数据储存式无线传感器网络下一个具有高效能的密钥管理方案

潘中强 常新峰
(平顶山学院网络计算中心 平顶山 467000)

摘 要 针对无线传感器网络能量、存储空间、通信开销等局限性问题,基于 pDCS(Security and Privacy Support for Data-Centric Sensor Networks),在保证不失其安全性的前提下,以互斥基底系统(Exclusion Basis System,EBS)建构一个具有更高效率的分布式密钥管理方案,将其命名为 ERP-DCS。该方案将网络密钥的管理工作(包括密钥分配、重置及撤销)分散至各个簇集中,藉以降低密钥重置阶段所需的通信量,节省能源,进而延长网络寿命。论证分析表明,与 pDCS 相比,ERP-DCS 仅增加了些微的储存成本,却能大幅地降低密钥重置时的更新通信量。

关键词 密钥管理,数据储存式无线传感器网络,信息安全,互斥基底系统,分散式系统架构
中图法分类号 TP393 **文献标识码** A

Efficient Key Management Scheme for Data-centric Storage Wireless Sensor Networks

PAN Zhong-qiang CHANG Xin-feng
(Network and Computation Center, Pingdingshan University, Pingdingshan 467000, China)

Abstract Based on the Exclusion Basis Systems(EBS), we proposed an efficient distributed key management scheme, termed as ERP-DCS, to improve the deficiencies identified in the *p*DCS scheme. ERP-DCS attempts to distribute the key *management tasks, including key distribution, rekeying, and key revocation, to each cluster(i. e. grid cell) to reduce the* number of rekeying messages. The results show that, comparing to the *p*DCS scheme, the ERP-DCS is superior, in terms of update messages needed in the rekeying process, at a little cost in key storage.

Keywords Key management, Data-centric storage sensor network, Information security, Exclusion basis system, Distributed system architecture

无线传感器网络(Wireless Sensor Network,WSN)是由一群资源有限(如内存、计算能力、能源等)、体积小、成本低廉、具感测与无线传输功能的传感器节点(Sensor node)所建构而成的网络[1]。传统上,传感器节点在与基站(Base Station,BS)进行通信时常引发两个问题:1)数据在节点与基站传送过程中,将迅速消耗传感器节点的能源,间接影响网络的存活时间。2)数据的流向过于向基站集中,容易产生热点现象,导致路径上节点无法及时接收新的信息,进而发生封包遗失,影响数据搜集的质量。

数据储存式(Data-Centric Storage,DCS)无线传感器网络架构应运而生[2,3]。在 DCS 的无线传感器网络架构下,传感器节点根据其所侦测到的事件属性(如事件种类、地理位置等),通过定位函数计算出所处网络中的储存位置后,将事件数据送往该位置上或其附近的节点进行储存[2]。之后,基站或管理者再针对感兴趣的事件,通过相同的规则计算出感兴趣的数据储存位置后,直接送出请求封包来取回数据。

在数据传递的过程中,传感器节点由于先天上的硬件限制,难以保证节点遭到掳获攻击时不会泄漏出恶意入侵者感兴趣的数据。再者,由于无线通信的开放性,通信内容极容易遭到拦截、监听、窜改、仿冒及复制[4-6]。因此,对数据的加、解密成了必要之手段。一般,常见的数据加解密方案大致可分为非对称式密钥(Asymmetric Key Schemes)及对称式密钥(Symmetric Key Schemes)两大类[7]。非对称式密钥中,最具代表性的为公钥方案(Public Key Scheme),其特征是加密与解密时使用不同的密钥。对称式密钥方案最大的特征是加密与解密时皆使用同一把密钥。

欲将对称式密钥方案应用于无线传感器网络上,首先需考虑传感器节点内密钥的分配问题(Key Distribution)。与传统网络不同的是,传感器节点并非一开始就散布在环境中,用户可在节点布置前将一些安全信息(如密钥)预先置入传感器节点内。当传感器节点配置到环境后,就可通过这些安全信息建立起所需的密钥系统。当然,要维护网络的安全性,还必须谨慎地管控密钥系统。

网络的存活时间(Lifetime)一直是无线传感器网络研究领域上常被关注的议题之一。包含数据感测、通信传输、计算、储存装置等都需要消耗能源,其中尤以通信传输所耗费的能源最甚。因此,在安全的相关研究上,已有不少学者关注密钥管理方案所带来的各项成本(如通信开销、储存成本)支出。另外,为了维护网络的整体安全,管理者必须在适当的时机对网络内的节点进行密钥管控,相关的更新通信也需要耗费节

本文受河南省科技厅:无线传感器网络密钥管理方案研究(12B520043)资助。
潘中强(1978—),男,硕士,副教授,主要研究方向为网络通信技术;常新峰(1982—),男,硕士,助教,主要研究方向为无线传感器网络,E-mail:xin83@126.com(通信作者)。

点的能源。因此，拥有一个具有能源效益的密钥管理方案，在无线传感器网络相关的安全议题上是非常重要的。

对于数据储存式无线传感器网络架构(DCSN)，现研究者多半仅着重于如何储存及取回数据，却忽略了数据储存过程中的安全风险性[11,12]。S. Min 最早提出 pDCS[8] 的安全方案，其是将网络中节点依照其地域位置分成 5 种不同的群组，并赋予不同的密钥，用来进行群组内节点间的安全通信。pDCS 除了利用一个简单的加密方案来隐匿数据储存的位置，防止攻击者得知数据所在的位置外，还提出了密钥重置(Rekey)的具体做法，能够使网络在遭受到攻击后，迅速恢复正常的运作。pDCS 虽有着上述的优点，但在密钥重置时需要大量的信息交换，这严重影响了网络能源耗损，间接缩短了网络存活时间。本文希望通过建构一个分布式的密钥管理方案来解决上述缺点，并不失 pDCS 原有的优点。

本文思想是在 pDCS 的基础之上，以互斥基底系统(EBS)为每个簇集(网格)建立起局部的密钥管理中心，将网络遭受到攻击时的损害范围局限在一小部分的区域内，以此来降低密钥重置时所需的信息交换量，达到节省能源、延长网络寿命的目的。

1 模型与基础

1.1 pDCS

pDCS 首先将整个网络环境切割成数个矩形网格细胞(Cell)(或称之为簇)。每个传感器节点依其功能需要配置 5 种密钥：主密钥(Master key)、配对密钥(Pairwise key)、网格密钥(Cell key)、列密钥(Row key)、全局密钥(Group key)。

其流程简单归纳如下：

步骤 1　决定事件的储存位置：当一事件在网格被侦测后，感测节点会依据事件的某些属性，以一个不可逆的哈希函式计算出该事件信息在网络上的储存位置，并将事件信息用发生地的网格密钥加密，准备传送。此份密文在被(基站)管理者取回之前，不会进行解密。

步骤 2　数据传送：加密后的信息经由 GPSR 协议逐步送抵目的地储存。过程中点对点之间各自使用彼此的配对密钥来进行安全通信。

步骤 3　数据取回：当(基站)管理者想要取回所需信息时，配合前述储存信息的相关属性，计算出其储存网格位置，并对该网格发送请求。待密文送返(基站)管理者后，再以事件发生地的网格密钥解密取得原始信息。

1.2 互斥基底系统

互斥基底系统(Exclusion Basis System，EBS)[9,10]是一种集合元素分配的概念，却可作为一种极佳的密钥重置机制。其基本观念如下：令 n,k,m 为正整数，其中 $1<k,m<n$。$EBS(n,k,m)$代表由多个整数子集所构成的母集合；子集的样本空间为$[1\cdots n]$，t 为整数，$t\in[1\cdots n]$，且满足以下两个特性：

(1)t 最多存在于 k 个子集内。

(2)恰好有 m 个子集 $A_1,A_2,A_3,\cdots,A_m$，当 $U_i^m A_i$ 时，其联集将独缺 t。

$EBS(n,k,m)$若应用到无线传感器网络环境下可解释为：设有 n 个传感器节点、$k+m$ 把密钥的情况下，若每个传感器节点储存 k 把密钥，则密钥分配中心(Key Distribution Center，KDC)最少仅需送出 m 个信息，即可解决某个被掳获节点的密钥重置问题。

2 分布式密钥管理方案(ERP-DCS)

为便于描述，需要对网络环境做以下假设。

2.1 预设网络环境

(1)同构型的无线传感器网络：基于分布式的对等特性，除簇头节点外，假设网络内所有的节点均拥有相同的资源和处理能力。

(2)网格式的簇结构：比照 pDCS 作法，将整个环境切割成若干行、列的网格，使每一个网格自成一个簇(Cluster)。

(3)节点位置已知(Location-aware)：为简化方案的运作说明，本文进一步假设每个节点位置均已通过定位设备计算出其所属的网格，并回传给基站。

(4)网格簇内存在簇头节点(Cluster Head，CH)的选择算法：本文同时假设簇内节点存在一个簇头的选择算法。

(5)完善的入侵检测方案：由于本文主要探讨密钥管理的效益，因此对如何侦测入侵行为并不深入。这里假设环境中已存在一套完善的入侵检测系统，并可快速正确地指出任何已遭捕获的节点。

(6)安全的密钥设定阶段：为了让方案得以运作，本文进一步假设节点散布后至整个密钥管理系统建置完成前的一小段时间，入侵者无法捕获任何节点或得知任何安全信息。

2.2 方案实施步骤

本文所提密钥管理方案类似于 pDCS，首先将网络环境切割成 $N_r\times N_c$ 的网格。不同于 pDCS，本文在每一网格簇中选定一个节点来担任该网格的簇头，或称该网格的密钥分配中心，用来负责网格内节点密钥的管理工作。换言之，本方案中仍保留了 pDCS 节点中的主钥、配对密钥与网格密钥，但撤销了全局密钥和列密钥，取而代之的是由各个簇头构建出自己网格的 EBS 密钥矩阵，并分配对应密钥至网格内节点。此法虽对每个节点所必须储存的密钥数量可能会有所增加，但在密钥更新阶段可以节省通信开销。方案中的符号含义如表 1 所列。

表 1　符号对应表

S_i	编号(id)为 i 的节点
$Cell_{a,b}$	第 a 列第 b 行的网格
$Mem_{a,b}$	$Cell_{a,b}$ 中成员节点的集合
$Ch_{a,b}$	$Cell_{a,b}$ 中的簇头
BS	基站
K_{INI}	初始密钥(initial key)
K_i	传感器节点 s_i 的主密钥(master_key)
$K_{a,b}$	第 a 列第 b 行网格的网格密钥(cell_key)
N_r	切割的网格之列(row)的总数
N_c	切割的网格之行(column)的总数
$K_{sp}^{(a,b)}$	$Cell_{a,b}$ 的 EBS 密钥矩阵中，第 p 把密钥
k	每一个节点所持有的 EBS 密钥子集大小
m	EBS 系统下，密钥更新时所需的通信数量

2.2.1 密钥预分配阶段

此阶段的时间为传感器节点布署到目标区域前。此时 BS 先将一些必要的安全信息储存至各个传感器节点内，为稍后密钥设定阶段做准备。此阶段通信包括：

(1)一把与 BS 共享的私有主密钥 K_i，用以加密节点 S_i 和 BS 之间的通讯数据，BS 也可用此密钥认证节点 S_i。

(2)一把不同于 K_i 的初始密钥 K_{INI}。所有的传感器节点

都分配到相同的 K_{INI}，在密钥设定阶段用以产生其他密钥。

(3)一个不可逆的单向哈希函式(One-way Hash Function)，用以计算新的密钥和推算感测信息的储存位置。

2.2.2 密钥设定阶段

此阶段的时间点在传感器节点布署至目标感测区域后的一小段时间内，目的是建立往后通信协议中所需的密钥。本文假设在设定阶段完成前，传感器节点皆不会被恶意者捕获或入侵。此阶段有以下 4 个目标：

(1)配对密钥设定：节点可以透过一个被信任的第三方(如 BS)，或是由一些预先分配式的机率性密钥分配法，来取得和邻近节点进行安全通信的配对密钥。

(2)网格密钥设定：节点可由 GPS 得知自己所在的坐标位置，及所属网格编号(a,b)，并以 $K_{a,b}=H(K_{INI},a|b)$计算出该网格的网格密钥。

(3)每一个网格(即簇)挑选出其内的簇头，根据簇成员数量，建构出最适当(具有最佳的 k 与 m 值)的 EBS 密钥矩阵，并将每个成员所分配的 k 把 EBS 密钥以配对密钥加密后分别传送给各个成员节点。

(4)当所有密钥被设定完成后，节点撤销其内的初始密钥。网格簇头将该网格密钥分配的信息(包含 EBS 密钥矩阵及成员节点所持有的 EBS 密钥代码)回传给基站。

2.2.3 系统运行阶段

ERP-DCS 密钥管理方案在正常运作下，配合 DCS 架构，与 pDCS 并无太大差异。其流程如下：

(1)当一个事件种类 E，在时间区段 T，发生于网格(a,b)的事件被侦知时，储存数据的网格位置 $V(x,y)$也将被计算出来。即

$$V_x=H(0|a|b|E|K_{a,b}|T) \bmod (N_r)$$

$$V_y=H(1|a|b|E|K_{a,b}|T) \bmod (N_c)$$

为了防止攻击者在捕获节点后推知先前的信息被送往何处，系统在经过一段时间后，所有的节点都会自我更新网格密钥(cell_key)，即 $K_{a,b}=H(K_{a,b})$。由于 $H(x)$是一个不可逆推的哈希函式，攻击者将很难回溯之前的储存位置。

(2)节点以自己的网格密钥加密数据后产生一份密文件(Me)。

(3)节点将信息转传至储存网格(Storage Cell)中。转传方式可采用点对点的路由协议，例如 GPSR。此阶段的通信数据经由两节点间的配对密钥加密传送。

(4)数据抵达储存网格后，直接将密文件(Me)储存于结点上，且不做任何解密的动作。

(5)合法的使用者想要取回某特定事件信息(如事件属性为 E、T、(a,b))时，则可利用相同的定位规则计算出数据储存的位置，再对网格 $V(x,y)$送出请求封包。

(6)待被加密的文件送返使用者手上后，使用者再以正确的网格密钥解密取得的原文。

2.2.4 密钥重置阶段

在系统运行中，若假设攻击者随机掳获节点，并破解其中信息，此时管理者就必须启动密钥重置措施，以更新网络中其它节点的密钥，来防止网络的持续毁灭。密钥重置手段，依被掳获节点的类型可分为两类，一为针对普通节点，二为针对簇头节点。

(1)由于普通节点所持有的密钥类型有：主密钥、配对密钥、网格密钥与 EBS 密钥组。当某一节点遭受掳获时，相关密钥均需作废或更新，并撤销此节点。此时该网格的簇头即可利用 EBS 机制的特性，以 M 个该掳获节点未拥有的 EBS 密钥加密更新通信(内含将被撤销的节点 ID、新的 EBS 密钥矩阵与网格密钥等)，并广播通知给其余节点进行变更。

(2)簇头扮演着网格内的密钥管理中心角色，一旦被掳获，所泄漏的密钥信息不止主密钥、网格密钥与配对密钥，甚至该网格的 EBS 矩阵也会一并泄漏。此时必须依赖基站来协助密钥重建的工作。步骤如下：

步骤 1 基站须给重建的网格内成员(扣除被捕获的节点)分别发送一份数据包，如下：

$$E_{K_i}(ID_{revoked}|K_{a,b}^{new}|"re\text{-}elect")$$

$ID_{revoked}$表示要被撤销的节点 ID，$K_{a,b}^{new}$表示新的网格密钥，"*re-elect*"则是一段关键词代表接下来网格内的簇头将进行重新选择的动作。这段信息由每一个节点的主密钥加密。

步骤 2 节点在收到基站发出的重建数据包后，以自己的主密钥解密，进而撤销被掳获节点的配对密钥，置换新的网格密钥。由于被掳获的节点无法正确地解开这段通信，因此无法得知新的网格密钥。

步骤 3 每一个成功完成网格密钥更新的节点使用新的网格密钥发出竞选消息，重新竞选出新的簇头。

步骤 4 待新的簇头产生后，立刻建构新的 EBS 密钥矩阵，再分配新的 EBS 密钥给各成员节点，如此完成工作。

3 方案分析

从安全性、成本消耗等方面对 ERP-DCS 与 pDCS 进行分析，并通过仿真给予证实。

3.1 安全性分析

在 ERP-DCS 与 pDCS 中，均假设传感器节点被布置于网络环境中，并成功地建立起密钥管理方案。此外，两方法中皆已假设感测环境中存在一套完善的入侵检测系统。以下做详细说明：

(1)感测信息的隐密性：在两方案中，感测信息均通过侦测到事件的节点的网格密钥进行密文生成，并通过单向不可逆的哈希函式 H 计算出储存网格位置，然后储存到该位置的节点上。每经过一定的时间，网络内所有的节点都会进行网格密钥的更新，即 $K_a^b=H(K_a^b)$。假设攻击者随机捕获节点，并取得节点内的密钥信息和加密过的感测信息。由于攻击者无法推算出过去所使用的网络密钥，他将无法计算出过去的感测信息储存位置，此法可确保感测信息的隐匿性。另一方面，攻击者若想要解开已加密过的感测信息，则必须得知事件发生的网格位置，并且取得该网格的网格密钥。由于网格密钥在自动更新的过程中采用单向不可逆的哈希函式，即使攻击者取得了目前的网格密钥，也无法用它来解开过去的感测信息。因此，ERP-DCS 同样可以达到 pDCS 所提供的资料保密性。

(2)密钥重置：基于群组式密钥方案的特性，在 pDCS 中，系统发现有密钥泄漏的情况时，就会启动密钥重置的方案来撤销或替换掉已泄漏的密钥。系统针对感测环境中的节点，必能找出至少一把妥当的密钥来加密更新数据包，以进行节点的密钥重置。已遭受攻击的节点由于无法解开更新封包，从而被排除在系统之外。而 ERP-DCS 则是整合了群组式密

钥方案与分布式系统的概念，在每一个网格中建立一个以互斥基底系统为基底的密钥管理中心（称为簇头）来负责网格（即簇）成员节点的密钥分配与重置。当簇头发现有成员节点遭到捕获时，它便可以利用被捕获的节点所没有的一至数把EBS密钥对其他成员节点广播更新数据包，进行密钥重置，簇头会将撤销的节点信息发送至周围的网格，以便撤销泄漏的配对密钥。由以上可知，两方法所提的密钥重置措施均可行，但两者在密钥储存成本以及密钥重置阶段所耗费的通信开销上是有差异的。

3.2 成本分析

由于传感器节点受硬件及能源上的限制，成本开销是研究者关注的一个重点，对于成本问题，主要有储存和能耗两个方面。储存成本即建立密钥管理系统使用的储存空间。对于能耗，本文主要关注在密钥重置阶段系统所必须发送的更新数据包数量。

3.2.1 储存成本分析

在ERP-DCS与*p*DCS中，为了建立密钥管理系统，每个节点必须储存数种不同的密钥，以确保通信的安全性或进行密钥重置之用。在*p*DCS中每个节点均储存相同的5种类型密钥，而在ERP-DCS中，节点被区分为一般节点和簇头节点，其储存的密钥种类如表2所列。

表2 ERP-DCS与pDCS储存成本分析

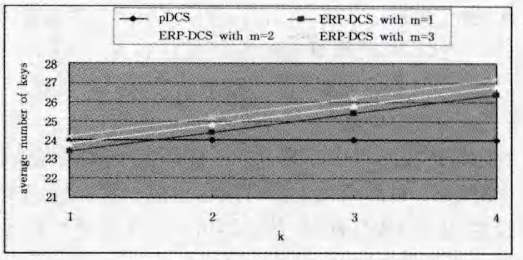
节点类型	ERP-DCS	pDCS
一般节点	2+δ+k	4+δ
簇头节点	2+δ+k+m	N/A

在*p*DCS中，每个节点储存5种密钥，分别为一把主密钥、一把全局密钥、一把列密钥、一把网格密钥与δ把配对密钥，δ代表一个节点的邻近节点数。整理可得，*p*DCS中每个节点必须储存$4+\delta$把密钥。在ERP-DCS中，每个一般节点储存一把主密钥、一把网格密钥、δ把配对密钥与k把EBS密钥，由于簇头节点必须储存EBS矩阵中所有的EBS密钥，因此簇头节点比一般节点多储存m把EBS密钥。归纳得出，ERP-DCS中的一般节点必须储存$2+\delta+k$把密钥，簇头节点则必须储存$2+\delta+k+m$把密钥。由以上可推导出一个传感器节点的平均密钥数量。在*p*DCS中，节点平均密钥数量可表示为$4+\delta$。本文则可表示为

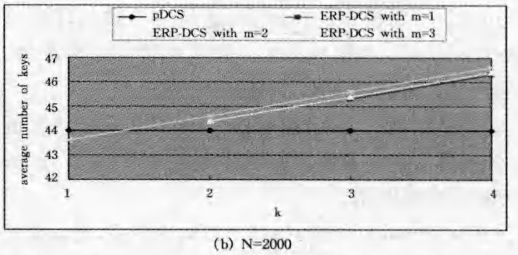
$$[\frac{N-N_{ch}}{N}\times(2+\delta+K)]+[\frac{N_{ch}}{N}\times(2+\delta+K+m)]$$

其中，N代表传感器网络中的节点总数，N_{ch}代表簇头的数量，即本文中的网格总数。

根据上式，将1000及2000个节点，布置于500×500平方米区域，将其划分为20列20行，每个传感器节点的传输半径为40米，来比较ERP-DCS与*p*DCS中每个节点所必须储存的密钥数量。由于ERP-DCS中应用了EBS的特性，因此参数k（即每个一般节点必须储存的EBS密钥量）与m（即密钥更新时所使用的数据量）会限制每个密钥管理中心所能掌控的成员节点数量，即必须符合$\frac{(k+m)!}{k!m!}\geqslant n_{member}$。以图1(b)为例，平均每个网格包含5个节点，其中一个将被选为簇头，因此该簇的EBS设定必须符合$\frac{(k+m)!}{k!m!}\geqslant 4$，而$(k,m)=(1,1)$、$(2,1)$、$(1,2)$则不适用于该簇。由分析结果可知，ERP-DCS与*p*DCS相比，储存成本应该会略微提高。



(a) N=1000



(b) N=2000

图1 不同节点数下ERP-DCS与pDCS储存成本的分析比较

通过仿真实验，本文模拟了1000到4000个节点，预设$m=2$，分别计算在两种方案下，每个节点所需储存的密钥数量，如图2所示。实验结果显示，即使节点的数量有显著的增加，ERP-DCS的储存成本也只有相当小的提高。

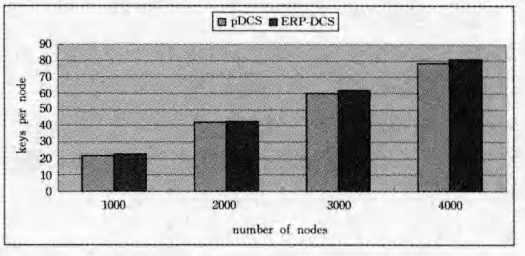


图2 不同节点数下ERP-DCS与*p*DCS储存密钥的数量比较

3.2.2 通信开销成本分析

在无线传感器网络中，节点进行通信传输时，其消耗的能源量与通信的数量及传输距离的平方成正比，若传输距离过大，甚至会与距离的4次方成正比。

在*p*DCS中，由于每个节点都握有一把相同的全局密钥，因此当网络遭受到节点捕获攻击时，系统就必须启动密钥重置方案来对传感器网络中所有的节点进行密钥更新，即便*p*DCS中设有列密钥来简化密钥重置的流程，对整体网络能源耗损的影响仍会很大。ERP-DCS中重新规划了DCS传感器网络，融合了分布式系统及互斥基底系统的概念，并撤销了*p*DCS中的全局密钥与列密钥，以降低密钥重置阶段时所使用的通信量，进而延长网络的生命周期。对两种方案的节点更新通信开销分析如下：

假设有一节点S_c位于网格(x,y)（即第x列第y行），其遭到攻击者捕获。*p*DCS中的BS应进行以下的操作：

(1)对第x列以外的每一列，分别运算出一份更新数据包，总数为N_r-1，N_r代表传感器网络切割中的最大列数。这些数据包将被送达目标列中的其中一个节点，然后再由该节点以泛滥(Flooding)的方式传至该列的每一个节点。

(2)在第x列中，除了网格(x,y)以外的每一个网格，分别运算出一份更新数据包，总数为N_c-1，N_c代表传感器网络切割中的最大行数，其传播方式类似于(1)。

(3)在网格(x,y)中,对S_c以外的节点,分别运算出一份更新数据包,总数为$mem-1$,mem代表一个网格内所有的平均节点数。BS以主密钥进行安全通信,因此本步骤中BS必须对这些节点进行共计$mem-1$次点对点的通信。

由以上步骤可得,pDCS进行一次密钥更新时,BS必须运算并送出的更新数据包量为$N_r+N_c+mem-3$。

在ERP-DCS中,传感器节点分为一般节点与簇头节点,因此密钥重置流程可分为两种情况。

(1)若遭到捕获攻击的节点S_c为一般节点,则网格(x,y)的簇头先随机产生一把新的网格密钥,接着调阅S_c的EBS密钥通信,以S_c所未持有的m把EBS密钥对新的网格密钥加密,共产生m个更新封包,再对网格(x,y)进行m次的广播,簇内的成员节点即可取得新的网格密钥。此外,簇头将对S_c的邻近节点送出更新数据包,以撤销与S_c通讯所使用的配对密钥,这些数据包的数量为α,即S_c通信半径所涵盖的网格数,并由这些网格中第一个收到更新数据包的节点进行广播。此情况下簇头发出的更新包量为$m+\alpha$。

(2)若遭到捕获攻击的节点S_c为簇头,由于网格(x,y)的网格密钥与EBS密钥矩阵内所有的密钥通信都已泄漏,BS必须介入密钥重置流程。BS首先随机运算一把新的网格密钥,并以网格(x,y)内节点的主密钥加密并分别送达各节点,排除S_c后总数为$mem-1$。BS送出α个数据包至网格(x,y)周围的网格。接着收到更新包的$mem-1$个节点,将会取得新的网格密钥,并广播一份加密过的竞选包至网格中的其他节点,共$mem-1$个。待新的簇头产生后,它将重新建立起EBS密钥矩阵。本文假设新的簇头可以用一份广播消息将密钥资料分配至所有的成员节点上。虽然重选簇头的流程中,绝大部分仅涉及网格成员,但因牵涉到整个密钥重置的重要环节,所以在分析中仍将这些数据包量计入其中,更新数据包量为:

$(mem-1)+\alpha+(mem-1)+1$,即$2\times mem+\alpha-1$

在ERP-DCS中,簇头与一般节点被捕获的机率可写作$\frac{N_{ch}}{N}$与$\frac{N-N_{ch}}{N}$,因此平均更新数据包量为:

$$\frac{N_{ch}}{N}\times(2\times mem+\alpha-1)+\frac{N-N_{ch}}{N}\times(mem+\alpha)$$

在pDCS中,平均更新数据包量为$N_r+N_c+mem-3$。若以3.2.1节同样的环境来分析,α参考节点传输能力与网格大小,采用最大可能值20为常数,当节点总数为1000时,ERP-DCS的平均更新数据包量为22.2到23.4,pDCS中为39.5,ERP-DCS仅用了pDCS中58%的通信量;当节点总数为2000时,ERP-DCS为22.6到24.2,pDCS中则为42,仅占pDCS中的56%。

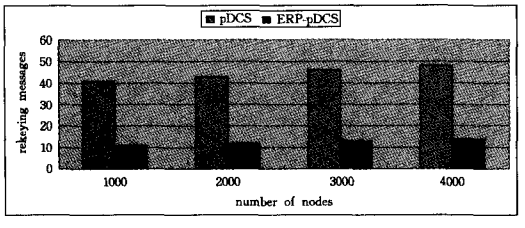


图3 不同节点数下ERP-DCS与pDCS更新通信量的比较

仿真中,将节点数量调整为1000到4000,预设$m=2$,此外,与分析时不同,α是依照仿真环境事实上必须通知的网格数量,换言之,没有S_c邻点座落的网格,密钥更新时将不需要传送数据包。图3的仿真结果显示,ERP-DCS所使用的更新通信量远低于分析时的预测数据,仅占pDCS中的24%~27%。

结束语 本文在pDCS基础上,提出一个在数据储存式无线传感器网络上的密钥管理方案,即ERP-DCS。其原理为在每个网格中建立互斥基底系统(EBS),由遴选出的簇头担任该网格的密钥分配中心,以期能达到簇可自主性地进行密钥重置。由于EBS是一个优良的密钥重置机制,仅需少量的更新通信即可完成对簇成员的密钥重置,能有效降低密钥重置时所耗费的能源成本,进而延长网络生命周期。由仿真看出,ERP-DCS虽然会些微地提高密钥的数量(约3%),但因为有效地缩小了受影响的范围,使得密钥更新阶段所使用的通信量有显著的减少(约75%),对网络生命周期的延长有显著贡献。

参考文献

[1] 黄梅根,常新峰.一种基于蒙特卡罗法的无线传感器网络移动节点定位算法研究[J].传感技术学报,2010,23(5):562-566

[2] Ratnasamy S, Karp B, Yin L, et al. GHT: a Geographic Hash Table for Data-Centric Storage[C]// Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications. 2002:78-87

[3] Ghose A, Grossklags J, Chuang J. Resilient Data-Centric Storage in Wireless Ad-Hoc Sensor Networks Mobile Data Management [C]// Lecture Notes in Computer Science. 2003:45-62

[4] Newsome J, Shi E, Song D, et al. The Sybil Attack in Sensor Networks: Analysis &Defenses[C]// Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks. 2004:259-268

[5] Parno B, Perrig A, Gligor V. Distributed Detection of Node Replication Attacks in Sensor Networks[J]. IEEE Symposium on Security and Privacy. 2005:49-63

[6] Peng T, Leckie C, Ramamohanarao K. Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems [J]. ACM Comput. Surv., 2007, 39(1)

[7] Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6):644-654

[8] Min S, Sencun Z, Wensheng Z, et al. pDCS: Security and Privacy Support for Data-Centric Sensor Networks[J]. IEEE Transactions on Mobile Computing, 2009, 8(8):1023-1038

[9] Eltoweissy M, Heydari M H, Morales L, et al. Combinatorial Optimization of Group Key Management[J]. Journal of Network and Systems Management, 2004, 12(1):33-50

[10] Younis M F, Ghumman K, Eltoweissy M. Location-Aware Combinatorial Key Management Schemefor Clustered Sensor Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2006, 17(8):865-882

[11] Alzaid H, Foo E. A taxonomy of secure data aggregation in wireless sensor networks[J]. International Journal of Communication Networks and Distributed Syetems, 2012, 8(1):101-148

[12] 程芳权,彭智勇.可信云存储环境下支持访问控制的密钥管理[J].计算机研究与发展,2013,50(8):1613-1627