文章编号:1009-3087(2014)03-0080-09

基于异构性的传感网密钥预分配协议设计与评测

王希忠[1,2],钟晓睿[3*],陈德运[1],曲家兴[2],方 舟[2],马春光[3]
(1. 哈尔滨理工大学 计算机科学与技术学院,黑龙江 哈尔滨 150001;2. 黑龙江省电子信息产品监督检验院,黑龙江 哈尔滨 150090;
3. 哈尔滨工程大学 计算机科学与技术学院,黑龙江 哈尔滨 150001)

摘 要:针对现有异构性研究系统性不足,缺乏与现实世界相契合的适用模型等问题,对传感网异构性进行了详细划分,并基于空间理论提出了形式化的异构空间模型,分析了动态异构性的变化趋势。随后,针对动态能量异构提出了一种能量有效的随机密钥预分配协议,并在特定的异构空间模型下对长期连通概率、抗毁性以及协议性能进行了评测。仿真实验结果表明,通过合理利用异构性,所提方案能够在保持一定连通概率、提高抗毁性的基础上,提供较其他同类方案更长的网络寿命。

关键词:传感网;异构性;密钥预分配;性能评测
中图分类号:TP393.08 **文献标志码**:A

Heterogeneity-based Design and Evaluation of Key Predistribution Protocols for Wireless Sensor Networks

WANG Xizhong[1,2], *ZHONG Xiaorui*[3*], *CHEN Deyun*[1], *QU Jiaxing*[2], *FANG Zhou*[2], *MA Chunguang*[3]
(1. College of Computer Sci. and Technol., Harbin University of Sci. and Technol., Harbin150001, China;
2. Heilongjiang Province Electronic and Info. Products Supervision Inspection Inst., Harbin 150090, China;
3. College of Computer Sci. and Technol., Harbin Eng. Univ., Harbin 150001, China)

Abstract: To compensate the lack of systematicness and realistic model, heterogeneities were classified into several categories, a heterogeneity space model was built up by utilizing space theory, and the variation trend of dynamic heterogeneity was discussed. Then, an energy efficient random key pre-distribution protocol was proposed, which is inspired by dynamic energy heterogeneity. Under a certain heterogeneity space model, several evaluation metrics including long-term network connectivity, resilience and lifetime were also analyzed. Simulation result showed that by rational using of heterogeneity, the proposed protocol doesn't only keep connectivity and improve resilience, but also provide a much better network lifetime than other protocols.

Key words: sensor network; heterogeneity; key predistribution; performance evaluation

传感器节点是传感网的最小组成单元,传感网的异构性也始于"传感器节点的异构性"。近年来,研究者们通过将一些能量充足,安全性好,计算效率高的高级节点引入传感网中,将协议设计为分簇管理模式,并将耗能的复杂操作交给这些高级节点完成,显著提高了网络传输速率、改善了网络可靠性、减少了网络能耗、降低了端对端传输延迟、延长了网络寿命[1-3]。由此将异构传感网(heterogeneous sensor networks,以下简称HSN)总结为"由不同类型的传感器节点构成的网络"。

在异构传感网研究中,Yarvis等[4]首先对能量异构和链路异构进行了研究,证明了对HSN进行最优部署是一个NPC问题,但通过恰当部署异构节点可以成倍提高网络传输速率,延长网络寿命。Mhatre等[5]研究了在保证HSN寿命不变的前提下,两种不同类型节点的最优配置比例问题。随后,Mache等[3]研究了异构性对传感网安全的影响,提出一个轻量级点对点安全框架,为每个节点都配置

收稿日期:2013-10-30
基金项目:国家自然科学基金资助项目(61170241);黑龙江省杰出青年科学基金项目(JC201117)
作者简介:王希忠(1968—),男,博士生,研究员级高级工程师. 研究方向:网络安全;物联网安全.
* 通信联系人 E-mail:zhongxiaorui@hrbeu.edu.cn

了公私钥对,但只有高端节点执行签名运算。在国内,卿利等[6]提出一种适合 HSN 的分布式能量有效的成簇协议,基于节点剩余能量与网络节点平均能量的比例选举簇头节点,使网络能量均匀消耗,延长了网络寿命。潘巨龙等[7]对传感网的异构性表现形式、HSN 的体系结构和相关标准进行了概述。近三年的异构性研究则主要致力于利用添加高能节点的方式优化网络覆盖[8-10]和网络寿命[2]。

虽然现有研究结果已经成功应用于拓扑控制、成簇算法、路由协议等方面,对提高网络传输率、节约和平衡网络能耗、提高网络可靠性、延长网络寿命等起到了积极作用,但一方面这些研究并不针对密钥管理协议,另一方面它们均局限于节点能力异构,尤其是初始节点能量,缺乏对异构性随时间动态变化的考虑。这种局限性的存在,主要是由于节点能量异构是最易发现和测量的,其对密钥管理协议设计的影响也最容易量化。但它远远不是传感网异构性的全部。如何合理刻画和利用异构性已经成为了辅助传感网密钥管理协议设计与评测的一大重要课题。实际上,对异构性进行多维度细粒度刻画和建模,将有利于从不同的角度改进协议,提高性能,设计更贴近现实的评测场景,获得更合理的评测结果。

1　异构性

1.1　定义与分类

为了便于描述与理解,给出更广义的 HSN 定义及相关概念,并对传感网异构性进行了分类。

定义 1(异构性)　指在传感器节点、数据链路、网络协议、服务质量、部署环境等方面具有差异的特性。

定义 2(异构传感网)　指具有异构性的传感网。

定义 3(异构类 x)　指差异的类型,如能量异构,链路异构,位置异构,温度异构,计算能力异构等。

定义 4(异构值 v)　指不同节点在同一异构类上所呈现的不同参数值。如节点的能量异构值就等于当前节点的剩余能量。

定义 5(异构度 d)　指某一异构类的异构程度,在数值上等于该异构类呈现出的不同异构值数目。

定义 6(异构态)　指在某一时刻,网络呈现出的异构类及其异构值的状态,记为$\langle d_1x_1,\cdots,d_kx_m\rangle$,其中,$m$ 为网络中异构类的数目。$\forall i \le m, d_i$ 可以进一步表示为$(v_1\times n_1,\cdots,v_{d_i}\times n_{d_i})$,其中,$v_j(1\le j\le d_i)$为第 i 种异构类 x_i 的第 j 个异构值,$n_j(1\le j\le d_i)$ 为异构值为 v_j 的节点数目。

例 1:网络中有 3 个节点 s_1、s_2 和 s_3,其能量分别为 10 J、5 J、5 J,则该网络具有能量异构性,其能量异构类 x_1 的异构度为 2,节点 s_1 的能量异构值为 10 J,其他两个节点的能量异构值均为 5 J,网络异构态表示为$\langle 2x_1\rangle$ 或$\langle(10\times1,5\times2)x_1\rangle$,其中,$(10\times1,5\times2)$ 为 x_1 的异构态。可见,网络异构态是由多个异构类异构态构成的。

从节点的角度来说,异构类可细分为节点内部异构和外部环境异构。其中节点内部异构包括计算能力异构、通信能力异构、存储能力异构、安全能力异构、能量异构和基础协议异构;外部环境异构可以进一步细分为链路环境异构,地理位置异构和敌手攻击能力异构等。有时为了提高效率,会在传感网中人为引入异构,如引入能力较强的节点,用以负责耗能的复杂操作。称这种为达到某种目的而人为引入的可控异构为主观异构。与之不同,在部署的过程中及部署后,传感网节点内部及外部环境本身会存在非人为引入的差异,如电池电量消耗不均,部署地理位置不同,链路质量优劣差异等。随着时间的推移,这些差异还可能发生变化,从而产生新的异构类,同时旧的异构类也可能消亡。异构类之间相互影响,异构类的异构度可能扩大、缩小,甚至消失。这样的变化是客观存在的,且不以人的意志为转移,称这类无目的的随机不可控异构类为客观异构。主观异构主要存在于网络部署前期,通常是针对于某种应用需求而人为构造的。而客观异构却随网络的运行长期存在,且与应用需求无关。应当注意,对于无人值守的传感网来说,主观异构的可控性仅存在于网络初期,随后则演变为客观异节点内部异构还是外部环境异构,都可能随时间变构。事实上,不论是主观异构还是客观异构,节点内部异构还是外部环境异构,都可能随时间变化,也可能在网络整个生命周期中始终保持相同的异构状态。因此,从是否随网络运行发生变化的角度,异构类也可以划分为静态异构和动态异构。此外,多个异构类还可能相互组合,共同构成一种新的复合异构类。若一个异构类仅对应一项不可分割的简单网络参数、节点参数或者协议指标,则该异构类称为简单异构类。任何一个复合异构类总是可以进一步分解为若干简单异构类的组合。图 1 对上述异构类的分类进行了系统的总结说明。

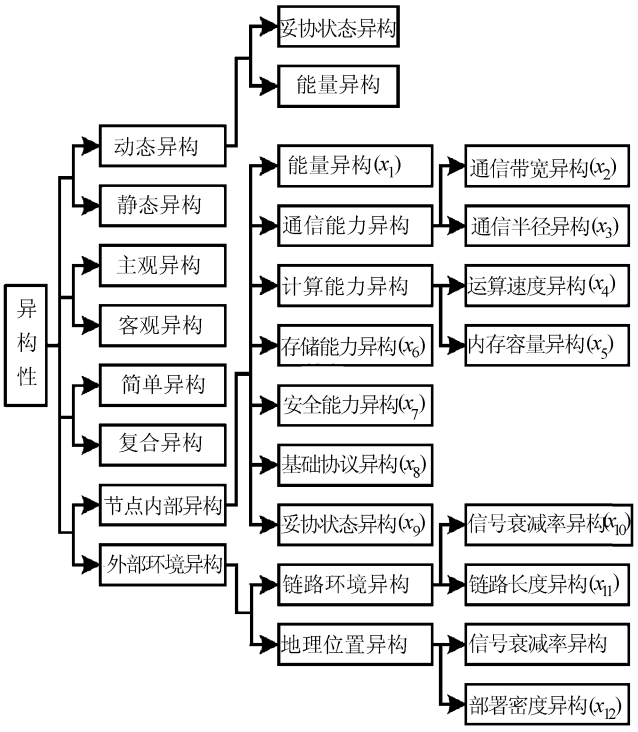


图1 异构类分类

Fig. 1 Classification of heterogeneities

本节定义是为后续刻画异构空间服务的,一方面在后续所提协议中用于根据异构值计算动态临界值,推动协议的进行;另一方面最终用于为性能分析提供异构环境的刻画,并结合第3.2和3.3节所提分析方法对异构环境下的全网连通概率和抗毁性进行恰当分析。

1.2 异构空间

提出一个异构空间模型,用以实现对异构类的多维度细粒度刻画。

定义7[11](拓扑) 设X为一个集合,T为X的一个子集族。如果T满足下列条件:

1) $X, \varnothing \in T$;

2) 若$A, B \in T$,则$A \cap B \in T$;

3) 若$T_1 \in T$,则$\cup_{A \in T_1} A \in T$,

则称T为X的一个拓扑。

定义8[11](拓扑空间) 若T是集合X的一个拓扑,则称(X,T)为一个拓扑空间,或称集合X是一个相对于拓扑T的拓扑空间。

定义9[11](基) 设(X,T)为一个拓扑空间,B为T的一个子族。若T中的每个元素都是B中某些元素的并,即对于每一个$U \in T$,存在$B_1 \in B$使得$U = \bigcup_{B \in B_1} B$,则称$B$为拓扑$T$的一个基,或称$B$为拓扑空间$X$的一个基。

定义10(异构空间) 设(X,T)为一个拓扑空间,B是拓扑T的一个可数基,若T的每一个元素都代表一种异构类,$\varnothing$表示同构,则称(X,T)为一个异构空间。

例2:假设网络中有4种简单异构类:能量异构x_1,通信带宽异构x_2,通信半径异构x_3和计算速度异构x_4。异构类集合$X = \{x_1, x_2, x_3, x_4\}$。则根据定义7有$T = \{\varnothing, \{x_1\}, \{x_2\}, \{x_1, x_2\}, \{x_3, x_4\}, \{x_1, x_3, x_4\}, \{x_2, x_3, x_4\}, \{x_1, x_2, x_3, x_4\}\}$为$X$的一个拓扑,则$(X,T)$构成一个异构空间,而$B = \{\varnothing, \{x_1\}, \{x_2\}, \{x_3, x_4\}\}$为该异构空间$(X,T)$的一个可数基。该异构空间中的异构类既有简单异构类(如x_1),也有复合异构类(如$\{x_3, x_4\}$)。

定义11(派生和反派生) 设有异构空间(X,T),$\forall x_i \in T$,$\exists x_1, x_2, \cdots, x_n \in T$,使得$x_i = \{x_1, \cdots, x_n\}$成立,则称异构类$x_i$可以由其它异构类$x_1, x_2, \cdots, x_n$共同派生。其逆向过程称为反派生。

派生的结果将产生复合异构类。但复合异构类不一定全由简单异构类组成,还可能包括了低级别的其他复合异构类。

定义12(极小基下的坐标) 设有异构空间(X,T),T的一个基$B = \{\varnothing, \{x_1\}, \cdots, \{x_n\}\}$,则此异构空间下任意一个异构类和任何一种异构态都可以表示为$\langle k_1x_1, k_2x_2, \cdots, k_nx_n\rangle$的形式。如果$B$中任何一个异构类不能再进一步反派生为其他异构类的并,则称这组基为极小基或极大无关基,称$(k_1, k_2, \cdots, k_n)$为异构类在这组基下的坐标。

利用坐标来表示异构类和异构态的方式有所不同。对于异构类来说,只需要表示为基的组合,而异构状态则需要刻画异构度或者异构值。故约定令$k_i = -1$表示该异构类为新异构类的组成成分之一;$k_i = 0$表示不含该异构类或异构度为0;$k_i > 0$表示异构度,此时的坐标称为异构度坐标;$k_i = (v \times n)$表示具体的异构值与节点数的乘积,此时的坐标称为异构值坐标。

定义13(维度) 如果$B = \{\{x_1\}, \cdots, \{x_n\}\}$为异构空间$(X,T)$的极大无关基,称$\dim(H) = \mathrm{rank}(B) = n$为异构空间$(X,T)$的维度。

例3:设网络W的异构空间维度为3,极小基$B = \{\{x_1\}, \{x_2\}, \{x_3\}\}$,且节点异构仅由$x_1$、$x_2$、$x_3$共同派生。$W$中共有3个节点$s_1$、$s_2$和$s_3$,其能量分别为10、5和5 J,通信半径分别为20、30和40 m,其他参数相同。则网络异构态可以表示为$\langle(10 \times 1, 5 \times 2)x_1, (20 \times 1, 30 \times 1, 40 \times 1)x_3\rangle$或$\langle 2x_1, 0x_2, 3x_3\rangle$,节点异构类则表示为$\langle -1x_1, -1x_2, -1x_3\rangle$,

其异构态就是网络异构态。

1.3　异构类关系

在异构空间中,各种异构类之间存在 2 种关系——派生和并列,这使整个空间像网一样展开。派生关系决定了高级复合异构类由哪些低级复合异构类或简单异构类组成。由于派生关系的存在,任何异构性都可以首先退化为简单异构性,再进行相关性能分析。显然,派生的异构类会受到其组成异构类的制约,如布撒在洼地或山林里的节点可能通信受阻,链路质量较低,而布撒在开阔地界上的节点则通信畅通,链路质量较高,故链路质量异构若可以反派生为通信带宽异构,部署位置异构等,并随着其组成异构类的变化而变化。除了派生关系以外,异构性之间还存在并列关系。并列关系是指异构性之间的彼此独立关系,即 A 的变化不对 B 产生影响,但它们可能同时与 C 存在派生关系。

1.4　动态异构类的变化趋势

随着网络的运行,主观异构不断发生变化,最终转变为客观异构。如高级节点因为处理复杂的操作而大量耗费能量,与执行低能耗操作的普通节点的能量差距逐渐减小,甚至低于普通节点,这使得人为引入的高能节点可能无法继续产生积极作用,反而可能随着协议的持续运行,快速死亡。可见,虽然主观异构能够在理想的静态网络中带来优势,但由于缺少对动态异构类在整个网络运行周期中的长期作用情况的研究,无法合理预测网络运行趋势,更无法为协议的设计与改进提供契合现实的模型。这也是致力于划分和刻画异构性,研究动态异构类随机变化对协议产生何种长期影响的根本原因。

假定网络中共有 N 个节点,网络的异构空间为 (X,T),极小基为 $B = \{\varnothing,\{x_1\},\cdots,\{x_p\}\}$。在初始时刻,网络的各种简单异构性相互独立存在。随着时间的推进,由于信息的收发量,电池电量的减少量,受外界环境的影响等的差异,异构类的异构态将越来越复杂。当所有节点都呈现出不同异构值时,其异构度达到峰值 N。当某些节点出现死亡或撤销,网络规模开始减小,异构度又随之降低。可见,网络中动态异构类的异构状态是在不断的发生随机波动的。

假定 $N(t)$ 为一个计数过程,表示到时刻 t 为止已经发生的波动次数,且 $N(0) = 0$。单位时间内发生波动事件的次数服从参数为 λ 的泊松分布,则在时间区间$[s,s+t]$ 内发生 i 次波动的概率为:

$$\Pr(N(t+s) - N(s) = i) = (\lambda t)^i e^{-\lambda t}/i! \quad (1)$$

令 $s = 0$ 容易得到至时刻 t 已经发生 i 次波动的概率为:

$$\Pr(N(t) = i) = (\lambda t)^i e^{-\lambda t}/i! \quad (2)$$

异构类的波动有 2 种情况,一是单调波动的,如无能量补给的节点,其能量波动呈现递减趋势;二是伯努利正负向波动,即对应异构值要么升高若干个单位,要么降低若干个单位,且每次波动都是独立无记忆的(之后的波动与过去的波动无关)。

对于单调波动,由式(2)可知,到时刻 t 波动总次数的期望为:

$$C(t) = \sum_{i=1}^{\infty} i \times p(N(t) = i) = \lambda t \quad (3)$$

对于伯努利正负波动,其波动规律服从 2 项分布,令 p 是正向波动的概率,$q = 1 - p$ 是反向波动的概率,则在 t 时刻,已发生的 i 次波动中有 x 次正向波动的概率为:

$$k_i(x) = \binom{i}{x} p^x q^{i-x} \quad (4)$$

故对于发生伯努利波动的异构类,在时刻 t 整体波动(正向)总次数的期望为:

$$C(t) = \sum_{i=1}^{\infty} \left(\left[\sum_{j=0}^{i} (2j - i) \times k_i(j) \right] \times \Pr(N(t) = i) \right) \quad (5)$$

2　动态多阶段随机密钥预分配

2.1　协议内容

对于以 EG[12] 方案为基础的若干随机密钥管理协议[13-15]来说,资源受限的节点均匀部署在网络中,以固定的通信半径彼此通信。事实上,大范围通信确实能够减少信息通信的跳数,增加直接密钥建立概率,但需要消耗大量的能量用于信号放大和抵抗路径损耗。倘若能够在保证网络连通概率的条件下,动态调整节点的通信半径,则可以在减少跳数和降低放大能耗之间寻求平衡,延长网络寿命。另一方面,对于多阶段部署的网络来说,节点在不同的阶段先后部署到网络中,节点密度增大,即使缩小节点的通信半径,也能够保持一定的全网连通概率。基于这样的思想本节提出一个动态的多阶段随机密钥预分配协议,该协议在通过引入动态半径异构和动态密钥环规模异构来在延长网络寿命的同时,将网络连通率保持在一个可接受的范围内。协议的具体内容如下:

1)初始化:在第一个部署期 DP_1,基站产生一个容量为 M 的密钥池 $KP_1 = \{(k_i,id_{ki}) \mid i \in [1,M]\}$,其中,$k_i$ 为第 i 个密钥,id_{ki} 为 k_i 的唯一标识。每个预

部署的节点 u 都分配一个全局唯一标识 id_u,设定其初始通信半径 r_u 为最大通信半径 $r_{\max}$,并从 $KP_i(i \geq 1)$ 中随机选取 m_1 个不重复密钥构成密钥环 KC_u,加载密钥材料 $\{id_u, cnt_u, KC_u\}$ 到节点 u 中。其中,cnt_u 是阶段计数器,初始为1。

2)初次直接密钥建立:令 u 和 v 为2个在彼此通信范围以内,欲建立共享密钥的节点。二者的通信半径分别为 r_u 和 r_v。初次直接密钥建立过程如下:

① 节点 v,u 分别广播 hello 消息,$Hello = \{id_v, cnt_v, nonce_v, KCidList_v\}$,$Hello = \{id_u, cnt_u, nonce_u, KCidList_u\}$,包含节点标识、阶段计数器 cnt、随机 $nonce$ 和密钥环 ID 列表 $KCidList$。

② 令 u 与 v 的共享密钥总数为 Q。当节点 u 接收到 v 的消息,它首先检查该信息中的计数器是否与自己的一致。如果 $cnt_v > cnt_u$,则令 $cnt_u = cnt_v$,并对密钥链中密钥进行哈希运算 $k_i = H^{cnt_v - cnt_u}(k_i)$,使得二者的计数器相等。如果 $cnt_u \geq cnt_v$ 且 $id_u < id_v$,则 ID 较小的节点 u 随机选择 $1 \leq q \leq Q$ 个共享密钥组成集合 $S = \{k_1, k_2, \cdots, k_q\}$,对应的密钥 ID 几何为 $S_{id} = \{id_{k1}, id_{k2}, \cdots, id_q\}$。最后,计算所有共享密钥的异或 $k = k_1 \oplus k_2 \oplus \cdots \oplus k_Q$。以该结果为密钥加密标识集合 S_{id},即 $E_k(S_{id})$,发送给节点 v。

③ 节点 v 通过接收 u 发送的 hello 消息计算 k,并在接收到 $E_k(S_{id})$ 之后,解密得到本次密钥建立所选择的共享密钥材料标识集合 S_{id},从而得到密钥集合 S。

④ 最后,双方利用随机 nonce 和单项累加器[16] $f(x,y)$ 生成共享密钥:

$$k_{u,v} = H(f(id_u \oplus id_v, S) \oplus nonce_u \oplus nonce_v),$$

$$k_{v,u} = H(f(id_v \oplus id_u, S) \oplus nonce_v \oplus nonce_u)。$$

其中,单项累加器具有累加集合元素可交换性,即如果有 $Y = \{y_1, y_2\}$,则 $f(x,Y) = f(f(x,y_1),y_2) = f(f(x,y_2),y_1)$。

3)通信半径 r 与密钥环规模 m 异构的多阶段动态部署:令 n_i 表示在 $DP_i(i \geq 1)$ 中部署的节点数目,有 $\sum n_i = N$。在第 i 个部署期 $DP_i(i \geq 1)$,基站更新密钥池为 $KP_i = \{(H^{i-1}(k_i), id_{ki}) \mid i \in [1, M]\}$。监测节点能量。若节点的平均能量较上一次测试时下降幅度 $\overline{E}_{DP_{i-1}} - \overline{E}_{DP_i} < \theta$,则记录 $\overline{E}_{DP_i} = \overline{E}_{DP_{i-1}}$,并根据步骤1)从 KP_i 中为欲部署的 n_i 个节点加载密钥材料,保持密钥环规模和通信半径与上一部署期 DP_{i-1} 相同,即 $m_i = m_{i-1}$,$r_i = r_{i-1}$。否则记录 $\overline{E}_{DP_i}$,并更新节点通信半径和新部署节点的密钥环规模,具体方法是:

① 计算欲缩减到的节点半径 $r = r_{i-1} - rstep$($rstep$ 为半径缩减步长),新密钥环规模 $m = m_{i-1} + mstep$($mstep$ 为密钥环增长步长),以及在 DP_i 中部署完 n_i 个节点后的平均密度 $\bar{\rho} = N/A$ 和平均密钥环规模 $\overline{m} = \sum_{j=1}^{i} m_j n_j / N$。

② 由于密钥管理协议必须保证一定的密钥连通概率,节点通信半径不能盲目的削减并靠密钥环规模的扩大来补偿,因为新补偿节点的邻居节点数目和作用范围是有限的,其补偿效果也是有限的。故在确定当前部署期的节点通信半径和新节点密钥环规模时,应当检查削减半径后是否能够将连通概率维持在可接受范围内,并称在当前部署期状态下使得连通概率刚好维持在可接受范围下界的节点通信半径为通信半径临界值,记为 $r_{\min}$。计算 $r_{\min}$(计算方法见2.2节)。若 $r > r_{\min}$,更新 $m_i = m$,$r_i = r$;否则 $m_i = m_{i-1}$,$r_i = r_{i-1}$。

③ 根据步骤1)从 KP_i 中为预部署的 n_i 个节点加载密钥材料,其中密钥环规模为 m_i,设定通信半径为 r_i。

④ 基站通过安全信道广播动态更新通知,收到的节点重新调整自己的通信半径为 $r_i = r_{i-1} - rstep$。最后,将新节点均匀部署于网络中。

2.2 动态临界值计算

根据文献[12,15]和随机图理论可知,由 n 个节点组成的承载随机密钥管理协议的网络可以看做一个以概率 Pc 连通的随机图 $G(n,p)$,其中任意2点间以 $p = (\ln(n) + c)/n$ 的概率存在链路。则容易得到节点度期望:

$$d = p \times (n-1) = \frac{(n-1) \times (\ln(n) - \ln(-\ln(Pc)))}{n} \tag{6}$$

两邻居节点共享密钥(或具有安全链路)的概率:

$$p' = 1 - \frac{\binom{M-m}{m}}{\binom{M}{m}} \approx 1 - \frac{(1-m/M)^{2(M-m+0.5)}}{(1-2m/M)^{(M-2m+0.5)}} \tag{7}$$

其中,M 和 m 分别为密钥池和密钥环规模。此时,任意节点的度期望为 $d' = p' \times (n'-1)$,n' 为邻居节点数目。由于 $d' = d$,故可以得到邻居节点数目与全网连通概率的关系满足:

$$p' \times (n'-1) = (n-1) \times (\ln(n) - \ln(-\ln(Pc)))/n \tag{8}$$

令网络平均节点部署密度为 ρ,$Pc_{\min}$ 表示应用需求所要求的最小全网连通概率,$n_{\min}'$ 为邻居节点数目阈值。则节点通信半径的阈值为:

$$r_{\min} = \sqrt{(n_{\min}' + 1)/\pi\rho} \tag{9}$$

其中,

$$n_{\min}' = \frac{(n-1) \times (\ln(n) - \ln(-\ln(Pc_{\min})))}{np'} + 1 \tag{10}$$

根据式(7)、(9)和(10)就可以在确定密钥池、密钥环和网络规模,平均密度和最小全网连通概率的基础上,得到节点通信半径的最小临界值。对于动态的密钥环规模,该通信半径临界值也是动态的。

3　性能分析

3.1　网络假设

为了准确的评测所提协议的有效性,后续将在分析所提协议其各项性能的同时,将之与同类型的典型协议 EG[12]、q-composite[18] 和 MPDKE[15] 进行对比。上述协议涉及的相关参数和模型假设如下:

1)基础参数设定

设整个监测区域总面积 $A = 100\ 000\ m^2$,密钥池规模 $M = 10\ 000$。选择 Crossbow 公司的 MICAz 节点(ATmega128 L,2.4 GHz,传输速率 250 kbps,存储器 512 k 字节)作为网络组成节点。设定节点最大通信半径 $r_{\max} = 30$ m,初始阶段在监测区域内分布式均匀部署 $n_0 = 1\ 000$ 个节点。当全网平均能量下降值超过阈值 $\theta = 100$ J 时,所提协议触发下一个部署期。

2)能耗模型

表 1 给出了信号路径传输时涉及的参数,其值均来自文献[17]。不难发现,当一只普通 AA 电池的能量约为 $1.5 \times 2.5 \times 3\ 600 = 13\ 500$ J 时,一个由 2 节 AA 电池供电的 MICAz 节点所拥有能量能够达到 27 000 J。根据文献[17]所述能耗模型,将 1 Byte 数据传输 d 米远的总能耗为:

$$e = e_{te} + e_{ta}d^{\alpha} \tag{11}$$

表 1　相关参数

Tab. 1　Parameters

参数	值/(μJ · Byte^{-1})	说明
e_{te}	8.528	发送电路能耗
e_{re}	4.424	接收电路能耗
e_{ta}	0.001 527	放大器能耗
电池电压	1.5	电压/V
电池容量	2 500	容量/mAH
α	2.5	路径损益指数

3)异构空间模型

由于网络中先后部署的节点均是 MICAz 节点,故它们在存储能力、计算能力、和安全能力上不存在差异。这也使得异构网络场景有别于以往的以分级节点来构造的异构传感网。随着时间推进,节点会因为运行时间、执行操作的不同而导致剩余能量差异,从而存在能量异构性。随着攻击者攻击能力的积累,节点妥协数目非均匀变化,网络妥协状态也会呈现动态异构。另一方面,对于所提协议,虽然网络初始时节点是均匀部署的,后续部署节点对同一部署期的节点来说也是均匀部署的,但前一部署期的节点却会因为新节点的加入而打破整体上的均匀状态,产生部署密度异构的结果。此外,为了保证密钥连通概率,延长网络寿命,所提方案还人为引入了通信半径异构和密钥环规模异构。其中密钥环异构属于同一协议在不同节点上呈现的参数异构,因此将之归为基础协议异构一类。

综上所述,MPDKE 方案较 EG 和 q-composite 方案多引入了主观密度异构,所提方案又可看做是 MPDKE 方案在加入半径和密钥材料异构性的基础上进行的改进。为了更直观地刻画网络的异构情况,设动态异构类的变化每次仅波动一个单位的异构值,半径的削减步长为 1 m。依据图 1,所提方案的网络异构空间 (X, T_1) 的极小基 $B_1 = \{\varnothing, \{x_1\}, \{x_3\}, \{x_8\}, \{x_9\}, \{x_{12}\}\}$,MPDKE 方案的网络异构空间 (X, T_2) 的极小基 $B_2 = \{\varnothing, \{x_1\}, \{x_9\}, \{x_{12}\}\}$,而 EG 方案和 q-composite 方案的网络异构空间 (X, T_3) 的极小基均为 $B_3 = \{\varnothing, \{x_1\}, \{x_9\}\}$。令 1 表示妥协状态,0 表示为未妥协状态,上述各异构空间所包含的异构性的初始异构态设定为:

$$st_1 = \langle 27\ 000\ \text{J} \times n_0)x_1\rangle,$$
$$st_3 = \langle (r_{\max} \times n_0)x_3\rangle,$$
$$st_8 = \langle (200 \times n_0)x_8\rangle,$$
$$st_9 = \langle (0 \times (n_0 - 1), 1 \times 1)x_9\rangle,$$
$$st_{12} = \langle ((\pi r_{\max}^2 n_0/A - 1) \times n_0)x_{12}\rangle。$$

其中,x_1 随消息发送次数的增加将按照式(11)所示能耗模型消耗能量。在任意一个部署期中,节点能量在无补给的条件下是单调递减的,即服从 1.4 节所述单调波动。在 t 时刻,任一节点的能量波动值期望满足式(3)。x_3,x_4 根据变化步长、阈值 θ 和能量下降梯度动态变化。x_9 随攻击者获得的有效妥协节点数目的变化而变化,符合1.4节所述伯努利波动。x_{12} 在每个部署期变化一次,平均密度呈增长趋势。

3.2 全网连通概率

根据上节所述异构空间模型,令节点初始能量为 E_0,则在部署期 DP_i 部署的节点到 t 时刻的能量 $E_t^i = E_0 - C(t') \approx E_0 - \lambda(t - (i-1) \times d_{DP})$。全网平均能量为:

$$\overline{E_t} = \sum_{j=1}^{i} n_j E_t^j / \sum_{j=1}^{i} n_j \tag{12}$$

$\overline{E_t}$ 每降低1个梯度,节点通信半径调整为 $r_t = r_{t-1} - rstep \geq r_{\min}$。此时节点邻居数为:

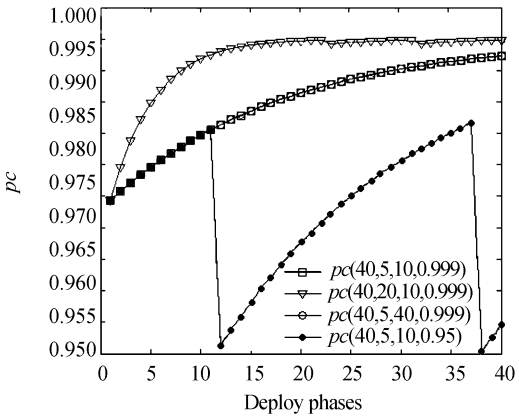
$$n_t' = \pi r_t^2 \overline{\rho} - 1 \tag{13}$$

根据式(7)可以得到所提方案在 (X, T_1) 下的实时连通概率:

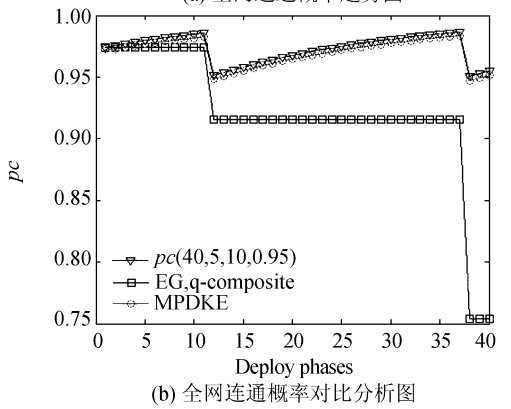
$$Pc_t = \exp\left(-\exp\left(\ln N - \frac{(n_t' - 1)Np'}{N-1}\right)\right) \tag{14}$$

图2(a)展示了在40个部署期中,所提方案在不同参数 $pc(DP, nadd, mstep, pcmin)$ 下的全网连通概率变化情况。其中,DP 表示部署期数目,$nadd$ 表示后续每个部署期的节点部署量,$mstep$ 表示节点密钥环的增长步长,$pcmin$ 表示要维持的最小全网连通概率。从图中可见,由于新部署节点数量相对全网节点数目来说非常少,因此密钥环增长步长对全网密钥连通概率的影响最小,此时增加部署量和改变最小连通概率则会产生明显影响。对于前3条曲线来说,初始全网连通概率均无法达到最小连通概率需求,因此每个部署期都会在保持通讯半径不变的基础上持续扩大密钥环规模。直到节点半径降低一个梯度的结果不会使全网连通概率重新低于最小阈值时,才将节点半径缩减一个梯度,此时全网连通概率将发生跃变,这也解释了 $pc(40,5,10,0.999)$ 和 $pc(40,5,10,0.95)$ 2条曲线的跃变点发生原因。

图2(b)以跃变最明显的 $pc(40,5,10,0.95)$ 为例,在3.1节所述异构网络下,与采用不同异构空间模型的其余3个方案[12,15,18]进行了对比分析。可以发现,所提方案通过人为控制通信半径和密钥材料异构性,使得连通概率一旦达到阈值则始终保持在阈值之上的范围内自主调整通信范围,以节省能量。MPKDE方案和EG方案均不能动态适应能量变化,在同等通信半径条件下,前者的连通概率略低于所提方案,后者则对半径变化十分敏感。如果随所提方案同步削减通信半径,则EG的连通概率下降迅速;若保持固定的通信半径,EG和MPKDE均需要耗费额外的传输代价来维持更大的通信范围,降低了网络寿命。



(a) 全网连通概率趋势图



(b) 全网连通概率对比分析图

图2 全网连通概率分析

Fig. 2 Overall network connectivity

3.3 抗毁性

敌手攻击能力与攻击者获得的有效妥协节点数目成正比。一个妥协节点对攻击者来说是有效的当且仅当其妥协状态没有被检测到。一旦妥协节点被检测出来,将被立刻从网络中删除。例如全网有5个节点,网络妥协状态异构态为 $(1 \times 1, 0 \times 4)x_9$,此时网络中有效妥协节点比例为1/5。若下一时刻,又有一个未妥协节点被妥协,则网络妥协状态异构态变为 $(1 \times 2, 0 \times 3)x_9$,有效妥协节点比例上升为2/5。若随后有一个妥协节点被检测到并被删除,此时网络妥协状态异构态改变为 $(1 \times 1, 0 \times 3)x_9$,有效妥协节点比例下降到1/4。可见,在一段时间内,敌手的攻击能力可能随妥协节点数目的增多正向波动数个单位级,又可能在某一时刻由于妥协节点失效而负向波动,妥协节点数目服从伯努利分布,使得密钥管理协议的实时抗毁性也随之变化。

对于妥协状态异构,根据式(4)可知,若至第 t 个部署期已发生了 i 次波动,其中 x 次正向波动(相当于妥协了 x 个节点),则有 $i-x$ 次负向波动(相当于有 $i-x$ 个妥协节点被删除),此时全网节点的实时数目 $N_t = N - (i-x)$ 个,实时有效妥协节点数目

$x_t = x - (i - x) = 2x - i \geq 0$。故在 DP_t,有效妥协节点数目为:

$$C(t) = \sum_{i=1}^{\infty} \left(\left[\sum_{x=0.5i}^{i} (2x - i) \times k_i(x) \right] \times p(N(t) = i) \right) \tag{15}$$

由于每一个新的部署期,新、旧节点的密钥均会通过哈希操作进行更新,而哈希运算具有单向性,因此即使攻击者捕获了一组节点,获得了其密钥环中全部密钥,也仅能对在之后的部署期对利用这些密钥建立链路密钥的节点产生影响,而不能攻破之前部署期建立的链路密钥。例如,假设攻击者在部署期 DP_a 捕获了在 $DP_b(b \leq a)$ 中部署的节点 u,能够获得密钥材料 $H^{a-1}(k_1), H^{a-1}(k_2), \cdots, H^{a-1}(k_l)$,则攻击者仅能继续更新得到后续密钥材料 $H^c(k_1), H^c(k_2), \cdots, H^c(k_l), c > a$,以及用这些密钥材料建立的链路密钥,而对于使用 $H^d(k_1), H^d(k_2), \cdots, H^d(k_l), 0 \leq d \leq a-2$,建立的链路密钥则无法攻破。考虑两个在部署期 DP_i 建立链路密钥的未妥协节点 u 和 v,当共有 $C(i)$ 个节点在部署期 DP_i 之前(包括 DP_i)妥协,由于攻击者并知道 $k_{u,v}$ 到底选择了几个共享密钥来构建链路密钥,则 $k_{u,v}$ 暴露的概率为:

$$P_i^r = \sum_{j=1}^{m_i} \left(1 - \left(1 - \frac{m_i}{M} \right)^{C(i)} \right)^j \frac{p_i(j)}{\sum_{k=1}^{m_i} p_i(k)} \tag{16}$$

其中,m_i 为部署期 DP_i 的密钥环规模,$p_i(j)$ 表示两节点恰好有 j 个共享密钥的概率,且

$$p_i(j) = \binom{M}{j} \binom{M-j}{2(m_i - j)} \binom{2(m_i - j)}{m_i - j} \Big/ \binom{M}{m_i}^2 \tag{17}$$

可见,所提方案的链路密钥妥协概率仅与其建立期和建立期之前妥协节点数目相关。从全网的角度来看,在 $DP_i(1 \leq i \leq L)$,欲部署新节点 n_i 个,平均邻居数目 d_i,两邻居节点共享密钥的概率 p_i^s,则所提方案在 (X, T_1) 下的抗毁性可以表示为任一未妥协链路妥协的概率,即:

$$P_{\text{resistent}} = \frac{\sum_{i=1}^{L} n_i d_i p_i^s p_i^r}{\sum_{i=1}^{L} n_i d_i p_i^s} \tag{18}$$

图 3 展示了相应异构空间下经典 EG 方案[12]、q-Composite 方案[18]、MPDKE 方案[15]与所提方案的抗毁性对比情况。所提方案的部署期设定为 4 个,每个部署期被妥协节点均匀,即若共捕获 20 个节点,则每个部署期部署 5 个。q-Composite 方案的参数 q 设定为 2。实际上,所提方案的密钥数目选择过程可以看做 q-Composite 方案的 $q = 1$ 的特例,即至少共享 1 个密钥的两节点可建立共享密钥,且二者自主选择大于等于 1 个预加载密钥进行链路密钥建立。即使所提方案比 q-Composite 的约束条件更为宽泛,仍然能够获得略优于 q-Composite,明显优于 EG 和 MPDKE 方案的网络抗毁性。

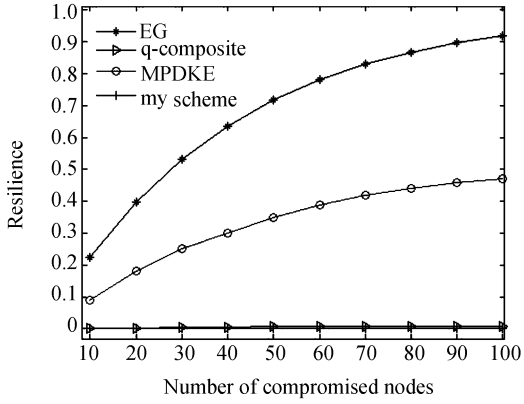


图 3　抗毁性对比

Fig. 3　Resilience comparison

3.4　寿　命

借助 OMNET + + 平台,模拟不同异构空间,对上述各协议的寿命进行了定量分析。根据 3.1 节所述参数和模型在 OMNET + + 中建立起测试网络并运行。

在测试过程中,只需考虑协议的运行方式和 MICAz 节点的性能参数。仿真过程中,采取以固定的时间间隔重复执行密钥建立过程的方式来实现寿命测试。所选取的测试时间间隔分别为 1 s、1 min 和 10 min,得到了如表 2 所示的测试结果,单位:d。从表中容易看出,在保持全网连通概率始终大于 0.95 的条件下,改进协议的寿命较其他 3 项方案明显增长。

表 2　寿命仿真结果

Tab. 2　Lifetime simulation results

更新间隔	EG	q-Composite	MPDKE	所提方案
1 s	3.4	2.7	2.1	23
1 min	201.4	164.1	158.2	1369
10 min	2 013.6	1 641.5	1 585.4	13 694

4　结　论

深入探讨了异构传感网的异构性及其应用问题,主要贡献有:

1)给出了异构性的广义定义,详细划分了传感网异构性种类,解释了传感网中都有哪些异构类的问题;

2)提出了异构空间模型,为网络异构类构成,异构类之间的关系以及异构状态的描述提供了清晰的刻画手段,解决了如何刻画异构类及其相互关系的问题;

3)总结了动态异构类随时间的变化趋势,为评测异构环境下的协议长期性能提供了必要的技术手段;

4)通过合理利用通信半径和密钥材料异构性,提出了能量有效的密钥管理方案,为如何利用异构性来辅助传感网密钥管理协议设计与评测提供了参考和示例。

在后续研究中,将进一步研究综合利用其它异构性实现密钥管理协议的最优配置问题。

参考文献:

[1]Lee C, Eun D Y. Exploiting heterogeneity to prolong the lifetime of large-scale wireless sensor networks[C]//Proceedings of ICC 2011. New Jersey, USA: IEEE Computer Society, 2011: 1 - 5.

[2]Soni S, Katiyar V. Prolonging the lifetime of wireless sensor networks using multi-level clustering and heterogeneity [C]//Proceedings of SEPADS'11. Athens, Greece: World Scientific and Engineering Academy and Society, 2011: 72 - 77.

[3]Mache J, Chieh-Yih W, Yarvis M. Exploiting Heterogeneity for Sensor Network Security[C]//Proceedings of SECON'08. New Jersey, USA: IEEE Computer Society, 2008: 591 - 593.

[4]Yarvis M, Kushalnagar N, Singh H, et al. Exploiting heterogeneity in sensor networks[C]//Proceedings of INFOCOM'05. New Jersey, USA: IEEE Computer Society, 2005: 878 - 890.

[5]Mhatre V P, Rosenberg C, Kofman D, et al. A minimum cost heterogeneous sensor network with a lifetime constraint[J]. IEEE Transactions on Mobile Computing, 2005, 4(1): 4 - 14.

[6]Qing Li, Zhu Qingxin, Wang Mingwen. A distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks[J]. Journal of Software, 2006, 17(3): 481 - 489. [卿利,朱清新,王明文. 异构传感器网络的分布式能量有效成簇算法[J]. 软件学报, 2006, 17(3): 481 - 489.]

[7]Pan Julong, Wen Yu. A study of heterogeneity in wireless sensor networks[J]. Aeronautical Computing Technique, 2007, 37(2): 124 - 130. [潘巨龙,闻育. 无线传感器网络的异构性研究[J]. 航空计算技术, 2007, 37(2): 124 - 130.]

[8]Aderohunmu F, Deng J D, Purvis M. Optimization of energy-efficient protocols with energy heterogeneity for coverage preservation in wireless sensor networks: An empirical study[C]//Proceedings of HPCC-ICESS 2012. Washington DC, United States: IEEE Computer Society, 2012: 1173 - 1178.

[9]Ammari H M. Joint mobility and heterogeneity for connected k-coverage in sparsely deployed wireless sensor nets[C]//Proceedings of 7th International Conference on Wireless Algorithms, Systems, and Applications. Heidelberg, Germany: Springer Verlag, 2012: 258 - 271.

[10]Li Ming. K-coverage node scheduling algorithm for heterogeneous sensor networks under non-uniform distribution [J]. Journal of Huazhong University of Science and Technology, 2013, 41(6): 61 - 64. [李明. 非均匀分布的异构传感器网络 K 覆盖调度算法[J]. 华中科技大学学报, 2013, 41(6): 61 - 64.]

[11]熊金城. 点集拓扑讲义[M]. 北京:高等教育出版社, 2003: 1 - 198.

[12]Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks[C]//Proceedings of CCS'02. Washington DC, United States: Association for Computing Machinery, 2002: 41 - 47.

[13]Kur J, MatyášV, Švenda P. Two improvements of random key predistribution for wireless sensor networks[C]//Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2013. Heidelberg, Germany: Springer Verlag, 2013: 61 - 75.

[14]Miyaji A, Omote K. How to build random key pre-distribution schemes with self-healing for multiphase WSNs [C]//Proceedings of AINA 2013. New Jersey, USA: IEEE Computer Society, 2013: 205 - 212.

[15]Ashok Kumar Das. A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks[J]. International Journal of Information Security, 2012, 11(3): 189 - 211.

[16]Camenisch J, Kohlweiss M, Soriente C. An accumulator based on bilinear maps and efficient revocation for anonymous credentials[C]//Proceedings of 12th International Conference on Practice and Theory in Public Key Cryptograph. Heidelberg, Germany: Springer Verlag, 2009: 481 - 500.

[17]Haapola J, Shelby Z, Raez C P. Cross-layer energy analysis of multi-hop wireless sensor network[C]//Proceedings of EWSN 2005. New Jersey, USA: IEEE Computer Society, 2005: 33 - 44.

[18]Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks[C]//Proceedings of SECPRI 2003. Berkeley, CA, United states: Institute of Electrical and Electronics Engineers Inc, 2003: 197 - 213.

(编辑 杨 蓓)