第 37 卷 第 24 期
Vol.37 No.24

计 算 机 工 程
Computer Engineering

2011 年 12 月
December 2011

• 安全技术 •

文章编号：1000—3428(2011)24—0123—03 文献标识码：A 中图分类号：TP393.08

一种改进的无线传感器网络密钥管理方案

周文粲，赵一鸣

(复旦大学软件学院，上海 200433)

摘 要：在无线传感器网络中，针对已有动态更新密钥管理方案的无身份认证、可扩展性差等问题，提出一种实用的无线传感器网络密钥管理方案。采用增加身份认证模块的方法，设计可行的新节点加入机制。分析结果表明，与原方案及同类密钥管理方案相比，该方案在保持安全高效的同时，具有更好的可扩展性和网络连通性。

关键词：无线传感器网络；密钥管理；一次一密；身份认证；可信服务器

Improved Key Management Scheme for Wireless Sensor Network

ZHOU Wen-can, ZHAO Yi-ming

(Software School, Fudan University, Shanghai 200433, China)

【Abstract】Based on the existing dynamically updated key management scheme on Wireless Sensor Network(WSN), this paper improves its flaw of no identity authentication and weak scalability by adding identity authentication modules and proposes a new key management scheme and a feasible new node joining mechanism on WSN. Compared with the original one and similar key management schemes, this scheme maintains efficiency while ensuring higher security and bringing in better scalability, network connectivity and other features.

【Key words】Wireless Sensor Network(WSN); key management; one-time pad; identity authentication; trusted server

DOI: 10.3969/j.issn.1000-3428.2011.24.041

1 概述

无线传感器网络(Wireless Sensor Network, WSN)是一种特殊的 Ad-hoc 网络，近年来得到人们的极大关注，它具有快速展开、抗毁性强、无需固定网络支持等优点，在军事侦察、环境监测、交通管理等领域很实用。

传感器节点往往部署在无人看护、甚至是敌对的环境中，因此安全问题非常重要，节点间的通信必须加密，但传感器节点受到能源、计算能力、存储空间及通信能力的限制，导致 WSN 上的密钥管理机制和传统无线网络有很大差异。

近年来，一系列 WSN 上的密钥管理方案被提出，根据密钥体制可分为对称和非对称方案。由于非对称体制资源消耗过大，即使是计算效率较高和存储要求较低的 ECC 体制，也与对称密钥体制差距很大，使得它在 WSN 中的应用受到极大限制。

在对称加密体制中，又分为信任服务器模式和预分配模式。其中，预分配体制应用最为广泛，有随机预分配、确定性预分配和基于数据结构预分配之分。提出次数最多的是随机预分配密钥管理方案，最初由文献[1]提出方该案，被其他人不断改进，继而有 q-Composite 随机密钥预分配方案、多密钥空间随机密钥预分配方案、对称多项式随机密钥预分配方案等。随机预分配方案的弱点是网络连通性基于概率，不能提供确定的安全性；每个节点需要预存大量的密钥信息以便部署后与网络中任意可能的节点通信；未提供节点间的认证机制。而确定性预分配方案，如 Blom 方案[2]，计算负载太大，可扩展性较差。

另外一种应用较广泛的是基于位置敏感预分配方案[3-4]，属于基于数据结构预分配模式的一种，将监视区域划分为网格，节点被划分为组，部署时以组为单位部署到相应的网格中，部署前需根据网格的位置信息建立密钥空间，并为网格中每个节点配置密钥，配置工作繁重且耗时。

总结以前提出并在 WSN 上应用的各种密钥管理机制，主要存在如下问题：预分配机制的连通性差，对节点的存储要求高；采用地理位置信息密钥分配机制，部署时密钥配置工作繁重，部署较慢，网格间连通性差，节点部署出错就无法正常工作。而且它们都不能保证网络的全连通性。

文献[5]中的类似一次一密的动态可更新会话密钥管理方案(下称动态更新密钥方案)，满足部分要求，但存在一定的安全隐患以及不完整性，本文在它的基础上做了一些改进，在保证安全性的前提下仍能实现密钥管理的高效性以及良好的连通性。本文方案建立在这样的事实基础上：即实际上由于 WSN 节点通信距离能力的限制，节点只能与相邻节点直接通信并建立通信密钥。

2 预备知识

由于无线传感器网络自身的特点，无线传感器网络密钥管理方案主要的评价指标[6]有连通性、抗毁性、负载和可扩展性。

(1)连通性：通过节点安全连通概率来衡量连通性，即节点部署以后任意 2 个节点之间建立对密钥的概率。

(2)抗毁性：某些节点被捕获后，攻击方能破坏的节点个数占整个网络节点个数的百分比。

(3)负载：包括通信负载、计算负载、内存负载。

(4)可扩展性：能否方便快速地增加和删除新节点。

3 动态更新密钥方案的缺陷

本节简述文献[5]中提出的动态更新密钥方案以及它存在的问题。

基金项目：“十一五”国家密码发展基金资助项目

作者简介：周文粲(1989－)，女，硕士研究生，主研方向：密码学，信息安全；赵一鸣，副教授

收稿日期：2011-06-28 **E-mail：**wenc.zhou@gmail.com

3.1 动态更新密钥方案简述

本节介绍此方案的网络假设以及密钥管理机制。

(1)网络假设

原方案建立在如下的网络假设模型上:

1)无线传感器网络节点在部署阶段和部署后的一小段时间内，既没有攻击者进行物理攻击，也没有如无线电干扰攻击、窃听或者泛洪等攻击；当交换密钥完成后，网络中可以存在多种形式的攻击者。

2)无线传感器网络中，在节点无线电通信范围内，邻居节点进行直接的通信；非邻居节点需要经过中间节点多跳段才能进行通信。

(2)密钥管理机制

原方案是类似一次一密的动态会话密钥更新机制，这里的“一次”指一次会话过程。节点在部署前未加载任何密钥，部署后相邻节点通过协商生成初始会话密钥。密钥管理机制如图 1 所示，初始密钥协商如图 2 所示。

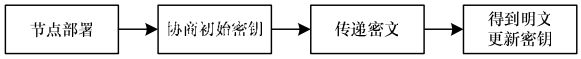

图 1 会话密钥管理示意图

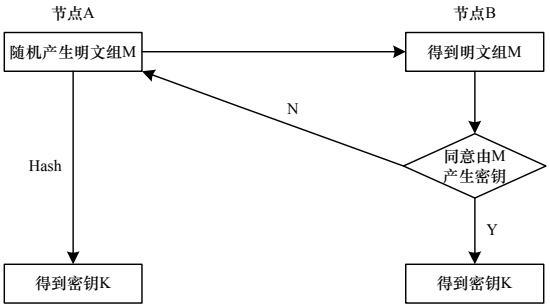

图 2 初始密钥生成过程

会话密钥更新过程如下:

节点间每次会话过程中使用一个密钥，会话结束后，发送和接收双方随即利用明文计算出新的会话密钥并更新，新密钥供下次会话使用。

3.2 动态更新密钥方案存在的问题

对动态更新密钥方案进行分析，可以发现存在如下 2 个问题:

(1)方案建立在较理想的网络假设中。此方案假设在节点部署阶段和部署之后的一小段时间内无恶意节点，在交换密钥之后可存在多种形式的攻击。因此，方案中并未为节点设置身份认证。而在实际环境中，无线传感器网络虽然可快速部署节点，但节点部署后，相邻的网络节点通过协商生成初始密钥需要过程和时间，依据图 2，每对相邻节点之间至少需要一次交互(若 B 不同意还将大于一次)，交互时间包括节点响应时间和 Hash 计算时间。

另外，原方案未说明节点部署之后，节点是与所有相邻节点均协商密钥，还是只与当前有会话要求的节点协商密钥。如果是前者，无线传感器网络中每个节点有多个相邻节点，多次交互的时间耗费无法忽略；如果是后者，会话需要事件触发，而触发的时间无法预计，并且无法与当前无会话要求的节点之间建立信任，恶意节点可以对尚未建立信任的节点对进行冒充或攻击。传感器网络通常部署在恶劣环境下，存在恶意节点的可能性很大。所以，此网络假设过于理想，未考虑在和邻居节点建立会话密钥之前如何保证节点的安全性，在实际应用中会存在较大的安全隐患。只要外部恶意节点在部署后与节点相互认证之间的时间段侵入网络，它不仅可以对网络中的节点进行物理攻击以及泛洪攻击等外部攻击，还可以无须经过认证冒充正常节点，对网络进行任意内部攻击，如女巫攻击、污水池攻击、虫洞攻击等，而且恶意节点的计算能力和资源都强于普通节点，甚至可以伪装成基站对网络进行控制，对网络的危害性极大。

(2)因为新节点无法向网络提供身份认证的途径，新节点无法加入。在此方案中，无线传感器网络是一次性部署，相邻节点在部署之后通过彼此协商的会话密钥进行通信和认证，而之后想要加入的新节点无任何途径向已部署的老节点认证，也无与老节点之间的会话密钥，所以，在原方案中新节点无加入网络的可行途径。

4 改进的动态可更新密钥管理方案

4.1 改进思路

对于动态更新密钥方案存在的以上 2 个问题，分析其主要原因在于此方案中只有消息认证，缺少身份认证模块，相邻节点协商初始密钥、新节点加入时都无身份认证，因此无法保证节点以及网络的安全性。为了增加身份认证模块，结合前文中提到的信任服务器模式，对此方面进行改进。

信任服务器模式依赖于通信节点双方都信任的服务器管理密钥，计算复杂度低，对节点存储和计算能力要求不高，节点的捕获也不会影响到网络其他节点的通信。但每次通信节点都需要与基站通信，网络过分依赖基站，网络的通信开销很大，网络的可扩展性与支持的网络规模取决于基站的能力。在信任服务器模式中，每次通信时节点都需要与基站通信，基站负载很大。

在下文的改进方案中利用信任服务器(即基站)作为类似公钥体制中的 CA 来认证身份，但只对节点进行初始认证，而且不是利用证书体制，而是使用共享密钥来认证，可以避免大部分负载问题。

4.2 具体改进方案

传感器网络配置好之后，每个节点预存一个与基站共享的唯一密钥。节点通过此共享密钥与基站通信得到与另一节点的会话密钥，替换掉原方案中的初始密钥协商过程，整个方案的过程如图 3 所示。

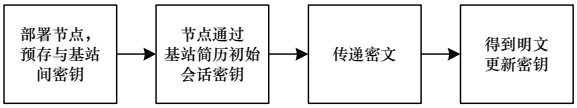

图 3 改进方案的会话密钥管理示意图

初始密钥生成过程如图 4 所示，参照 SPINS 协议[7]中的 SNEP 协议。

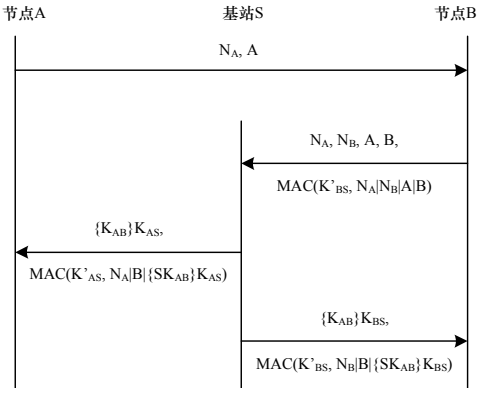

图 4 节点间初始密钥生成过程

在图 4 中，N_A 是由 A 产生的随机数；K_{AS} 和 K_{BS} 分别为 A、B 与基站的共享密钥；MAC(K, s)表示 s 使用 K 对称加密后的消息验证码；{M}K 表示用密钥 K 对消息 M 进行加密；SK_{AB} 为节点 A 和 B 的会话密钥。

假设节点 A 需要与节点 B 通信，则节点 A 先通知 B，然后 B 使用 B 与基站的共享密钥，与基站通信，基站生成 A 与 B 之间的会话密钥，分别加密发送给 A 和 B，作为 A 与 B 之间的初始会话密钥(即图 4 中的 SK_{AB})。

A 与 B 通过此初始密钥建立起连接之后，会话过程与原方案的密钥会话更新过程(如图 5 所示)一致，将信息传递和密钥更新过程同时完成。节点双方的初始会话结束时，使用 M'计算并更新会话密钥。会话密钥更新过程如下：发送节点 A 产生明文信息 M，使用当前会话密钥加密成密文，发送给密文，接收节点 B 收到密文后解密得到明文 M。此时双方的数据通信过程就已经完成，接下来通信双方更新其会话密钥。

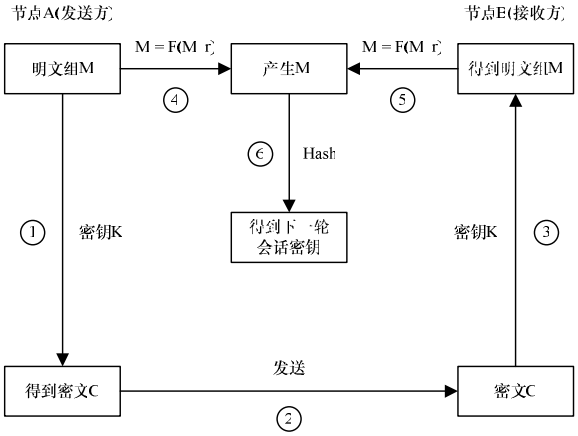

图 5　会话密钥更新过程

发送方和接收方都使用一个可逆的函数将 M 转换为 M'= F(M, r)，对 M'进行 Hash 计算得到密钥 K，作为下一轮会话密钥。其中，r 是一个可以调节的参数。该函数将相同的 M 转换成不同的 M'，为了在接收方和发送方同步每次 r 的值，可以将 r 的值隐藏在 M'中。r 是为了防止根据相同的明文进行 Hash 函数计算得到相同的密钥。

4.3　新节点加入过程

对于新节点的加入问题，只须配置新节点与基站的共享密钥，通过可靠信道将此共享密钥发给基站节点，对新节点进行认证后，即可将新节点加入传感器网络。节点可按照上面的过程通过基站与相邻节点建立会话密钥进行通信。

基站 S 对新节点 C 的认证过程如下：

(1)C→S: C, $\{C, N_C\}K_{CS}$

(2)S→C: $\{C, N_C, N_S\}K_{CS}$

认证成功即可将新节点 C 加入网络。

5　安全性和效率分析

本节对改进方案的安全性和效率进行分析，并与原方案、随机预分配方案进行比较。

(1)网络连通性

在本文的改进方案和原方案中，邻居节点均可以通过可信服务器的验证和初始会话密钥的分发，进行安全的直接通信。因此，在无线电范围内的邻居节点是全连通的。而随机预分配方案中是依概率连通，节点的连通性依赖密钥的预分配机制和部署；确定性预分配方案中的连通概率也为 1，但其特殊的部署方式会降低网络的灵活性[8]。

(2)抗毁性

动态更新密钥方案已经证明了动态会话更新密钥机制的安全性[7]。

由于动态更新密钥方案部署后的一段时间内可能会受到攻击，因此本文的改进方案中增加了可信服务器认证阶段，部署前每个节点预存一个与基站共享的唯一密钥。非本网络的恶意节点无预存密钥，无法进行身份伪装，无法冒充本网络的合法节点对网络进行 WSN 上的 DOS 攻击。由于每个节点都与基站有唯一密钥的认证，且每次会话密钥均会更新，节点的捕获也不会影响到网络其他节点的通信。

在密钥预分配方案中，节点被捕获会影响到此节点预存过会话密钥的部分节点，网络连通性越大，受影响的节点越多。

(3)负载

1)通信和计算负载

在无线传感器网络中，无线电通信消耗的能量比执行代码或计算所消耗的能量更多。动态更新密钥方案的通信开销优势是显而易见的。密钥的更新和密文信息一起传递，不需要专门的通信开销。计算出会话密钥只需一个可逆函数 F 运算和 n 次 Hash 运算的计算开销(n 为分段数)，无需额外通信开销。

本文的改进方案基本保持原方案的开销优势。只是增加了初始密钥协商中的通信开销。基站需与每对需要通信的邻居节点进行一次会话来建立节点间的初始密钥，而且邻居节点间需要通信时才会对基站发起请求，不会在初始形成网络后使网络中的流量剧增。节点间建立起初始密钥后就无须与基站进行协商，依然保持高效。

在随机预分配模式中，邻居节点间若不存在直接的共享密钥，每次会话都需要多次通信建立间接密钥，不仅通信负载大，而且响应慢；确定性预分配方案，如 Blom 方案[2]，计算复杂度高，计算负载很大；基于位置敏感预分配方案在部署阶段计算负载很大，影响部署速度。

2)密钥存储负载

在原方案中，节点无须部署密钥，而在本文的改进方案中，节点只须部署与基站的共享密钥，基站须预存与每个节点的唯一共享密钥，存储负载较大。

在预分配模式中，每个节点需要存储一定数量的密钥来保持好的连通性，节点的存储负载与网络的连通性成正比。

(4)可扩展性

原方案无法加入新节点。在本文方案中，新节点只须通过基站认证，协商好与基站的通信密钥，即可加入网络。网络的可扩展性良好。

在预分配模式中，随机预分配方案的可扩展性良好，只须给新节点随机预分配其他节点的密钥即可加入网络，但不能保证新节点的连通性；确定性预分配方案和基于位置敏感预分配方案的扩展性均很差，前者由于节点以及密钥固定，后者由于网格间连通性差。

在预分配模式中，网络规模取决于普通节点的存储能力。本文的方案中网络规模取决于基站的存储能力。

综合来说，动态更新密钥方案较于应用广泛的预分配方案，具有高效、部署简单、全连通的优点，但无法扩展，特定时间段内抗毁性差，本文的改进方案在保证安全性的前提下仍较高效、部署简单、全连通、可扩展性好，缺点是网络的抗毁性依赖于基站的安全性。

(下转第 128 页)