第 34 卷 第 5 期 计 算 机 工 程 2008 年 3 月
Vol.34 No.5 Computer Engineering March 2008
·安全技术· 文章编号：1000—3428(2008)05—0153—02 文献标识码：A 中图分类号：TP393

传感器网络中基于簇的组密钥管理方案

赵治平[1]，林亚平[1,2]
（1. 湖南大学计算机与通信学院，长沙 410082；2. 湖南大学软件学院，长沙 410082）

摘 要：针对传感器网络中无长期可信节点的特点，基于传感器网络的簇结构和门限密钥共享机制提出一种新的组密钥管理方案，使得只有组中的合法节点才能存储一个有效的组密钥分量。组密钥更新时，组密钥由节点协同产生并由簇头安全分发。理论分析和仿真实验表明，该方案具有良好的安全性，在组密钥更新时存储开销和通信开销较低。

关键词：传感器网络；簇结构；门限密钥共享机制；组密钥管理

Cluster-based Group Key Management Scheme for Sensor Networks

ZHAO Zhi-ping[1], LIN Ya-ping[1,2]
(1. College of Computer and Communication, Hunan University, Changsha 410082; 2. College of Software, Hunan University, Changsha 410082)

【Abstract】 There are no trust nodes in sensor networks as that in traditional networks. Based on cluster structure of sensor networks and threshold secret sharing mechanism, a novel group key management scheme for sensor networks is proposed in this paper, in which only innocent nodes have an efficient group key share. When group is rekeying, multiple entities in a local neighborhood can jointly create a new group key to be distributed by cluster heads securely. Analysis and simulations show that the scheme has lower memory and communication overheads besides good security performance.

【Key words】 sensor networks; cluster structure; threshold secret sharing mechanism; group key management

1 概述

无线传感器网络(简称传感器网络)在军事和民用领域具有广泛的应用，如环境和交通监测、灾难救助甚至人体心脏监视，因此，传感器网络是一个非常活跃的研究领域[1]。

许多应用于军事、紧急救灾等场合的传感器网络需要安全组通信的支持。在组通信中，信息机密性和完整性通过组密钥加密实现，而组成员的变化都需要更新组密钥。因此，如何在传感器网络中有效实施安全组通信是一个十分有意义的研究课题[2]。传统有线网络的安全组通信研究已取得了很多进展[3-5]，然而由于传感器网络拓扑结构频繁变化以及自身资源有限等特点，已有的组密钥管理方案很难适用于传感器网络。目前对传感器网络组密钥的研究还很少，文献[6]提出了一种基于邻居协商的组密钥更新方案，但其存在安全性不高、通信和存储开销较大以及存在孤立节点的问题。

本文提出了一种基于簇的组密钥管理方案，其基本思想是：基于传感器网络中无长期可信节点的特点，将组密钥分布式存储在传感器网络的各个合法组节点中。当出现妥协节点等异常情况需要进行组密钥更新时，更新操作以簇为单位进行。同时，为了防止妥协节点的合谋攻击，在组密钥更新阶段对合法节点存储的组密钥分量进行更新操作。新方案在保证安全性的同时具有较小的存储和通信开销。

2 网络模型及相关假设

本文的传感器网络模型及相关假设如下：

(1)传感器节点以组为单位投放在物理监测区域，每组根据成簇算法划分为多个簇[7]，簇头与簇内节点通过层次密钥[8]实现安全单播通信。

(2)妥协节点能被及时检测出来，攻击者捕获新节点需要一定时间，期间合法节点足以进行组密钥更新操作。

(3)基站具有充足的能量以及较强的存储和通信能力。

3 基于簇的组密钥管理方案

假设传感器网络中每组包含N个节点，每个节点都有唯一的全局标识V_i, i=1, 2,…,N。

3.1 具体方案

3.1.1 初始化阶段

在网络部署前，由初始化服务器为每个节点预置：(1)节点的ID；(2)节点部署后用于通信的初始组密钥K_0；(3)节点的初始组密钥分量(group key share)GKS_0；(4)节点的初始组密钥分量根据门限密钥共享机制生成，生成过程为：在节点部署前，由初始化服务器随机选择一个t阶的初始组密钥多项式$g_0(x)$。每个节点的初始组密钥分量$GKS_0 = g_0(i)$。

3.1.2 组密钥的更新

假设传感器节点投出后进行的首次组密钥更新为第 1 次更新，第j-1 轮与第j轮更新完成的时间间隔称为第j阶段，第j阶段的组密钥称为K_j。j阶段的组密钥的更新操作Group_rekeying()描述如下：

Step1 当节点检测到其邻居节点被妥协时，将妥协节点的 ID 传给其簇头，簇头联合几个邻居簇的簇头对该信息进行核实，如属实则删除其与该妥协节点的安全链路。

Step2 该簇头向组内其他簇头发送组密钥更新消息，然后随机向其簇内 t 个节点发送组密钥分量请求消息。

Step3 组内其他簇头收到组密钥更新消息后，随机向其

基金项目：湖南省自然科学基金资助项目(03JJY3089)
作者简介：赵治平(1981－)，男，硕士研究生，主研方向：传感器网络；林亚平，教授、博士生导师
收稿日期：2007-05-14 **E-mail：**fenger1008@163.com

簇内 t 个节点发送组密钥分量请求消息。

Step4 簇内节点收到组密钥分量请求消息后，返回j阶段的组密钥分量GKS_j。

Step5 如果簇头没有获得 t 个簇内节点的组密钥分量，则继续向簇内其他未发送过组密钥分量请求消息的节点发送请求消息，直至簇头获得至少 t 个节点的组密钥分量。

Step6 当簇头获得至少t个簇内节点的组密钥分量后，加上其自身的组密钥分量，t+1 个组密钥分量根据拉各朗日插值原理生成该阶段的组密钥多项式$g_j(x)$，簇头由此计算出 j 阶段的组密钥 $K_j = g_j(0)$。

Step7 簇头用簇内节点的层次密钥加密组密钥，单播给簇内合法节点。

Step8 簇内合法节点通过其层次密钥解密获得新的组密钥K_j。

通过 Group_rekeying()，只有组中的合法节点才能获得新的组密钥。

3.1.3 组密钥分量的更新

根据 2.1.2 节，如果不对组成员的组密钥分量进行更新，那么，每个阶段生成的组密钥多项式$g_j(x)$都是相同的。攻击者只须在不同阶段妥协组中任意t+1 个以上的节点，就可以通过拉格朗日插值原理获得该组密钥，安全性不高。为了防止上述妥协节点的合谋攻击问题，需要对组成员的组密钥分量进行更新。GKS_update()的具体方案如下：

Step1 组密钥更新完成后，由基站随机选择一个t阶更新多项式$f_j(x)$，并用K_j加密构成更新广播。

Step2 对于组中的任意合法节点V_i，当收到更新广播后利用现有的组密钥K_j解密更新广播包，组密钥分量更新为：$GKS_{j+1} = GKS_j + f_j(i)$。更新完成后删除广播包。

通过 GKS_update()，只有组中的合法节点才能拥有有效的组密钥分量用于下次组密钥的更新。

3.2 安全性分析

节点被妥协后，攻击者可获得其存储的组密钥分量。但由于每个阶段的组密钥多项式$g_j(x)$都是t阶多项式，每个节点中仅存储了其分量$g_j(i)$，并且在每次组密钥更新时，都会对组中合法节点的组密钥分量进行更新，因此，即使敌方在不同阶段捕获了超过t+1 个节点，这些节点的组密钥分量也不能生成正确的组密钥多项式。因此，敌方必须在同一阶段捕获至少t+1 个节点才能获得正确的组密钥多项式，由此获得该阶段的组密钥。

上述分析表明，除非攻击者在同一个阶段至少妥协 t+1 个节点，否则本文的方案就是安全的。

3.3 算法开销

(1)存储开销

本方案中每个节点需要保存的信息包括节点的ID、节点的组密钥分量信息GKS_j和节点的组密钥K_j。假设所有的信息长度均为L位，则每个节点的存储开销为 $3L$。

(2)通信开销

本方案的通信开销主要包括局部通信开销和广播开销。局部通信开销主要为组密钥生成与分发时的开销，大小为 $2tn_hL+(N-n_h)L$，其中，n_h 代表组中的簇头数目。n_h 一般远小于 N，因此上式简化为 $2tn_hL+NL$。广播开销主要为组密钥分量更新时的广播开销。令 n_B 代表基站发出更新广播信息后组中所有合法节点均收到该广播消息包所必须转发的次数，则广播通信开销为 $(t+1)n_BL$。因此，本方案总的通信开销为 $(2tn_h+N+(t+1)n_B)L$。

4 相关工作的比较和仿真实验

4.1 相关工作的比较

为了进一步说明本方案的有效性，表 1 将本文方案和文献[6]的 B-PCGR 方案作了比较。在 B-PCGR 方案中，组密钥更新时，每个合法节点需要与其邻居节点进行协作，总通信开销为 n_1NL，其中，n_1 为更新时所需的邻居数。每个节点需要存储一个 t 阶多项式及其邻居节点的加密多项式分量，节点的存储开销为 $(n_1+1)(t+1)L$。表 1 表明，本文方案在存储开销、安全性及孤立节点方面优于 B-PCGR。本方案的通信开销与更新广播转发的次数 n_B 相关。

表 1 本文方案和B-PCGR[6]方案的比较

比较指标	B-PCGR	本文方案
节点的存储开销	$(n_1+1)(t+1)L$	$3L$
组密钥更新时的通信开销	n_1NL	$(2tn_h+N+(t+1)n_B)L$
安全性	妥协一定数量的节点，网络将被攻破	只要攻击者不能在同一阶段妥协至少 t+1 个节点，本方案就是安全的
孤立节点	当某节点的多个邻居被妥协时，成为孤立节点	以簇头为中心实现组密钥的更新，不存在孤立节点问题

4.2 仿真实验

本文的仿真实验如下：传感器节点均匀分布在一个 400×400 m^{2}的正方形区域内，每个节点的通信半径 c_r =40 m。取 $t=n_1=n/3$，其中，n为节点的平均邻居数；组中的簇头数 n_h =0.05N[7]。本方案按照ZBP广播算法[9]进行实验，取多次实验的平均值作为单次广播所需的转发次数 n_B。图 1 显示了N为 1 000~3 000 时本方案与B-PCGR方案通信开销的比较。

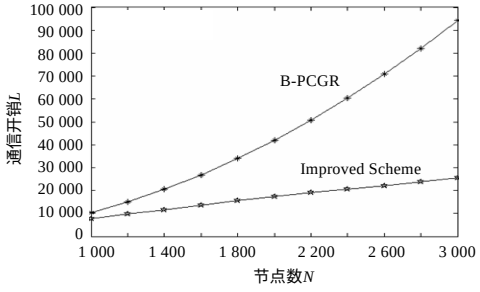

图 1 本文方案与B-PCGR[6]方案通信开销的比较

图 1 表明，本文方案的通信开销小于 B-PCGR。这是因为节点的邻居数随着节点数的增加而增加，使 B-PCGR 的通信开销迅速增大，而本方案采用 ZBP 算法，在固定区域内广播信息转发的次数随节点数的增加先稍有增大然后逐步减小，总的通信开销随节点数的增加逐步增大。

5 结束语

本文提出了一种适应传感器网络特点的组密钥管理方案，在组密钥更新过程中以簇为单位实现组密钥的生成与分发。同时，引入合法节点的组密钥分量更新机制避免妥协节点的合谋攻击。和文献[6]的 B-PCGR 方案相比，在保证安全性的同时，本文的方案在存储开销和通信开销上均有较大的改善。理论分析和仿真实验表明本方案是传感器网络中一种有效的组密钥管理方案。但本方案存在的问题有：更新广播包的丢失会导致合法节点组密钥分量更新失效以及随着网络规模的增大组密钥更新时延会增大。如何更好地解决上述问题是下一阶段研究的课题。 （下转第 157 页）