第36卷 第20期 计 算 机 工 程 2010年10月
Vol.36 No.20 Computer Engineering October 2010
·安全技术· 文章编号：1000—3428(2010)20—0134—03 文献标识码：A 中图分类号：TP393.08

基于树型结构的WSN密钥管理方案

于海霞，余梅生，吴晓娟，关 健
(燕山大学信息科学与工程学院，河北 秦皇岛 066004)

摘 要：为满足无线传感器网络的高安全性要求，提出基于树型结构的无线传感器网络动态密钥管理方案。采用MAC机制与节点唯一ID相结合的认证方法和逻辑树型密钥池，利用平衡二叉树实现动态密钥更新。实验结果表明，与原有方案相比，该方案的计算能耗和通信能耗均较小。

关键词：网络安全；无线传感器网络；动态密钥管理；树型结构

Wireless Sensor Network Key Management Scheme Based on Tree Structure

YU Hai-xia, YU Mei-sheng, WU Xiao-juan, GUAN Jian
(College of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China)

【Abstract】 To meet the high security needs of WSN, this paper proposes WSN dynamic key management scheme based on tree structure. MAC mechanism and unique ID method are combined. Logic tree key pool is used. Dynamic key update is realized by balance binary tree. Experimental results show that compared with existing schemes, this scheme needs littler energy consumption for computation and communication.

【Key words】 network security; WSN; dynamic key management; tree structure

1 概述

无线传感器网络(WSN)因其巨大的应用前景而受到学术界和工业界越来越广泛的重视。WSN由大量功能相同或不同的无线传感器节点以自组网络的方式构成，节点间的通信采用组播通信[1-2]。由于WSN网络规模庞大、节点数目多，且具有网络拓扑结构变化快、节点易失效和能源有限等特性，因此其安全问题面临严峻考验。

因为任何一种单一的密钥机制都不可能实现WSN所需的安全通信，所以LEAP协议[3]提出在传感器网络中，针对不同数据提供不同的安全机制，建立了4种密钥类型。LEAP协议的优点是任何节点受损都不会影响其他节点的安全，缺点是对簇以及簇密钥的生成、更新十分低效。

近年来，WSN密钥管理的研究已取得许多进展，根据节点在部署后密钥是否更新，WSN密钥管理可分为静态密钥管理和动态密钥管理2类[4]。在静态密钥管理中，节点在部署前预分配一定数量的密钥，部署后通过协商生成通信密钥，通信密钥在整个网络运行期内不考虑密钥更新和撤回。在动态密钥管理[5-6]中，密钥的分配、协商、更新和撤回操作周期性进行。

本文研究的方案采用文献[3]提出的4种类型密钥，适用于无线传感器网络的密钥管理。

2 基于树型结构的WSN动态密钥管理方案

在层次式WSN中，整个网络被划分成许多簇，普通的簇内成员节点和簇头节点起着完全不同的作用。为了保证通信的安全性，本文采用树型密钥管理和认证机制相结合的密钥管理方案，利用平衡二叉树结构提高了密钥管理效率，并实现了动态密钥更新。

2.1 拓扑结构和密钥管理方案

本方案采用分层式网络拓扑结构，根据各个节点的功能和能量不同将节点分成3类：基站，簇头和普通传感器节点。分层式密钥管理的拓扑结构如图1所示。由图1可知，L_0层为最底层，包含了所有传感器节点，这些节点按照簇生成协议划分为不同簇，如A_1、A_2、A_3、A_4这4个节点为一簇。每个簇都有一个簇头，选取簇内具有较强通信能力和存储能力的节点作为簇头节点。本文假设A_1、A_7、A_9分别是所在簇选举出的簇头，它们形成了L_1层，称为簇头层，每一簇均存在一个仅由簇成员节点共享的簇密钥实现簇内通信，同簇内的节点间建立了点对点的安全通信信道。基站可以直接与网络中的任何节点进行点对点通信，如果需要给某个簇发送信息，可以先将信息传给簇头，再由簇头节点用簇密钥加密，群发给簇内节点。

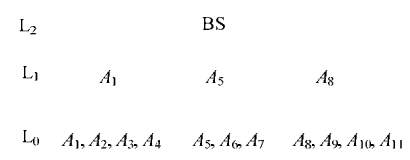

图1 簇密钥管理拓扑结构

2.2 簇头选择

2.2.1 节点的认证机制

在网络部署之前，由可信任的安全中心为每个节点(A_i)

作者简介：于海霞(1979－)，女，硕士研究生，主研方向：信息安全；余梅生，教授；吴晓娟、关 健，硕士研究生

收稿日期：2010-05-21 **E-mail：**yuhaixia0729@126.com

分配一个全局唯一的身份标识号(ID_{A_i})和一个初始密钥(K_s)。在本方案中，假设每个传感器节点都能和周围的邻居节点建立点对密钥(pair-wise key)。如节点 A_1 利用 K_s 和哈希函数 f 产生它的主密钥(K_{A_1})，即 $K_{A_1}=f_{K_s}(ID_{A_1})$，$A_1$ 广播一个消息(ID_{A_1}, $NOUNCE_{A_1}$)，$NOUNCE_{A_1}$ 表示 A_1 到达的邻居节点的跳数，等待其邻居节点识别后回复，A_2 收到广播，并通过消息(ID_{A_2}, $MAC_{K_{A_2}}(ID_{A_2}||NOUNCE_{A_2})$)回应，可表示为：

$A_1 \rightarrow *$: ID_{A_1}, $NOUNCE_{A_1}$

$A_2 \rightarrow A_1$: ID_{A_2}, $MAC_{K_{A_2}}(ID_{A_2}||NOUNCE_{A_2})$

同理，A_2 也可产生主密钥(K_{A_2})$K_{A_2}=f_{K_{A_2}}(ID_{A_2})$，则 A_1 和 A_2 能产生它们之间的点对密钥 K_{A_1}，$A_2=f_{K_{A_2}}(ID_{A_1})$。每个传感器节点可以使用节点 ID 计算邻居节点的密钥，邻居节点之间如果想通信，只需直接将自己的 ID 发送给对方即可。如果有恶意节点想加入网络，则通过唯一的 ID 就可将其识别出来。

2.2.2 簇头节点的选择

在分簇式 WSN 中，相对于普通传感器节点，簇头拥有较高的信息处理和存储能力，它负责将节点分簇、收集并处理来自簇内节点的信息，并将信息发送给基站。因此，簇头节点的选择很重要，本文考虑到节点能量的有限性和整个 WSN 的安全性，提出簇头节点选择算法，具体描述如下：

通过节点自身的评价(如能量等)决定是否成为簇头节点的候选人，一个拥有更高能量的节点更可能被选为簇头节点。如果想成为簇头节点，还需要其他节点的参数来决定：

$$T(n)=\begin{cases}\dfrac{P}{1-P[r \bmod (1/p)]}[\eta+(i\times P)(1-\eta)] & n\in G\\ 0 & \text{otherwise}\end{cases}$$

其中，$T(n)$为选择簇头的函数；P 是簇头在所有节点中所占的百分比；r 是选举轮数；$r \bmod (\frac{1}{P})$ 代表这一轮循环中当选过簇头的节点个数；i 为节点空闲时轮的总和(当选择出簇头时 i 置为 0)；G 是最近 $1/P$ 轮未当选过簇头的节点集合；η 为节点剩余能量的百分比。

在建簇过程中，簇头节点必须能被簇内节点合法识别，如果一个节点不能用点对密钥与它的邻居节点正确通信，它就可能是恶意节点，不可能成为簇头节点。

2.3 簇的形成

在部署网络时，传感器节点被随机投掷在目标区域，随后节点搜寻自己无线范围内的临近簇头自组织形成网络。一旦某一节点成为簇头节点，它将发出广播消息组建簇。此过程包括：簇头广播阶段，簇成员加入阶段，簇稳定阶段。簇建成后，簇头节点向基站发出请求信息要求建立分簇的安全网络，同时动态密钥管理也将建立。

2.3.1 簇头广播阶段

根据簇头产生算法，一个节点被选为簇头(称为 H)，H 广播一个加密的消息给无线范围内的成员节点，即 $H\rightarrow *$: (ID_H, K_H)ID_H 为 H 的唯一节点标识符，K_H 为 H 产生的随机密钥。

2.3.2 簇内加入阶段

非簇头的节点(A_i)收到广播消息后，加入 H 为簇头的簇。

非簇头的节点单播一个加入消息(ID_{A_i}, K_{A_i}, H, TK_{A_i}, H)给簇头节点 H(TK_{A_i}, H 是根据位置产生的一个临时密钥，其初始值为 K_{A_i}, H)，H 收到一个 $MAC(K_{A_i}, H, ID_{A_i})$加密的 A_i 的加入请求消息，则 H 解密此消息，依此 H 可得到在无线范围内的应加入此簇的所有簇成员节点的 ID 和 TK_{A_i}, H。H 产生一个平衡二叉树的密钥池，一旦密钥池产生，H 就回复 A_i 的请求，(ID_{A_i}, $P_{A_i,H}$)，$P_{A_i,H}$ 为 A_i 在密钥池中的位置。簇头与该簇的成员节点协商产生簇密钥，如在此簇中包括 H、A_1、A_2、A_3，它们分别提供子密钥 K_H、K_{A1}、K_{A2}、K_{A3}，H 计算簇密钥 $CK=K_H^{K_{A1}, K_{A2}, K_{A3}}$。

可通过以下算法计算出 $P_{A_i,H}$ 的值：

假设平衡二叉树中有 n 个节点，传感器节点也有 n 个，左子树有 x 个节点，右子树有 y 个节点，则 $n=x+y+1$、$|x-y|\leq 1$，有：

$$P_{A_i,H}=\begin{cases}0\cdots010\cdots, & ID_{A_{i,j}}\text{为树根节点}\\ \quad x \quad y & \\ 0\cdots00\cdots010\cdots0, & ID_{A_{i,j}}\text{为右子树根节点}\\ x+1 \quad x^r \quad y^r & \\ 0\cdots010\cdots010\cdots0, & ID_{A_{i,j}}\text{为右子树根节点}\\ \quad x^1 \quad y^1 \quad y+1 & \end{cases}$$

以此类推，基站和簇头之间也根据上述算法建立平衡二叉树，由此监测区域内可建成由各簇管理的网络拓扑结构。

2.3.3 稳定阶段

在平衡二叉树建好后，无线传感器网络开始进入稳定阶段。

3 密钥更新

静态密钥管理方案不适合长期运行的 WSN，为了保证网络通信的安全性，本文利用平衡二叉树的特性提出动态密钥管理方案。

3.1 基站和簇头检验各节点的向量值

非簇头节点给簇头发单播信息，在簇头认证和融合后，簇头加密消息 $MAC(KP_{BC,Hi}, ID_{h|j})$发给基站($j$ 表示轮次，保证 BS 接收消息的正确性)，则基站和簇头检验各节点的向量值是否发生了变化。

3.2 更新频率

定义 CT 为簇内密钥更新的参数，BT_i 为簇和基站之间密钥更新的参数($i\leq CT$、$BT_i\leq 2^{2k/3}$)，可通过调整 CT、BT_i 的值来控制更新密钥的频率。当且仅当 $CT=BT_i=1$ 时，密钥更新方案为一个实时更新方案。

由于平衡二叉树的特点，一旦某一节点不正常，如没有应答或者应答出错误的密钥向量信息等，都能被簇头节点检测出来，都引起至少是二叉树中的某一子树的改变，簇头会立即广播给整个簇内成员节点并更新密钥和重新生成部分平衡二叉树。因此，尽管节点被俘获，但整个网络还是安全的，且密钥更新只是在一定范围内，不会引起整个网络的更新，极大节省了传感器节点有限的能量。

当 BS 或 CH 收到一定数量的加密消息(接近于参数 CT 或 BT_i)时，密钥就不再安全了，BS 或 CH 会通知每个子节点(簇头和非簇头)及时更新密钥。

4 方案分析

与原有方案相比，本方案的突出特点是动态密钥管理。

4.1 方案的应用分析

通过节点认证机制证明发送信息者是合法的，可以进行下一步的安全通信。

应用本文方案时，每个簇内传感器节点间可建立一个可达的邻居节点集，且该节点只接收本集合中节点发来的请求信息包 REQ，而忽略伪造(敌对)节点发来的请求包，可以在很大程度上抵御攻击。每个节点转发的请求包 REQ 都使用密钥进行加密，新的加密密钥在通信时协商建立。此时，发送请求信息包 REQ 节点的可达邻居节点由于都与发送节点共

享相同的密钥，因此，均可以对接收的 REQ 消息进行解密并认证。攻击者不知道相应的密钥而无法发起攻击，即使攻击者获悉节点间的共享密钥可以发起 Rushing 攻击(见图 2)，此时，接收节点会认为接收的请求信息包 REQ 是由入侵节点发出的，因此导致节点把入侵节点当成合法节点并进行应答。针对上述情况，可以采用计算的新密钥结合节点间的应答机制来保护传感器节点免受 Rushing 攻击(见图 3)。

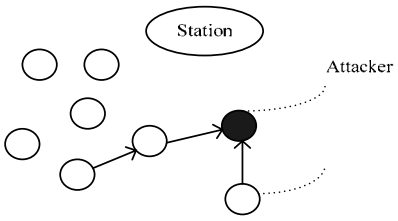

图 2　发起 Rushing 攻击

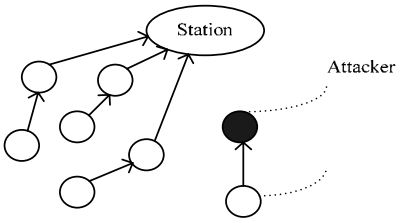

图 3　抵御 Rushing 攻击

4.2　方案的能耗分析

对一个簇内的节点与 m 个邻居节点间建立密钥的能耗与 LEAP 协议进行比较分析。分析中假设一次加密运算所产生的能耗为 e_E，发送一条消息的能耗为 e_S，接收一条消息的能耗为 e_R。

在本方案中，节点广播 1 条消息，接收 m 个邻居节点的广播消息各 1 条，由此产生通信能耗为 $1e_S+m\times e_R$。此过程中的计算包括计算广播消息中的散列值域 1 次，计算用于生成密钥的参数(Y_{M1})1 次，验证 m 个邻居节点广播消息中的散列值域各 1 次，以及计算 m 个邻居节点的点对密钥各 1 次，由此产生的计算能耗为$(2+2m)\times e_E$。同理，在 LEAP 协议中，节点广播 1 条 HELLO 消息，分别给 m 个邻居节点发送回复消息 1 条，接收 m 个邻居节点的 HELLO 消息各 1 条和 m 个邻居节点的回复消息各 1 条，由此产生通信能耗$(1+m)\times e_S+2m\times e_R$。此过程中的计算包括生成随机数 1 次来实现主密钥的生成，生成 HELLO 消息中的随机数 1 次，计算 m 个邻居节点的主密钥各 1 次，验证 m 个邻居节点回复消息中的 MAC 码各 1 次来检验邻居节点的合法性，生成给 m 个邻居节点的回复消息中的 MAC 码各 1 次，以及生成随机数来实现与 m 个邻居节点的密钥各 1 次，由此产生的计算能耗为$(2+4m)\times e_E$。

图 4、图 5 是对 LEAP 和本方案中一个节点与 m 个节点之间建立点对密钥的能耗进行模拟分析后的结果，包括计算能耗和通信能耗。实验结果表明，本方案在建立点对密钥时，节点所消耗的计算能耗和通信能耗都比 LEAP 协议小。

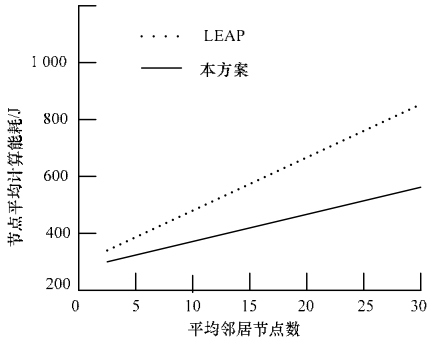

图 4　节点平均计算能耗

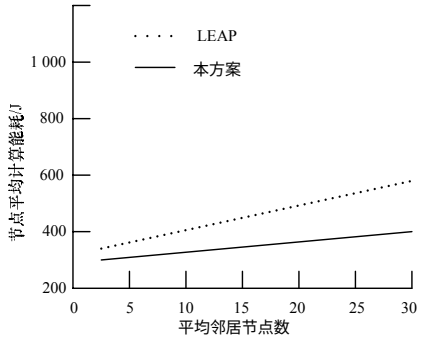

图 5　节点平均通信能耗

5　结束语

本文方案建立多种类型的通信密钥，满足单播、组播或广播通信等需求。该方案利用动态树减少节点能量的消耗，使网络具有更长的生命周期。

参考文献

[1] 李志军, 秦志光, 王佳昊. 无线传感器网络密钥分配协议研究[J]. 计算机科学, 2006, 32(2): 87-91.

[2] 杨　庚, 王江涛, 程宏兵, 等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报, 2007, 35(1): 180-184.

[3] Zhu Sencun, Setia S, Jajodia S. LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks[C]//Proc. of the 10th ACM Conf. on Computer and Communications Security. New York, USA: ACM Press, 2003: 62-72.

[4] Moharrum M A, Eltoweissy M. A Study of Static Versus Dynamic Keying Schemes in Sensor Networks[C]//Proc. of the 2nd ACM Int'l Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks. New York, USA: ACM Press, 2005: 122-129.

[5] Younis M, Ghumman K, Eltoweissy M. Location-aware Combinatorial Key Management Scheme for Clustered Sensor Networks[J]. IEEE Trans. on Parallel and Distribution System, 2006, 17(8): 865-882.

[6] Eltoweissy M, Moharrum M, Mukkamala R. Dynamic Key Management in Sensor Networks[J]. IEEE Communications Magazine, 2006, 44(4): 122-130.

编辑　陈　文