信开销		可扩展性
			路由安全	节点加入	
原协议	基站 8n Byte,一个 ENC + 节点 8 Byte 一个 MAC	2 或 $n+1$	无		差
修改后	基站 8 Byte,一个 ENC + 节点 16 Byte 三个 MAC	1	4		较好

4 结束语

SPINS 是一种基于可信基站的无线传感器网络安全协议。本文在分析 SPINS 的基础上,针对其存在的不支持网络拓展、无密钥更新机制等问题,提出了相应的改进措施。分析表明,本方案对网络扩展有较好的支持,自更新的密钥机制在一定程度上增强了 SPINS 的安全性,全局网络密钥验证路由信息降低了通信开销。

参考文献:

[1] 任丰原,黄海宁,林闯. 无线传感器网络[J]. 软件学报,2003,14(7):1282-1290.

[2] KARL H,WILLIG A. 无线传感器网络协议与体系结构[M]. 邱天爽,等译. 北京:电子工业出版社,2007:6-50.

[3] AKYILDIZ I F,SU W,SANKARASUBRAMANLAM Y,*et al*. Wireless sensor networks:a survey[J]. Computer Networks,2002,38(4):393-422.

[4] HILL J,SZEWCZYK R,WOO A,*et al*. System architecture directions for networked sensors[J]. ACM SIGPLAN Notices,2000,35(11):93-104.

[5] 苏忠,林闯,封富君,等. 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.

[6] PERRIG A,SZEWCZYK R,WEN V,*et al*. SPINS: security protocols for sensor networks[J]. Wireless Networks,2002,8(5):512-534.

[7] ZHU S,SETIA S,JAJODIA S. LEAP: efficient security mechanisms for large-scale distributed sensor networks[C]//Proc of ACM Conference on Computing and Communication Security. Washington DC: ACM Press,2003:62-72.

[8] WATRO R,KONG D,CUTI S F,*et al*. TinyPK :securing sensor networks with public key technology[C]//Proc of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks. Washington DC: ACM Press,2004:59-64.

[9] ZigBee Alliance. ZigBee document 053474r17,version 1.0[S/OL]. (2008-01). http://www.zigbee.org.

[10] KARLOF C,SASTRY N,WAGNER D. TinySec:a link layer security architecture for wireless sensor networks[C]//Proc of ACM International Conference on Embedded Networked Sensor Systems. Maryland: ACM Press,2004:162-175.

[11] LI T,WU H,WANG X, *et al*. SenSec:sensor security framework for TinyOS[C]//Proc of the 2nd International Workshop on Networked Sensing Systems. San Diego:IEEE Press,2005:145-150.

[12] LUK M,MEZZOUR G,PERRIG A,*et al*. MiniSec:a secure sensor network communication architecture [C]//Proc of the 6th International Conference on Information Processing in Sensor Networks. Cambridge:ACM Press,2007:479-488.

[13] DEVESH J,DHIREN P,KANKAR D. FlexiSec:a configurable link layer security architecture for wireless sensor networks[J]. Journal of Information Assurance and Security,2009,4(6):582-603.

[14] 程宏兵,王江涛,杨庚. SPINS 安全框架研究[J]. 计算机科学,2006,33(8):106-108.

[15] 彭志娟,王汝传,孙力娟. 无线传感器网络 SPINS 安全协议分析与改进[J]. 无线通信技术,2007,16(1):14-16.

[16] KARLOF C,WAGNER D. Secure routing in wireless sensor networks: attacks and countermeasures[J]. Ad hoc Networks,2003,1(2-3):293-315.