第 68 卷 第 1 期
2022 年 2 月

武汉大学学报(理学版)
J. Wuhan Univ. (Nat. Sci. Ed.)

Vol. 68 No. 1
Feb. 2022, 83~92

DOI: 10.14188/j.1671-8836.2021.2006

环形区域无线传感器网络的密钥管理方案

吴万青,张子扬†,董亚华

河北大学 网络空间安全与计算机学院,河北 保定 071000

收稿日期:2021-06-30 † 通信联系人 E-mail:zhangziyang_hbu@163.com
基金项目:河北省高等学校科学技术研究项目(ZD2021011);河北大学创新资助项目(HBU2021ss058)
作者简介:吴万青,男,讲师,现从事信息安全研究。E-mail:wuwanqing8888@126.com

摘　要:密钥管理是无线传感器网络面临的极具挑战性的安全问题之一。无线传感器节点具有有限计算和储存能力,如何在连通性、能量消耗和安全性之间寻找平衡是热点问题。本文提出了一种环形区域无线传感器网络的密钥管理方案。该方案将无线传感器所在区域划分为环形区域,采用分层式网络结构,对环形区域进行再划分,利用数据包格式和传感器节点的广播特性将簇头进行隐藏。在方案的初始化阶段,构造簇间和簇内密钥并实现密钥的更新,分别使用基于二元对称多项式的密钥分配方案和基于中国剩余定理的密钥分配方案实现簇间和簇内密钥通信;在执行阶段,进行簇头更换、节点退出和节点加入等操作。实验结果表明,与现有方案相比,本方案平衡了连通性、能量消耗和安全性之间的矛盾关系,具有更高的安全性和有效性,同时还具有更低的能量消耗。

关　键　词:无线传感器网络;密钥管理;簇头;安全;路由

中图分类号:TP393　　**文献标志码**:A　　**文章编号**:1671-8836(2022)01-0083-10

Key Management Scheme of Wireless Sensor Network in Ring Area

WU Wanqing, ZHANG Ziyang†, DONG Yahua

School of Cyberspace Security and Computer, Hebei University, Baoding 071000, Hebei, China

Abstract: Key management is one of the most challenging security issues faced by wireless sensor networks. Wireless sensor nodes have limited computing and storage capabilities. How to find a balance between connectivity, energy consumption and security is a hot issue. This paper proposes a key management scheme for wireless sensor networks in a ring area. The scheme divides the area where the wireless sensor is located into a ring area, adopts a hierarchical network structure, subdivides the ring area, and hides the cluster head by using the data packet format and the broadcast characteristics of the sensor node. In the initialization phase of the scheme, the inter-cluster and intra-cluster keys are constructed and the keys are updated. The key distribution scheme based on the binary symmetric polynomial and the key distribution scheme based on the Chinese remainder theorem are used to realize the inter-cluster and intra-cluster key communication; in the execution phase, operations such as cluster head replacement, node exit, and node addition are performed. Experimental results show that, compared with the existing scheme, this scheme balances the contradictory relationship between connectivity, energy consumption and security, has higher security and effectiveness, and also has lower energy consumption.

Key words: wireless sensor network; key management; cluster head; security; routing

0　引　言

无线传感器网络(wireless sensor network,WSN)通常由大量具有有限资源(包括有限计算能力、有限内存、有限电源和有限功率)的传感器节点组成[1]。每个传感器节点包括四个子系统,即传感子系统、通信

引用格式:吴万青,张子扬,董亚华. 环形区域无线传感器网络的密钥管理方案[J]. 武汉大学学报(理学版),2022,68(1):83-92. DOI:10.14188/j.1671-8836.2021.2006.

WU Wanqing, ZHANG Ziyang, DONG Yahua. Key Management Scheme of Wireless Sensor Network in Ring Area [J]. *J Wuhan Univ* (*Nat Sci Ed*), 2022, 68(1): 83-92. DOI: 10.14188/j.1671-8836.2021.2006(Ch).

子系统、计算子系统和电源子系统[2]。传感器节点具有监控物理环境的能力,已经广泛应用于工业、农业等行业及智能家居和人体可穿戴设备[3]。

随着无线传感器网络的日益普及,其安全性逐渐引起了公众的关注[3]。传感器节点之间的数据传输需要通过特定的加密技术来保证通信安全。目前的加密技术有非对称密钥加密技术和对称密钥加密技术。非对称密钥加密技术能量开销(包括存储开销、计算开销和通信开销)较大,所以它无法很好地适用于无线传感器网络。相对于非对称加密,对称密钥拥有更低的计算开销和通信开销,因此对称密钥加密技术在无线传感器网络得到广泛应用[4]。

为了减少无线传感器网络能量开销,提高网络安全性,学者们对对称密钥分配方案进行了研究。2016年,Selva等[5]针对前人方案安全性能随着受损节点数量的增加而降低的问题,提出了一种基于多项式和多元映射的三重密钥分配方案。2017年,Chakavarika等[6]提出了一种改进的节能密钥分发和管理方案。此方案在存储开销和计算开销方面是可扩展的,在密钥更新阶段引入加密的随机数提高了网络安全性。Messai等[7]针对网络的安全性随着时间下降的问题,提出了一种适用于多相无线传感器网络的密钥预分配方案——多相q-composite密钥方案(multi-phase q-composite keys scheme,MPQ)。该方案在q-composite密钥方案的基础上进行改进,增加了网络的自愈能力。Gandino等[8]针对q-composite方案的内存开销问题,提出了一种新的协议q-s-composite,提高了内存管理效率。2019年,Albakri等[9]提出了一种基于概率多项式的组密钥预分发方案(group key pre-distribution scheme,GKPS),显著降低了传感器遭受节点捕获攻击的概率,提高了无线传感器网络的安全性。2020年,Manasrah等[10]基于多项式池密钥预分配方案和分块逻辑单元分解算法,提出了一种高效的无线传感器网络密钥管理方案。该方案使用多个空间来获得共享密钥,确保任何两个通信节点在通信开始之前必须共享一个公共密钥,减少了预先分配给传感器节点的信息量。同年,Li等[11]针对文献[8]中q-s-composite方案不能抵御节点复制攻击的缺点,提出了一种安全的随机密钥分配方案(secure random key distribution scheme,SRKD),将本地化算法与投票机制相结合,以支持恶意节点的检测和撤销,并进一步更改参数以抵御节点复制攻击。Harn等[12]针对无线传感器计算能力有限的问题,提出了一种新颖的密钥分配方案。其密钥分发协议只需要逻辑异或操作,相比其他方案,运算速度要快得多。

为了提高无线传感器网络的可管理性,延长网络的寿命,学者们提出了基于簇的密钥分配方案。2020年,Rehman等[13]利用多项式来实现有效的簇内密钥管理,并生成多项式来进行簇间密钥分配,通过减小密钥池的大小来延长网络的生存时间。2021年,Fang等[14]为了抵御内部攻击,提出了基于二项分布的轻量级信任管理方案(lightweight trust management scheme,LTMS),同时引入距离域、能量域、安全域和环境域,提出了基于动态维度权重的多维安全分簇路由(multidimensional secure clustered routing,MSCR)方案,实现了安全性、传输性能和能效之间的平衡。但是,在该方案中如果簇头被捕获,则簇内所有节点都会面临安全威胁。

为了解决上述问题且在连通性、能量消耗和安全性之间寻找平衡,本文将无线传感器所在区域划分为环形区域,提出了一种环形区域无线传感器网络的密钥管理方案。

1 本文方案

在本文方案中,簇间通信使用基于二元对称多项式的密钥分配方案;簇内的通信使用基于中国剩余定理的密钥分配方案。本方案使用分层式网络结构,并对簇头进行了隐藏。表1列出了本方案所用符号。

密钥分配方案包括两个主要阶段:初始化阶段和执行阶段。

1.1 初始化阶段

1.1.1 网络拓扑

网络拓扑如图1所示。拓扑图中,每个圆之间的距离为$r/2$,其中r为节点通信半径。第一环为一个半径为$r/2$的圆。每个环都有标识符,为$R_1,R_2,\cdots,R_n$。在环内沿逆时针划分区域。第二环有9个子区域,第三环有15个子区域,…,第n环有$3\cdot(2n-1)$个子区域。并且每个子区域的标识符按逆时针为$R_2D_1,R_2D_2,\cdots,R_2D_9,\cdots,R_nD_{(3\cdot(2n-1))}$。其中,$D$为子区域标识。若节点在径向边界线上,则统一属于最小子区域编号的区域。若节点在环向边界线上,则统一属于最小环编号的区域。若节点在径向和环向的交叉线上,则统一属于最小环编号且最小子区域编号的区域。

1.1.2 网络模型和协议安全假设

1) 网络模型

本方案中,节点有三种类型:基站、簇头和普通

表1　本方案符号

Table 1　Symbols of this scheme

符号	描述	符号	描述
BS	基站	min(*C*)	求集合*C*内元素的最小值
CH	簇头	max(C)	求集合*C*内元素的最大值
$CH_{i,j}$	第*i*环的第*j*个子区域的簇头	H()	哈希函数
BCH	备用簇头	$E_K(A)$	对信息*A*用密钥*K*加密
R_iD_j	第*i*环的第*j*个子区域	$D_K(A)$	对信息*A*用密钥*K*解密
$S_{i,j,g}$	第*i*环第*j*个子区域编号为*g*的节点	$f_{r_i}(x,y)$	第*i*环的多项式
$a_{i,j,g}$	$S_{i,j,g}$封装的随机数	K_{CH-CH}	簇头之间的通信密钥
$m_{i,j,g}$	$S_{i,j,g}$封装的独立种子密钥	key	簇内成员节点间的公共密钥
$K_{i,j,g}$	$S_{i,j,g}$封装的独立密钥	k_g	簇内编号为*g*的成员节点与簇头的通信密钥
K_{init}	节点的初始密钥	E_r	节点剩余能量
K_{initch}	簇头的初始密钥	*D*	节点到簇内其他节点距离之和
$ID_{i,j,g}$	$S_{i,j,g}$的ID($0\sim2^{16}$)	r_{CH}	节点担任过簇头的轮数
$ID_{i,j}$	$CH_{i,j}$的ID($0\sim2^{16}$)	$\oplus$	异或操作
$N_{i,j}$	$CH_{i,j}$生成的随机数($0\sim2^{16}$)	$A \parallel B$	将信息*A*和信息*B*进行连接

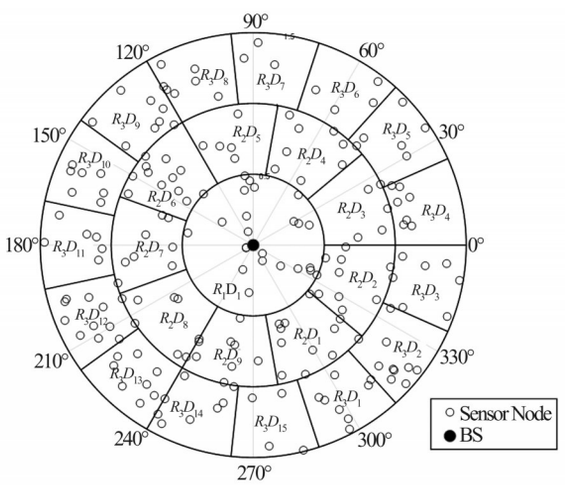

图1　网络拓扑

Fig. 1　Network topology

传感器节点。部署网络后,网络按照轮数运行,所有传感器节点都已固定,都拥有自己的剩余能量、所在区域、节点ID,且ID各不相同,并且具有确定的传输范围和传输速率。所有节点的初始电池电量、内存存储大小、CPU处理能力、无线电传输范围都相同。它们部署在一个监控区域。

基站是静态的且值得信任,通信范围覆盖整个传感器网络,具有无限的计算、通信和存储能力,并已经存储了网络中所有节点的基本信息。此外,基站可以验证节点的安全性。

簇头负责从簇内成员处收集数据,并逐层转发给基站。普通传感器节点负责收集周围环境数据,并将数据发送给其邻居节点或簇头。

成员节点只接收本区域的消息,不能向其他区域的节点发送消息,同时也不接收来自外部区域的消息,如果发送或接收,则被视为恶意成员节点。只有簇头可以接收外部区域消息,并且可以向外部区域发送消息。

2) 协议安全假设

在网络建立阶段,所有节点都不会被对手捕获,整个网络是安全的;一个子区域是一个簇,并且每个节点发送的消息总有一条路径可以到达基站;除了区域R_1以外,簇头只能与本区域的节点及其他区域的簇头进行通信;R_1区域的簇头可以和本区域节点、其他区域的簇头通信,并且可以和基站进行直接通信;所有节点(包括基站)只能以广播的形式进行通信。

1.1.3　密钥初始化阶段

1.1.3.1　簇头指定和密钥部署阶段

节点$S_{i,j,g}$部署之前封装一个随机数$a_{i,j,g}$、一个独立的种子密钥$m_{i,j,g}$、一个独立密钥$K_{i,j,g}$和一个相同的初始密钥K_{init}(其中,*i*代表环编号,*j*代表子区域编号,*g*代表节点在区域内的编号)。

所有节点同时开机,按照封装随机数的顺序使用数据包格式1(图2)广播ID,每个节点只接收本区域内的数据包,存储同区域其他节点的ID,加入ID列表,并回复确认消息。节点将自己的ID和所在区域标识发送至基站。基站将收到节点的ID和所在区域标识存储到列表中。

1) 簇头指定阶段。所有的簇头和备用簇头由基站随机指定,并验证其安全性,将簇头作为信任节点。基站为每个簇头生成新的ID(记作$ID_{i,j}$)和簇头的初

图2 数据包格式1

Fig. 2 Packet format 1

始密钥K_{initch}。将$E_{k_{i,j,g}}(\text{ID}_{i,j}, K_{\text{initch}}, \text{Hello CH})$广播至对应簇头,根据列表按环分批进行广播。首先广播第一环,然后逐步加大信号强度到最后一环。簇头对比数据包找到自己的区域标识并对比数据包中目的ID来接收发送给自己的消息。所以,只有簇头节点可收到并使用独立密钥$K_{i,j,g}$通过$D_{k_{i,j,g}}(\text{ID}_{i,j}, K_{\text{initch}}, \text{Hello CH})$解密得到消息,知道自己是簇头。

2)密钥部署阶段。基站在每个簇中寻找种子密钥的最小值$\min(m_{i,j,g})$并将$\min(m_{i,j,g})$发送至对应区域簇头,通知簇头广播自己的$\text{H}(\text{ID}_{i,j})$,相邻区域簇头和本区域成员节点接收$\text{H}(\text{ID}_{i,j})$并将其存储。

基站在有限域$\text{GF}(p)$上生成大量二元t次对称多项式

$$f_{r_i}(x,y)=\sum_{c,e=0}^{t} a_{ce}x^c y^e (\bmod p) \tag{1}$$

其中,有限域的素数p应该足够大。每个多项式有两个变量(x,y)和两个整数系数t以及从$\text{GF}(p)$中随机选择的a_{ce}。基站用每个簇头的ID替换簇头所在环和上一环多项式中的x,生成$f_{r_i}(\text{ID}_{i,j}, y)$和$f_{r_{i-1}}(\text{ID}_{i,j}, y)$。密钥分发中心(KDC)将$f_{r_i}(\text{ID}_{i,j}, y)$发送至第$r_i$环和第$r_i-1$环的所有簇头(第一环只存储$f_{r_1}(\text{ID}_{1,1}, y)$),直到网络中除了第一环以外,所有的簇头都收到$f_{r_i}(\text{ID}_{i,j}, y)$和$f_{r_{i-1}}(\text{ID}_{i,j}, y)$。

1.1.3.2 簇间密钥发现阶段

本阶段主要工作为:生成簇头之间的通信密钥$K_{\text{CH-CH}}$。

属于不同环的相邻子区域的簇头可以建立通信密钥。但是,属于相同环的簇头不能建立通信密钥。假设$\text{CH}_{1,1}$,$\text{CH}_{2,1}$分别为第一环的第一个子区域的簇头和第二环的第一个子区域的簇头。$\text{CH}_{1,1}$的ID为$\text{ID}_{1,1}$,$\text{CH}_{2,1}$的ID为$\text{ID}_{2,1}$。每个簇头节点在密钥初始化阶段已收到多项式,如$\text{CH}_{1,1}$收到$f_{r_1}(\text{ID}_{1,1}, y)$,$\text{CH}_{2,1}$收到$f_{r_2}(\text{ID}_{2,1}, y)$和$f_{r_1}(\text{ID}_{2,1}, y)$。

以下为簇间公共密钥发现阶段步骤:

Step 1 $\text{CH}_{1,1}$使用数据包格式2(图3)广播$E_{K_{\text{initch}}}(\text{ID}_{1,1}, N_{1,1})$,目的ID的哈希值为相邻区域簇头的哈希值;

Step 2 $\text{CH}_{2,1}$收到消息,通过$D_{K_{\text{initch}}}(\text{ID}_{1,1}, N_{1,1})$解密得到$\text{ID}_{1,1}$和$N_{1,1}$;

图3 数据包格式2

Fig. 3 Packet format 2

Step 3 根据区域标识,将$\text{ID}_{1,1}$带入对应环的多项式中,用$\text{ID}_{1,1}$替换y,生成$f_{r_1}(\text{ID}_{2,1}, \text{ID}_{1,1})$;

Step 4 $\text{CH}_{2,1}$广播$E_{K_{\text{initch}}}(\text{ID}_{2,1}, N_{2,1})$;

Step 5 $\text{CH}_{1,1}$收到消息,通过$D_{K_{\text{initch}}}(\text{ID}_{2,1}, N_{2,1})$解密得到$\text{ID}_{2,1}$和$N_{2,1}$;

Step 6 根据区域标识,将$\text{ID}_{2,1}$带入对应环的多项式中,用$\text{ID}_{2,1}$替换y,生成$f_{r_1}(\text{ID}_{1,1}, \text{ID}_{2,1})$。所以在二元对称多项式$f_{r_i}(x,y)$中,$f_{r_1}(\text{ID}_{2,1}, \text{ID}_{1,1})=f_{r_1}(\text{ID}_{1,1}, \text{ID}_{2,1})$;

Step 7 $\text{CH}_{1,1}$生成与$\text{CH}_{2,1}$的通信密钥

$$K_{\text{CH}_{1,1}-\text{CH}_{2,1}}=\text{H}(f_{r_1}(\text{ID}_{2,1}, \text{ID}_{1,1})\|\max(\text{ID}_{1,1}, \text{ID}_{2,1})\|\min(N_{1,1}, N_{2,1}))$$

Step 8 $\text{CH}_{1,1}$向$\text{CH}_{2,1}$回复确认消息;

Step 9 $\text{CH}_{2,1}$生成与$\text{CH}_{1,1}$的通信密钥

$$K_{\text{CH}_{2,1}-\text{CH}_{1,1}}=\text{H}(f_{r_1}(\text{ID}_{2,1}, \text{ID}_{1,1})\|\max(\text{ID}_{1,1}, \text{ID}_{2,1})\|\min(N_{1,1}, N_{2,1}))$$

且$K_{\text{CH}_{1,1}-\text{CH}_{2,1}}=K_{\text{CH}_{2,1}-\text{CH}_{1,1}}$。

1.1.3.3 簇内密钥建立阶段

本阶段主要工作为:利用中国剩余定理生成簇内成员节点与簇头的通信密钥k_g。

中国剩余定理如下

$$\begin{cases} X\equiv k_1(\bmod m_{i,j,1}) \\ X\equiv k_2(\bmod m_{i,j,2}) \\ X\equiv k_3(\bmod m_{i,j,3}) \\ \quad\vdots \\ X\equiv k_n(\bmod m_{i,j,n}) \end{cases} \tag{2}$$

其中,n为簇内成员节点的数量,k_g为成员节点和簇头的通信密钥。$m_{i,j,g}$为节点的种子密钥。k_g由X和节点的种子密钥$m_{i,j,g}$计算得到。根据中国剩余定理,k_g是互素的,并且同余的,所以X有唯一解。

设 $M=m_{i,j,1}\cdot m_{i,j,2}\cdot m_{i,j,3}\cdot\cdots\cdot m_{i,j,n}=\prod_{i=1}^{n} m_{i,j,g}$,$M_g=M/m_{i,j,g}$,$t_g=M_g^{-1}$,所以$X$的计算如下

$$X=\sum_{g}^{n} k_g t_g M_g (\bmod M) \tag{3}$$

簇头根据在密钥初始化阶段收到的$\min(m_{i,j,g})$,随机生成n个(n为簇内成员节点的数量)互不相等的通信密钥k_g,且$k_g\leqslant\min(m_{i,j,g})$。将所有$k_g$发送至基站。基站根据每个簇中所有成员节点的$m_{i,j,g}$和$k_g$利

用(3)式计算出每个簇的X,并将X发送至对应区域的簇头节点。X由簇头节点广播至区域内所有成员节点。簇内所有成员节点根据X和$m_{i,j,g}$计算自己与簇头的通信密钥k_g。计算过程如下

$$\begin{cases} k_1 = X(\bmod m_1) \\ k_2 = X(\bmod m_2) \\ k_3 = X(\bmod m_3) \\ \quad\vdots \\ k_n = X(\bmod m_n) \end{cases} \tag{4}$$

1.1.3.4　簇间密钥路径建立阶段

为了将数据路由到基站,以基站为根的簇头的定向虚拟骨干网(DVB)构建过程如下:

基站向第一环的簇头发送路由请求消息RREQ(包括自己的ID、等级)。基站的等级为0,即$L(\mathrm{BS})=0$,当第一环的$\mathrm{CH}_{v,j}$接收到请求消息,将自己的等级改为比基站高一级,即$L(v)=L(\mathrm{BS})+1$。并将基站作为自己的父节点,即$\mathrm{PN}(v)=\mathrm{BS}$。第一环的所有簇头指定为一级。递归地,$\mathrm{CH}_{v,j}$广播修改后的REEQ消息由它的ID、$L(v)$和$E_{\mathrm{r}}(v)$组成。如果$\mathrm{CH}_{u,j}$收到消息,并且它的级别$L(u)$等于或小于节点$v$的级别$L(v)$,那么$\mathrm{CH}_{u,j}$直接丢弃该消息。否则,$\mathrm{CH}_{u,j}$将其级别更新为比$\mathrm{CH}_{v,j}$的级别多一个级别,即$L(u)=L(v)+1$,并将其设置为其父节点之一,即$\mathrm{PN}(u)=v$。递归地,所有簇头广播RREQ,以完成定向虚拟骨干网的建立。

在定向虚拟骨干网中,一个簇头可能有多个父节点,因此通向基站的路径有多条。设$v_1,v_2,v_3,\cdots,v_p$是属于集合$\mathrm{PN}(u)$的一组簇头。在发送数据包之前,$\mathrm{CH}_{u,j}$计算比自己小一级别的邻居簇头的平均剩余能量:$E_{\mathrm{ave}}(u)=\dfrac{\sum_{i=1}^{p}E_{\mathrm{r}}(v_i)}{p}$。设$B=\{b_1,b_2,b_3,\cdots,b_l\}$是父节点中剩余能量大于或等于$E_{\mathrm{ave}}(u)$的簇头。$\mathrm{CH}_u$将包括其自身在内的所有需要发送的数据按以下比例分组分配:$E_r(b_1):E_r(b_2):E_r(b_3):\cdots:E_r(b_l)$,发送到相应的簇头。最终将数据汇聚到基站。

1.2　执行阶段

1.2.1　簇头更换

如果簇头节点的能量低于能量阈值,则将备用簇头替换为簇头并选取新的备用簇头。

需要被更换的簇头(记作$\mathrm{CH}_{\mathrm{old}}$)向基站发送簇头更换请求信息Change CH。基站通知备用簇头,将备用簇头充当为新的簇头(记作$\mathrm{CH}_{\mathrm{new}}$)。基站生成一个随机数$R$,并为$\mathrm{CH}_{\mathrm{new}}$生成$\mathrm{ID}_{(\mathrm{new})i,j}$,计算$K_{\mathrm{initch-new}}=R\oplus K_{\mathrm{initch}}$,将$\mathrm{CH}_{\mathrm{old}}$的种子密钥加入种子密钥列表,并对簇内所有节点的安全性进行验证。由于本方案侧重点并非恶意检测,所以本文将不再对恶意检测的区分以及是否需要定时检测进行详细说明。若发现恶意节点,则将恶意节点ID移除ID列表并通知簇内所有节点将其ID移除ID列表,直到区域中不存在恶意节点或者恶意节点ID已从所有节点的ID列表中移除才继续进行以下步骤。

基站删除列表中$\mathrm{CH}_{\mathrm{new}}$的种子密钥,将$\mathrm{CH}_{\mathrm{old}}$的种子密钥加入列表,寻找发生簇头更换区域内种子密钥的最小值$\min(m_{i,j,g})$,并将$\min(m_{i,j,g})$、$\mathrm{ID}_{(\mathrm{new})i,j}$和$K_{\mathrm{initch-new}}$发送至$\mathrm{CH}_{\mathrm{new}}$。将$R$发送给除$\mathrm{CH}_{\mathrm{new}}$以外所有簇头节点,簇头收到$R$后,计算$K_{\mathrm{initch-new}}=R\oplus K_{\mathrm{initch}}$。基站根据$\mathrm{CH}_{\mathrm{new}}$的ID生成$\mathrm{CH}_{\mathrm{new}}$所在环和上一环的多项式$f_{r_1}(\mathrm{ID}_{(\mathrm{new})i,j},y)$和$f_{r_1-1}(\mathrm{ID}_{(\mathrm{new})i,j},y)$,由KDC发送给$\mathrm{CH}_{\mathrm{new}}$。$\mathrm{CH}_{\mathrm{new}}$与邻居簇头交换ID和随机数生成新的簇间通信密钥$k_{\mathrm{CH-CH-new}}$,并随机生成$n$个($n$为簇内成员节点的数量)互不相等的通信密钥$k_g$,且$k_g\leqslant\min(m_{i,j,g})$,将所有$k_g$发送至基站。基站根据发生簇头更换区域中所有成员节点的$m_{i,j,g}$和k_g利用(3)式计算出簇内X_{new},并将X_{new}发送至$\mathrm{CH}_{\mathrm{new}}$。将$\mathrm{H}(\mathrm{ID}_{(\mathrm{new})i,j})$发送至簇内包括$\mathrm{CH}_{\mathrm{old}}$在内的所有成员节点。$\mathrm{CH}_{\mathrm{new}}$将$X_{\mathrm{new}}$广播至簇内所有成员节点并通知簇内所有成员节点广播自己的ID,所有成员节点收到X_{new}和ID后,回复确认消息并更新自己的ID列表,计算与$\mathrm{CH}_{\mathrm{new}}$的通信密钥$k_g$。随后,$\mathrm{CH}_{\mathrm{new}}$进行备用簇头选举阶段。

在备用簇头选举阶段,所有成员节点根据接收信号强度计算本节点到簇内其他节点的距离之和$D_{\mathrm{s}}(g)$。并将自己的剩余能量$E_{\mathrm{r}}(g)$、$D_{\mathrm{s}}(g)$和担任过簇头的轮数$r_{\mathrm{CH}}(g)$发送至$\mathrm{CH}_{\mathrm{new}}$。$\mathrm{CH}_{\mathrm{new}}$寻找簇内节点最大剩余能量$E_{\max}$、最小剩余能量$E_{\min}$和最大距离$D_{\max}$,并计算簇内所有成员节点剩余能量因素$E(g)=\dfrac{E_{\mathrm{r}}(g)-E_{\min}}{E_{\mathrm{r}}(g)}$、节点之间距离因素$D(g)=\dfrac{D_{\max}-D_{\mathrm{s}}(g)}{D_{\max}}$和担任过簇头的轮数因素$R(g)=\dfrac{r_{\mathrm{total}}-r_{\mathrm{CH}}(g)}{r_{\mathrm{total}}}$。其中,$r_{\mathrm{total}}$表示网络运行过的轮数。$\mathrm{CH}_{\mathrm{new}}$为每个成员节点计算簇头选举参量值

$$Z_g=w_1\cdot D(g)+w_2\cdot E(g)+w_3\cdot R(g) \tag{5}$$

其中,w_1,w_2,w_3为权重,用来调整每个因素的重要程度,且$w_1+w_2+w_3=1$。

权重的更新公式为

$$w_2=\frac{E_{\max}-E_{\min}}{E_{\max}} \tag{6}$$

$$w_1 = w_3 = \frac{1 - w_2}{2} \tag{7}$$

簇内节点的剩余能量两极分化越来越严重,则(6)式分子越来越大,导致能量因素所占比例也会变大。CH_{new}比较所有成员节点的Z_g,选取具有最大Z_g的节点作为备用簇头,并通知基站验证其安全性,作为信任节点。基站为CH_{old}分配$ID_{i,j,g}$并将其作为普通成员节点。

1.2.2 节点主动退出

1)成员节点退出

要主动退出的节点(记作S_{leave})向自己所在区域的簇头广播自己的节点标识(记作ID_{leave})以及退出消息Leave。簇头收到消息后向基站发送ID_{leave}和退出请求消息。基站将S_{leave}的种子密钥删除,并对簇内所有节点的安全性进行验证,然后进行以下步骤。

基站向簇头回复确认消息并通知簇头随机生成n个(n为簇内成员节点的数量)互不相等的通信密钥k_g,且$k_g \leqslant \min(m_{i,j,g})$。簇头将生成的所有$k_g$发送至基站;基站根据簇内成员节点的$m_{i,j,g}$和$k_g$利用(3)式计算得到$X_{new}$,并将$X_{new}$发送至簇头。基站和簇头将$ID_{leave}$移除ID列表。簇头将$X_{new}$发送至簇内所有成员节点,并通知簇内成员节点将$ID_{leave}$移除ID列表。成员节点收到$X_{new}$后,计算新的$k_g$。基站检查$ID_{leave}$,若$S_{leave}$是备用簇头节点,基站向簇头发送执行备用簇头选举操作命令。由簇头执行备用簇头选举。若S_{leave}不是备用簇头节点,则不进行备用簇头选举。

2)簇头退出

要退出的簇头(记作CH_{leave})发送退出请求消息Leave至基站。基站删除种子密钥列表中CH_{new}和CH_{leave}的种子密钥,然后执行簇头更换操作,将备用簇头替换要退出的簇头并选举新的备用簇头。

1.2.3 节点被捕或意外损坏

1)成员节点被捕或意外损坏

簇头定时检查区域内每个成员节点是否有消息回传。若没有,簇头向基站广播丢失节点的标识(记作ID_{loss})和节点丢失消息Loss。基站针对丢失节点执行簇内成员节点退出操作,更新k_g。

2)簇头被捕或意外损坏

基站定时检查每个区域的簇头是否有消息回传。若没有,则基站通知备用簇头作为新的簇头。基站针对丢失簇头执行簇头退出操作,更新K_{initch}、k_{CH-CH}、k_g并选举新的备用簇头。

1.2.4 节点加入

要加入网络的节点(记作S_{join})向所在区域簇头发送S_{join}的节点标识(记作ID_{join})和加入请求Join。簇头收到消息后向基站发送ID_{join}和节点加入请求Join。

基站对S_{join}所在簇内所有成员节点以及S_{join}进行安全性验证。若发现恶意节点是S_{join},则禁止S_{join}加入网络;否则,删除恶意节点并进行以下步骤。

基站将ID_{join}和S_{join}的种子密钥加入列表,寻找发生节点加入区域内节点种子密钥的$\min(m_{i,j,g})$,并将$\min(m_{i,j,g})$发送至簇头。簇头随机生成n个(n为簇内成员节点的数量)互不相等的通信密钥k_g,且$k_g \leqslant \min(m_{i,j,g})$,并将生成的所有$k_g$发送至基站。基站根据发生节点加入区域中所有成员节点的$m_{i,j,g}$和k_g利用(3)式计算出簇中新的X_{new},并将X_{new}发送至簇头。将簇头ID的哈希值发送至S_{join};簇头将X_{new}发送至簇内所有成员节点并通知簇内所有成员节点广播自己的ID,所有成员节点收到X_{new}和ID后,回复确认消息并更新自己的ID列表,计算与簇头的通信密钥k_g。

2 方案分析与仿真

本节将对密钥分发的正确性、安全性、连通性和能量消耗四个部分进行详细的分析。本方案和文献[3]方案的实验环境都是基于Windows 10(64位)系统,硬件配置是Intel(R)Core(TM)i5-9400(2.90 GHz)处理器,8 GB内存,采用MATLAB进行仿真实验。本方案加密消息使用AES对称加密算法,且多项式中的系数a_{ce}从GF(p)中随机选择。仿真参数如表2所示。

表2 仿真参数

Table 2 Simulation parameters

参数	参数值
监测区域半径/m	1 500
节点总数	600
部署方式	随机部署
节点通信半径/m	500
初始能量/J	2
E_{mul}/μJ	3.2
E_{send}/(μJ·bit^{-1})	60
$E_{receive}$/(μJ·bit^{-1})	30
E_{rinit}/μJ	760

2.1 密钥分发的正确性

密钥分发的正确性分析主要是分析密钥分发阶段执行的正确性,即密钥分发阶段执行完毕之后

是否达成了密钥分发阶段的目标。

节点在部署之前就已封装好K_{init}和$K_{i,j,g}$，K_{initch}的分发消息由$K_{i,j,g}$进行加密，$K_{i,j,g}$是节点独立的密钥且只有基站和$S_{i,j,g}$拥有，所以K_{initch}只有指定的簇头节点可以解密得到；多项式由基站生成，由KDC用$K_{i,j,g}$加密分发，只有指定的簇头节点可以解密得到，ID和随机数的交换用K_{initch}加密，簇头可信且K_{initch}是安全的，只有邻居簇头节点可以解密消息并生成$K_{\text{CH-CH}}$；k_g由节点独立的种子密钥和X计算得到，在寻找最小种子密钥之前，基站对簇内成员节点进行安全性验证。保证了$\min(m_{i,j,g})$的正确性，进而保证了k_g的正确性。X由基站生成用独立密钥$K_{i,j,g}$加密发送至簇头，由簇头用K_{init}加密广播至簇内所有成员节点，成员节点不能接收其他区域数据包，只有本区域节点可以收到X，保证了X分发的正确性；每个阶段开始之前都会由基站对簇内成员节点进行安全性验证，选举备用簇头的参与者都是安全节点，保证了备用簇头选举过程的正确性。

2.2　安全性

2.2.1　鲁棒性

考虑到网络中可能存在恶意参与者，他们会通过向协议中输入非法数据或者非法执行协议等行为来对协议的执行过程造成威胁，进而获取有用信息或者影响协议执行。鲁棒性要求本方案在有恶意参与者的情况下能部分地正确执行，同时也要保证其他诚实节点所持有秘密信息的安全性。

本方案中所有节点都是以广播的形式进行通信，数据包中的源ID和目的ID都由特定的哈希函数处理得到。网络中除邻居区域的簇头以外，其他节点都没有簇头的ID，所以簇头对于除邻居簇头以外的所有节点都是保密的。假设簇内共有P个节点，理想状态下簇头被捕获的概率为$\frac{1}{P}$，所以从簇内所有节点中找到簇头是困难的。由于簇头的ID列表中存有其他簇头ID，则攻击者捕获簇头并从其ID列表中获得其他邻居簇头ID的概率为$\frac{T}{P\cdot(P-1)}$，其中T为邻居簇头的数量。

成员节点和簇头的通信密钥k_g由(4)式计算得出，其中$m_{i,j,g}$为每个节点独立的种子密钥，对其他节点保密。即使成员节点中存在恶意参与者，但恶意参与者同簇头的通信密钥k_g与其他成员节点的不同。所以，恶意参与者无法影响其他成员节点与簇头的通信，也无法冒充簇头与其他成员节点进行通信。假设簇内共有P个节点，根据(2)式可得，要想求出X，则必须捕获所有成员节点，即捕获$(P-1)$个节点。捕获的节点数小于$P-1$，恶意参与者无法得出未被捕获成员节点与簇头的通信密钥k_g。

2.2.2　密钥分发的安全性

由于节点在部署之前就已封装好K_{init}和$K_{i,j,g}$，K_{initch}的分发消息由$K_{i,j,g}$进行加密，$K_{i,j,g}$是节点所独有的密钥且簇头是可信的，保证了K_{initch}分发的安全；$K_{\text{CH-CH}}$由多项式、簇头ID和簇头生成的随机数经过特定哈希函数作用生成。多项式由基站生成，KDC用$K_{i,j,g}$加密并分发，相邻簇头交换(包括ID和随机数)的消息由K_{initch}加密，保证了$K_{\text{CH-CH}}$生成的安全性；k_g由节点独立的种子密钥和X计算得到。X由基站生成用$K_{i,j,g}$加密发送至簇头，由簇头用K_{init}加密广播至簇内所有成员节点，成员节点不能接收其他区域数据包，只有本区域节点可以收到X。所以，保证了X分发过程的安全性，进而保证了k_g生成的安全性。

2.2.3　方案的安全性

在网络建立阶段，整个网络处于安全状态，所以只针对网络的执行阶段进行安全性分析。

由于本方案中所有节点都是以广播的形式进行通信，数据包中的源ID和目的ID都由特定的哈希函数处理得到。所以簇头对于所有节点都是保密的，从簇内所有节点中找到簇头是困难的；基站和簇头会定时检测簇头和簇内成员节点是否有消息回传，保证了整个网络的安全性；每个阶段开始之前都会由基站对簇内成员节点进行安全性验证，所以参与备用簇头选举的节点都是安全节点，即使有恶意节点捕获成员节点向簇头发送的能量距离等参考信息，但是由于恶意节点没有(5)式中的权重w_1，w_2，w_3以及权重的更新公式，无法计算出Z_g，所以备用簇头的选举过程是安全的；基站与特定节点之间的通信由独立密钥$K_{i,j,g}$加密从而保证了安全性；簇头之间的通信由$K_{\text{CH-CH}}$加密，由于簇头是可信的，所以簇头之间的通信是安全的；簇头和成员节点之间的通信由k_g加密，密钥生成时，簇头将X分发至成员节点，由于$m_{i,j,g}$为节点独立种子密钥，所以即使有恶意节点截获X，也无法计算出k_g。如果某个成员节点被捕获，则攻击者只可得到被捕获的成员节点的k_g、$m_{i,j,g}$和X，由于每个成员节点k_g都是独立的，只和成员节点封装的独立种子密钥有关，攻击者无法获得其他成员节点和簇头的通信密钥，所以无法影响簇内其他成员节点和簇头的通信。

2.3　连通性

在文献[3]方案中，每对节点都可以建立通信

密钥,全局连通率为1。在本方案中,从簇内连通性来看,簇内所有成员节点都与所在子区域簇头建立独立簇内通信密钥,所以簇内所有成员节点可以和所在子区域簇头通信。由于每个子区域面积小于节点通信范围,成员节点可以与同区域内其他节点通信,所以局部连通率为1。从簇间连通性来看,由于不同环的簇头可以建立通信密钥,相同环的簇头不能建立通信密钥,簇头只能径向通信。所以,不同环相邻子区域的所有节点可以通信。相同环相邻子区域的所有节点不能通信。因此,本方案中全局连通率小于1。本方案的全局连通率与节点的数量有关,如图4所示,节点数量越多,连通率越大。

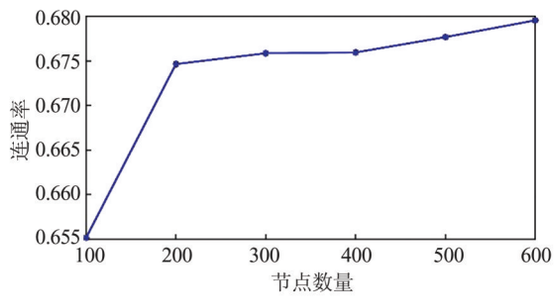

图4 本方案的连通性

Fig. 4 Connectivity of our method

2.4 能量消耗

对于无线通信,图5中显示了节点的简单通用能耗模型。接收k bits数据包的能量开销为$E_{rk}(k)$,发送k bits数据包的能量开销为$E_{TX}(k,d)$,计算公式分别如下

$$E_{rk}(k)=kE_{elec} \tag{8}$$

$$E_{TX}(k,d)=kE_{elec}+k\varepsilon_{mp}d^4 \tag{9}$$

其中,E_{elec}是接收或发送1 bit消息的能量开销,ε_{mp}为多径衰落因子,d为通信距离,$\varepsilon_{mp}d^4$是放大器放大每比特消息的能量开销。

下面将从存储、计算和通信三个方面分析网络的能量开销。

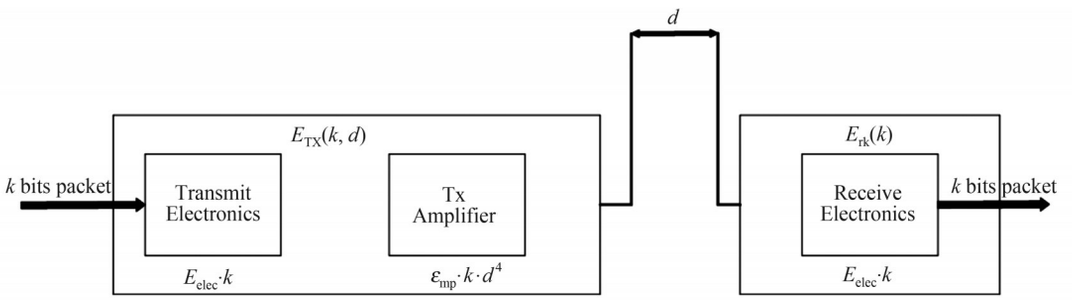

图5 能耗模型

Fig. 5 Energy consumption model

2.4.1 存储开销

假设网络中共有C个节点。则在文献[3]方案中,每个节点都要存储4个多项式、1个初始密钥和所有邻居节点ID,网络总存储开销为$O(C^2)$。在本方案中,随机数$a_{i,j,g}$、种子密钥$m_{i,j,g}$、成员节点和簇头的通信密钥k_g、独立密钥$K_{i,j,g}$、X、初始共享密钥K_{init}以及簇头共享的初始密钥K_{initch}各自都占用16 bits内存。每个对称二元多项式的系数占用$\log_2 p$ bits内存。所以每个多项式占用$(t+1)\log_2 p$ bits内存。在初始化阶段,每个节点都需要维护一个同区域节点ID列表(该列表记录了同区域内所有安全节点的ID)。假设每个ID占用16 bits内存,一个簇内共有P个节点,共有W个簇。所以,一个ID列表占用$(P-1)\cdot 16$ bits内存。假设每一位存储能量开销为E_b。

所有簇头的存储开销为

$$E_{SCH}=(6\cdot 16+(P-1)\cdot 16+(t+1)\log_2 p+(P-1)\cdot 16+16)\cdot W\cdot E_b \tag{10}$$

所有成员节点的存储开销为

$$E_{SSN}=(6\times 16+(P-1)\times 16+16)\cdot(C-W)\cdot E_b \tag{11}$$

所以,所有C个节点的存储总开销为

$$E_{Stotal}=E_{SCH}+E_{SSN} \tag{12}$$

因此,本方案总存储开销为$O(C^2)$。

由图6可知,当节点数量相同时,存储开销随着多项式次数t的增大而增大;当t相同时,存储开销随着节点数量的增大而增大。

2.4.2 计算开销

在文献[3]方案中,每对节点间建立一次通信,密钥需要进行8次多项式和两次哈希函数计算,网络总计算开销为$O(C^2)$。在本方案中,假设一个多项式的计算开销为E_f,哈希函数的计算开销为E_h,一次乘法的计算开销为E_{mul},一次加法的计算开销为E_{plus},一次模运算的计算开销为E_{mod}。

计算二元对称多项式需要$(t+1)^2$次乘法和t次加法,因此一个多项式的计算开销为

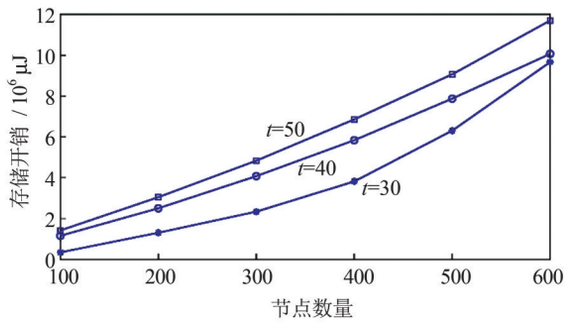

图6　不同t值和节点数量对存储开销的影响

Fig. 6　The impact of different t values and the number of nodes on storage overhead

$$E_{\mathrm{f}}=(t+1)^2E_{\mathrm{mul}}+tE_{\mathrm{plus}} \tag{13}$$

假设$T_{K_{\mathrm{CH-CH}}}$为$K_{\mathrm{CH-CH}}$建立的次数，则簇头建立$K_{\mathrm{CH-CH}}$的计算总开销为

$$E_{CK_{\mathrm{CH-CH}}}=T_{K_{\mathrm{CH-CH}}}\cdot(2E_{\mathrm{f}}+2E_{\mathrm{h}}) \tag{14}$$

成员节点建立k_g的计算总开销为

$$E_{Ck_g}=(C-W)\cdot E_{\mathrm{mod}} \tag{15}$$

所以，所有C个节点的计算总开销为

$$E_{\mathrm{Ctotal}}=E_{CK_{\mathrm{CH-CH}}}+E_{Ck_g} \tag{16}$$

因此，本方案总计算开销为$O(C)$。

由图7可以看出，与文献[3]方案相比，本方案计算开销受节点数量变化的影响较小，并且当节点数量相同时，本方案的计算开销小于文献[3]方案。

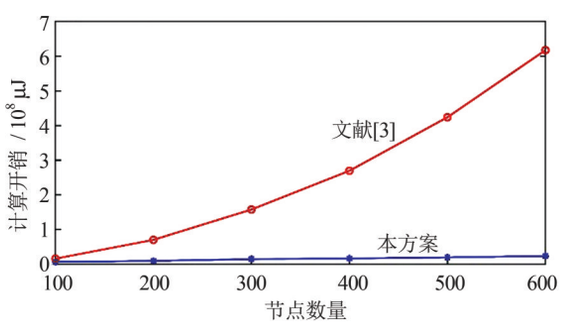

图7　计算开销对比

Fig. 7　Comparison of computational cost

2.4.3　通信开销

在文献[3]方案中，每对节点间建立一次通信密钥需要发送两次数据包和接收两次数据包，网络总通信开销为$O(C^2)$。在本方案中，在簇头指定和密钥部署阶段，每个节点的通信开销为E_{rinit}。

节点向其他节点发送k bits数据包的能量开销为E_{Tr}。节点向其他节点发送一个数据包的能量开销为

$$E_{\mathrm{send}}=E_{\mathrm{Tr}}\cdot k \tag{17}$$

节点从其他节点接收k bits数据包的能量开销为E_{Re}。节点从其他节点接收一个数据包的能量开销为

$$E_{\mathrm{receive}}=E_{\mathrm{Re}}\cdot k \tag{18}$$

生成$K_{\mathrm{CH-CH}}$，节点之间需要建立3次通信，所以，生成$K_{\mathrm{CH-CH}}$的通信总开销为

$$E_{TK_{\mathrm{CH-CH}}}=3\cdot T_{K_{\mathrm{CH-CH}}}\cdot(E_{\mathrm{send}}+E_{\mathrm{receive}}) \tag{19}$$

成员节点建立k_g，簇头需要发送两次和接收一次数据包，成员节点需要接收一次数据包。所以，生成k_g的通信总开销为

$$E_{Tk_g}=2\cdot W\cdot E_{\mathrm{send}}+C\cdot E_{\mathrm{receive}} \tag{20}$$

假设每个簇头各自收到Q个数据包，则执行阶段的通信总开销为

$$E_{\mathrm{Twork}}=(Q\cdot k\cdot(E_{\mathrm{send}}+E_{\mathrm{receive}})+(Q+1)\cdot k\cdot E_{\mathrm{send}})\cdot W \tag{21}$$

所以，所有C个节点的通信总开销为

$$E_{\mathrm{Ttotal}}=E_{TK_{\mathrm{CH-CH}}}+E_{Tk_g}+E_{\mathrm{Twork}}+E_{\mathrm{rinit}} \tag{22}$$

因此，本方案总通信开销为$O(C)$。

由图8可以看出，与文献[3]方案相比，本方案的通信开销更低，并且本方案通信开销受节点数量变化的影响较小。

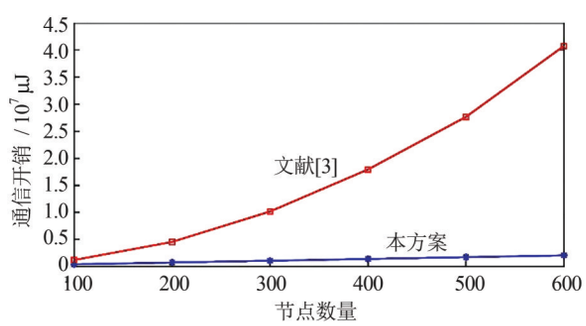

图8　通信开销对比

Fig. 8　Communication overhead comparison

综上所述，网络的总能量开销为

$$E=E_{\mathrm{Stotal}}+E_{\mathrm{Ctotal}}+E_{\mathrm{Ttotal}} \tag{23}$$

表3给出了本方案与文献[3]方案的性能比较结果。从表3和实验结果可以得出，虽然本方案的全局连通率较低，但是本方案的通信开销和计算开

表3　本方案与文献[3]方案的性能比较

Table 3　Performance comparison between this scheme and the Ref.[3] scheme

性能	本方案	文献[3]方案
连通率	局部连通率为1，全局连通率小于1	1
存储开销	$O(C^2)$	$O(C^2)$
通信开销	$O(C)$	$O(C^2)$
计算开销	$O(C)$	$O(C^2)$

销更小,并且本方案采用分层式网络结构增强了网络的可管理性和安全性。

3 结 语

本文提出了一种环形区域无线传感器网络的密钥管理方案。首先,该方案使用对称密钥技术,簇间为基于二元对称多项式的通信密钥分配,每环各分配一个二元对称多项式,显著节约传感器节点的通信和计算开销。簇内为基于中国剩余定理的通信密钥分配,使得每个成员节点和簇头的通信密钥各不相同,在减少存储空间的同时大大提升网络的鲁棒性。其次,该方案采用分层式网络结构,簇头负责从簇内成员处收集数据转发给基站,普通传感器节点负责收集周围环境数据,并将数据发送给簇头,提高了网络的效率和可管理性。最后,该方案充分利用数据包格式和传感器节点的广播特性,实现对簇头的隐藏,提高了网络的鲁棒性,保证了节点间的安全通信。实验结果表明,本方案具有更高的安全性和有效性。此外,与已有方案相比,本方案还具有更低的能量消耗。

参考文献:

[1] KUMAR A, BANSAL N, PAIS A R. New key pre-distribution scheme based on combinatorial design for wireless sensor networks[J]. *IET Communications*, 2019, **13**(7): 892-897. DOI:10.1049/iet-com.2018.5258.

[2] RAWAT P, CHAUHAN S, PRIYADARSHI R. A novel heterogeneous clustering protocol for lifetime maximization of wireless sensor network[J]. *Wireless Personal Communications*, 2021, **117**(2): 825-841. DOI:10.1007/s11277-020-07898-8.

[3] LIU Y H, WU Y M. A key pre-distribution scheme based on sub-regions for multi-hop wireless sensor networks[J]. *Wireless Personal Communications*, 2019, **109**(2): 1161-1180. DOI:10.1007/s11277-019-06608-3.

[4] WANG N C, CHEN Y L, CHEN H L. An efficient grid-based pairwise key predistribution scheme for wireless sensor networks [J]. *Wireless Personal Communications*, 2014, **78**(2): 801-816. DOI: 10.1007/s11277-013-1493-1.

[5] SELVA R A, BABURAJ E. Polynomial and multivariate mapping-based triple-key approach for secure key distribution in wireless sensor networks[J]. *Computers & Electrical Engineering*, 2017, **59**: 274-290. DOI: 10.1016/j.compeleceng.2016.10.018.

[6] CHAKAVARIKA T T, GUPTA S K, CHAURASIA B K. Energy efficient key distribution and management scheme in wireless sensor networks[J]. *Wireless Personal Communications*, 2017, **97**(1): 1059-1070. DOI: 10.1007/s11277-017-4551-2.

[7] MESSAI M L, SEBA H. A self-healing key pre-distribution scheme for multi-phase wireless sensor networks [C]//2017 *IEEE Trustcom/BigDataSE/ICESS*. New York: IEEE Press, 2017: 144-151. DOI:10.1109/Trustcom/BigDataSE/ICESS.2017.231.

[8] GANDINO F, FERRERO R, REBAUDENGO M. A key distribution scheme for mobile wireless sensor networks: *q-s*-composite[J]. *IEEE Transactions on Information Forensics and Security*, 2017, **12**(1): 34-47. DOI: 10.1109/TIFS.2016.2601061.

[9] ALBAKRI A, HARN L. Non-interactive group key pre-distribution scheme (GKPS) for end-to-end routing in wireless sensor networks [J]. *IEEE Access*, 2019, **7**: 31615-31623. DOI:10.1109/ACCESS.2019.2900390.

[10] MANASRAH A M, AL-RABADI A R, KOFAHI N A. Key pre-distribution approach using block LU decomposition in wireless sensor network[J]. *International Journal of Information Security*, 2020, **19**(5):579-596. DOI: 10.1007/s10207-019-00477-4.

[11] LI L P, XU G Q, JIAO L T, *et al*. A secure random key distribution scheme against node replication attacks in industrial wireless sensor systems [J]. *IEEE Transactions on Industrial Informatics*, 2020, **16**(3):2091-2101. DOI: 10.1109/TII.2019.2927296.

[12] HARN L, HSU C F, XIA Z. Lightweight and flexible key distribution schemes for secure group communications [J]. *Wireless Networks*, 2021, **27**(1):129-136. DOI:10.1007/s11276-020-02449-2.

[13] REHMAN E, SHER M, HUSNAIN S, *et al*. Polynomial based dynamic key management for secure cluster communication in wireless mobile sensor network [J]. *Tehnicki Vjesnik—Technical Gazette*, 2020, **27**(2):358-367. DOI: 10.17559/TV-20170807075015.

[14] FANG W D, ZHANG W X, CHEN W, *et al*. MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks[J]. *EURASIP Journal on Wireless Communications and Networking*, 2021, **2021**(1):1-20. DOI:10.1186/s13638-020-01884-1.

□