

# 无线传感器网络中基于散列链的随机密钥预分发方案

苏 忠 林 闯 任丰原

(清华大学计算机科学与技术系 北京 100084)

**摘 要** 密钥管理是无线传感器网络安全机制和服务的基石,随机密钥预分发是当前最有效的密钥管理机制,但目前的随机密钥预分发方案存在一个潜在的挑战:无法同时获取理想的网络安全连通性和网络抗毁性.文中提出了一种基于散列链的随机密钥预分发方案,通过有效调节散列链长度、公共辅助节点数、散列链数量等参数,节点仅需预分发数量较少的密钥信息,就能够以较高的概率建立对偶密钥.而且,即使存在大量的受损节点仍能保持较强的网络抗毁性.理论分析和模拟实验证明了所提出方案的有效性和安全性.

**关键词** 散列链;对偶密钥;预分发;安全;无线传感器网络

中图法分类号 TP393 DOI号: 10.3724/SP.J.1016.2009.00030

## Hash Chain Based Random Keys Pre-Distribution Scheme in Wireless Sensor Networks

SU Zhong LIN Chuang REN Feng-Yuan

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084)

**Abstract** Key management is the cornerstones of many security mechanisms and services in wireless sensor networks. Random pre-distribution of secret key is one of the most practical schemes in such networks due to its instinct property. These schemes, however, face a challenging problem, that is, it can not acquire the high network connectivity probability and reach strong resilience against the nodes compromise simultaneously. To address this limitation, a hash chain based random key pre-distribution scheme is proposed in the paper. Nodes only need to preload a few of secret keys and can establish pair-wise keys amongst its neighboring nodes with high probability through tuning some system parameters, such as the length of hash chain, the number of common auxiliary nodes, the number of hash chain. Moreover, the proposed scheme can maintain strong security strength even though there are a lot of compromised nodes. The theoretical analysis and simulation experiments show that the proposed scheme performs well in terms of network connectivity and security strength.

**Keywords** hash chain; pair-wise key; pre-distribution; security; wireless sensor network

## 1 引 言

无线传感器网络(Wireless Sensor Networks,

WSN)一直被认为具有广泛的应用前景,能够部署在当前典型网络所不能及的环境,为当前的众多领域,如污染监测、环境和交通流量监控等提供前所未有的良好解决方案<sup>[1]</sup>.若 WSN 被部署在无人触及

甚至敌方控制的环境时,节点将面临着各种各样的攻击,很容易被俘获,导致其所包含的机密信息可能完全曝露给攻击者.因此,如何保证 WSN 安全是 WSN 研究领域里的一项极其重要内容.其中,最基本的一项研究内容是密钥管理,主要目的是为 WSN 里通信节点建立对偶密钥(pair-wise key),从而为网络提供安全的通信链路.有效的密钥管理能为其他安全机制或服务(如安全路由<sup>[2]</sup>、安全定位<sup>[3]</sup>、安全数据融合<sup>[4]</sup>等)提供最基本的技术支持.

通常情况下,WSN 由大量的资源严格受限的节点组成,例如 Mica2 mote<sup>[5]</sup>使用 8 位 7.3828MHz ATmega 128L 处理器,4KB SRAM 和 128KB ROM,通信频率为 916MHz,带宽为 10Kbps.非对称的密钥管理方案<sup>[6-7]</sup>由于节点的存储复杂度、计算、通信复杂度和能耗过高,目前普遍被认为不适用于 WSN.在对称密钥管理方案里,最简单的方案是全部节点使用同一个密钥.这样每个节点仅需保存一个密钥,其存储复杂度最小,但抗毁性(resilience against nodes compromise)最差,只要俘获任意一个节点就可获取所有节点的对偶密钥;另一类方案是使任意一对节点都拥有不同的对偶密钥,该方案的抗毁性最好,任何一个节点受损(compromised)都不会曝露其他节点的对偶密钥,但其存储复杂度为  $O(n)$  ( $n$  为网络节点总数),扩展性差,不适用于大规模的 WSN 网络.

已有的 WSN 对称密钥管理方案大致可以分为两种类型:确定密钥管理和随机密钥管理.确定密钥管理方案沿袭传统网络的密钥管理思想,为每一个节点与其他任何节点都建立独立的对偶密钥.但此类方案可能对节点的部署有特殊的要求<sup>[8]</sup>,或者节点存储复杂度通常较高<sup>[9]</sup>.而且,在 WSN 里,节点仅与其相邻的节点进行通信,因此没有必要为任何一对节点都建立对偶密钥.在随机密钥管理方案里,部署前节点以随机方式从密钥池里获取部分密钥组成密钥环,部署后相邻节点能以一定的概率共享公共密钥,使用这些公共密钥就可建立相邻节点之间的对偶密钥.与确定密钥管理方案相比,随机密钥管理方案虽不能确保任意两个相邻节点都能够直接建立密钥,但却有效降低了节点的存储复杂度、计算复杂度和通信复杂度,被认为最适用于 WSN<sup>[10-11]</sup>.

但是,目前已有的随机密钥管理方案无法保证同时获取较高的网络安全连通性和较强的抗毁性.这是因为,若提高安全连通概率,就必须提高节点预分发的密钥数,或降低密钥池的大小;然而,要加强

网络抗毁性,则必须减少节点预分发的密钥数,或提高密钥池大小.网络安全连通性和抗毁性之间的矛盾给 WSN 随机密钥管理研究带来了很大的技术挑战.

本文提出了一种基于散列链的随机密钥预分发方案,试图在网络安全连通性和网络抗毁性的之间取得理想的折衷.其基本设计思想是:整个 WSN 由大量的普通节点(sensor nodes)和少量的辅助节点(auxiliary nodes)组成.密钥池由一系列的长度相等的散列链构成,部署前普通节点随机预分发一小部分特殊密钥,而辅助节点从密钥池里随机选取一部分密钥;部署后,普通节点借助辅助节点广播的信息生成新的派生密钥,并且使用公共派生密钥与相邻普通节点建立对偶密钥.通过调节散列链的长度、散列链的数量、共享辅助节点数等参数,使得相邻普通节点仅需预分发少量的特殊密钥,就能以较高的概率建立对偶密钥,同时确保即使存在数量较多的受损节点情况下仍保持较强的网络抗毁性.此外,这些调节方法对于降低节点的存储复杂度是非常有效的,可以使得节点的存储复杂度与网络规模无关,使之适用于大规模的 WSN.理论分析和模拟实验结果表明,本文所提出的方案被证明能够获取较高的网络安全连通性,同时保持较强的网络抗毁性.

## 2 已有研究工作

PIKE<sup>[8]</sup>是一种确定性密钥预分发方案.根据网络的节点数  $N$ ,构造一个  $m \times m$  序号网格(grid),其中  $m = \lfloor \sqrt{N} \rfloor$ .节点按照网格的行列号编号.部署前,每一节点与同一行同一列,共  $2(\sqrt{N}-1)$  个节点建立对偶密钥,然后按顺序号进行部署.部署后同一行或列的节点直接拥有对偶密钥,不同行或列的节点则通过公共行列的可信节点建立对偶密钥.显然,PIKE 方案的节点存储复杂度为  $O(\sqrt{n})$ ,不适用于大规模网络,并且,其节点部署也有特殊要求.

Camtepe 等人<sup>[9]</sup>把组合设计理论(combinatorial design theory)用于设计 WSN 确定密钥预分发方案.假设网络的节点总数为  $N$ ,用  $n$  阶有限射影空间(finite projective plane) ( $n$  为满足  $n^2 + n + 1 \geq N$  的素数)生成一个参数为  $(n^2 + n + 1, n + 1, 1)$  的对称 BIBD(Balanced Incomplete Block Design),支持的网络节点数为  $n^2 + n + 1$ ,密钥池的大小为  $n^2 + n + 1$ ,能够生成  $n^2 + n + 1$  个大小为  $n + 1$  的密钥环,任意

两个密钥环至少存在 1 个公共密钥,并且每一密钥出现在  $n+1$  个密钥环里.可见,任意两个节点的安全连通概率为 1.但素数  $n$  不能支持任意的网络规模.例如,当  $N > n^2 + n + 1$  时, $n$  必须是下一个新的素数,而过大的素数则会导致密钥环急剧增大,超出节点的存储空间而不适用于 WSN.

Eschenauer 和 Gilgor<sup>[10]</sup> 在 WSN 里首先提出了随机密钥预分发方案(简称 Eschenauer 方案).在部署之前,节点从一个密钥数量为  $P$  的密钥池里随机选取  $k$  个密钥( $k \ll P$ );然后节点随机部署在特定区域里.部署后若两个相邻节点共享一个密钥就可以直接建立对偶密钥,否则,就需要通过中间节点建立对偶密钥.因此,其安全连通概率  $p$  可描述为<sup>[10]</sup>

$$p = 1 - \frac{((P-k)!)^2}{(P-2k)!P!}$$

从中可以看出,节点预分发一定数量的密钥,便可以特定概率建立对偶密钥.例如,当密钥池大小为 10000 时,每个节点预分发 200 个密钥(存储容量约为 1.6KB),安全连通概率就可达 98%.要提高安全连通概率,可提高  $k$  值(当  $P$  值固定),或者降低  $P$  值(当  $k$  值固定).

在该方案里,假如部分节点受损,则其所包含的密钥也必受损,当其他未受损的节点使用这些受损密钥建立对偶密钥时,则该链路被认为是受损的.当存在  $\alpha$  个受损节点时,未受损相邻节点之间的链路受损概率  $p_c$  可表示为  $p_c = 1 - \left(1 - \frac{k}{P}\right)^\alpha$ .由此可知,要降低链路受损概率  $p_c$ ,可降低  $k$  值(当  $P$  值固定),或提高  $P$  值(当  $k$  值固定).

根据上述分析,随机密钥预分发方案存在一个严重挑战,就是无论如何调整节点预分发的密钥数( $k$  值)或密钥池大小( $P$  值)不能同时满足获取高网络安全连通性和强网络抗毁性的需求.

Chan 等人<sup>[11]</sup> 认为提高共享密钥阈值能够加强网络抗毁性,故提出  $q$ -composite 方案对 Eschenauer 方案进行修改,把共享密钥阈值从 1 提高到  $q$ ,即两个相邻节点必须共享  $q$  个密钥才能建立对偶密钥,这样使得攻击者必须俘获更多的节点才能达到 Eschenauer 方案相同的通信链路受损概率,从而加强网络抗毁性.但是,在受损节点数量较大时, $q$ -composite 方案的抗毁性反而比 Eschenauer 方案差.

Traynor 等人<sup>[12]</sup> 提出了适用于异构 WSN 的随机密钥预分发方案.在该方案里,节点被分为能力较

强的和能力较弱的两种类型,能力较强的节点预分发大量密钥,而能力较弱的节点则预分发少量密钥.相邻节点(同构的或异构的)相互建立对偶密钥.该方案充分发挥能力强的节点的作用,降低了通信开销,并且能够达到较为理想的网络安全连通性.但是,能力较强的节点大量受损,对网络的安全连通性和抗毁性影响巨大.

有研究人员把节点地理位置信息<sup>[13]</sup>、部署知识<sup>[14]</sup> 应用到随机密钥预分发方案,这些方案虽然提高密钥分配的针对性,加强了网络抗毁性,但是,地理信息或部署知识已知是一个较为苛求的假设.

近年来,有研究人员把轻量级的非对称密钥机制(如 ECC<sup>[15-16]</sup>) 应用到 WSN,但其计算复杂度仅为毫秒级,仍远高于微秒级的对称密钥机制,因此其实用性较差.

### 3 相关知识

#### 3.1 系统假设

在本方案里,WSN 由大量的普通节点(sensor nodes)和少量的辅助节点(auxiliary nodes)组成.

普通节点的资源严格受限,包括其能量、存储容量、计算能力以及通信能力等,所有普通节点都是同构的.部署后普通节点仅能与处于其通信半径范围内的其他普通节点通信,通信使用全向天线,因此它们之间的通信链路是对称的.与之相比,辅助节点在能量、存储容量、计算能力和通信能力等方面要优于普通节点.辅助节点的主要作用就是在网络部署之后把所预分发的密钥发送给普通节点.每一个辅助节点都有一个唯一的标识,该标识为一个随机散列值.

所有普通节点和辅助节点都被随机部署在一个特定的区域里.图 1 是适用于本方案的 WSN 结构示意图.在特定的区域里有大量的普通节点和少量的辅助节点.虚圆线表示辅助节点的通信半径.

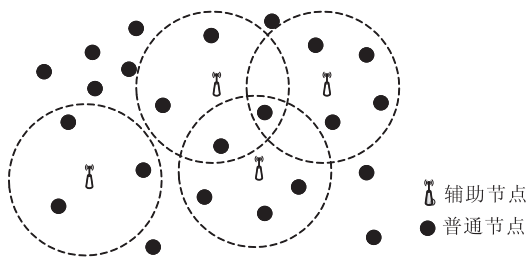


图 1 本方案的 WSN 结构示意图

在本方案里,假设攻击者的主要目的是破坏节

点之间的安全通信. 攻击者能够通过窃取通信信道或物理俘获等方式使得一定数量的普通节点或辅助节点受损, 若普通节点或辅助节点受损, 它们所携带的机密信息, 包括密钥、数据、代码等都随之曝露给攻击者. 攻击者可联合受损的普通节点或辅助节点对网络发起串谋攻击(collusion attack).

后面假设使辅助节点受损的难度要比普通节点的受损难度要大, 而且, 攻击者无法通过受损辅助节点来获取正常辅助节点的标识.

### 3.2 单向散列链

一个单向散列链是一个如下的散列值序列  $\{x_1, \dots, x_j, \dots, x_n\}$ , 满足  $\{x_j \mid \forall j: 1 \leq j \leq n, x_j = H(x_{j-1}, G)\}$ . 散列函数  $H$  满足以下属性: (1) 给定  $x_{j-1}$  和  $G$ , 很容易计算出  $x_j$ ; (2) 未给定  $G$ , 即使给定了  $x_{j-1}$  也很难计算出  $x_j$ ; 或未给定  $x_{j-1}$ , 即使给定了  $G$ , 也很难计算  $x_j$ .

在上述定义的散列链里, 如果要对一个给定的散列值  $x_j$  进行认证, 可以通过重复计算散列链, 然后与最后一个元素  $x_n$  之值进行比较.

在本方案里, 称  $G$  为生成因子, 散列链的最后一个元素  $x_n$  为 *commitment*. 显然, 每一个散列链仅有一个 *commitment*, 其他元素称为链密钥(chain key).

### 3.3 相关定义

为了便于本方案的讨论和分析, 特进行以下定义.

**定义 1.** 相邻普通节点(Neighboring Sensor Nodes). 两个普通节点  $u$  和  $v$ , 若它们之间的物理距离  $x$  小于其通信半径  $r$ , 即  $x < r$ , 则称它们为相邻普通节点. 如图 2 所示, 普通节点  $u$  和  $v$  是相邻普通节点.

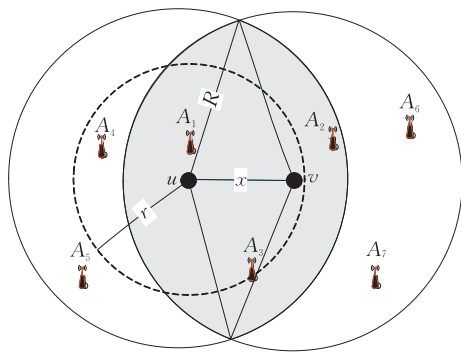


图 2 普通节点与辅助节点之间的相邻示意关系

**定义 2.** 相邻辅助节点(Neighboring Auxiliary Nodes). 如果一个普通节点  $u$  位于一个辅助节点  $A_w$  的通信半径范围  $R$  之内, 则称  $A_w$  为  $u$  的相邻辅

助节点. 类似地, 也称  $A_w$  有一个相邻普通节点  $u$ . 注意:  $A_w$  并不一定位于  $u$  的通信半径范围之内. 如图 2 所示, 辅助节点  $A_1$ 、 $A_4$  和  $A_5$  都是普通节点  $u$  的相邻辅助节点, 但  $A_5$  并不在  $u$  的通信半径范围之内.

**定义 3.** 辅助通信区域(Auxiliary Communication Area). 对于普通节点, 以该节点为中心, 辅助节点通信半径  $R$  为半径的区域, 称为该普通节点的辅助通信区域. 如图 2 所示的两个实线圆形, 分别为  $u$  和  $v$  的辅助通信区域. 该区域包含对应普通节点的所有相邻辅助节点.

**定义 4.** 公共散列链(Common Hash Chains). 对于普通节点  $u$  和辅助节点  $A_w$ , 若  $u$  从某一个散列链  $C_i$  提取了 *commitment<sub>i</sub>*, 同时  $A_w$  也从  $C_i$  提取一个或多个链密钥, 则称  $u$  和  $A_w$  共享一个公共散列链  $C_i$ . 类似地, 若两个普通节点都选取了 *commitment<sub>i</sub>*, 则称它们共享一个公共散列链  $C_i$ .

**定义 5.** 派生密钥(Derived Key). 普通节点使用接收到的链密钥以及对应的辅助节点标识所生成的密钥称为派生密钥.

**定义 6.** 受损散列链(Compromised Hash Chains). 若一个散列链的 *commitment* 被一个受损的普通节点所选取, 就称该散列链是受损的.

### 3.4 辅助节点的部署模型

辅助节点的密度决定相邻普通节点之间公共辅助节点的数量. 对于两个相邻普通节点, 若辅助节点位于它们公共辅助通信区域里, 该辅助节点就是这两个相邻普通节点的公共辅助节点. 如图 2 所示, 辅助节点  $A_1$ 、 $A_2$  和  $A_3$  是两个相邻普通节点  $u$  和  $v$  的公共辅助节点.

辅助节点的随机部署使用同构泊松点过程(homogeneous Poisson point process)<sup>[17]</sup>模型来描述. 具体地说, 若辅助节点部署后的密度为  $\rho_a$ , 则其随机部署可描述为服从速率为  $\rho_a$  的同构泊松点过程的一个事件序列.

设  $u$  和  $v$  之间的通信距离为  $x$  ( $x \leq r$ ), 则图 2 中阴影区域  $Z_{\text{shaded}}(x)$  可描述如下:

$$Z_{\text{shaded}}(x) = 2R^2 \cos^{-1}\left(\frac{x}{2R}\right) - x \sqrt{R^2 - \frac{x^2}{4}} \quad (1)$$

设辅助节点密度为  $\rho_a = \frac{N_a}{|Z|}$  (其中  $|Z|$  为部署区域,  $N_a$  为辅助节点总数), 则  $u$  有  $s$  个相邻辅助节点的概率就等于  $s$  个辅助节点位于区域  $\pi R^2$  的概率  $p(|NA_u| = s)$ :

$$p(|NA_u| = s) = \frac{(\rho_a \pi R^2)^s}{s!} e^{-\rho_a \pi R^2} \quad (2)$$



因此,一个普通节点平均拥有的相邻辅助节点数可表述如下:

$$\lambda = E[s \times p(|NA_u| = s)] = \rho_a \pi R^2 \quad (3)$$

更进一步,两个相邻普通节点至少共享  $g$  个公共辅助节点的概率就相当于  $g$  个辅助节点被部署在它们公共辅助通信区域  $Z_{\text{shaded}}(x)$  里的概率,可描述如下:

$$\begin{aligned} p(|NA_{\text{shaded}}| \geq g) &= 1 - \sum_{i=0}^{g-1} p(|NA_{\text{shaded}}| = i) \\ &= 1 - \sum_{i=0}^{g-1} \frac{(\rho_a Z_{\text{shaded}}(x))^i}{i!} e^{-\rho_a Z_{\text{shaded}}(x)} \end{aligned} \quad (4)$$

## 4 基于散列链的随机密钥预分发方案

本方案可分为 3 个阶段:(1)部署前预分发阶段.主要是如何把密钥信息分别分发给普通节点和辅助节点;(2)直接对偶密钥建立阶段,主要是如何在相邻普通节点之间建立对偶密钥;(3)路径密钥建立阶段,主要是如何借助中间普通节点,帮助相邻普通节点建立对偶密钥.下面详细阐述各阶段.

### 4.1 部署前预分发

一个离线的可信服务器生成一系列散列链并构成密钥池.所有散列链共用一个种子  $seed$ ,对于散列链  $C_i$ ,假设其生成因子为  $G_i$ ,则该散列链的第  $j$  个链密钥生成如下:

$$k_{i,j} = H^j(seed, G_i) \quad (5)$$

其中,  $H^j(seed, G_i) = H(H^{j-1}(seed, G_i), G_i)$  ( $1 \leq j \leq M$ ).散列链的最后一个元素,  $H^{M+1}(seed, G_i)$  被称为该散列链的  $commitment$ .该元素不做为密钥池的元素.

为了生成密钥池,可信服务器选择  $L$  个不同的生成因子,反复执行上述的散列链生成过程,生成  $L$  个散列链.最终的密钥池将由  $L$  个散列链组成,其中每个散列链包含  $M$  个链密钥.如图 3 所示.

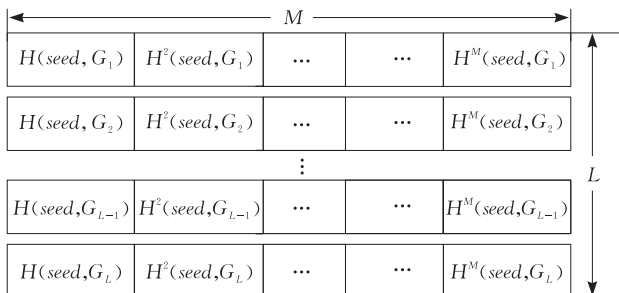


图 3 密钥池的组成

密钥池生成之后,对普通节点和辅助节点的密钥分配策略执行如下:

每一个普通节点从  $L$  个散列链里随机选取  $q_n$  个不同的  $commitments$ ,另外,普通节点还载入散列函数  $H$  和一个伪随机函数  $F$ (用于生成派生密钥).与其他随机密钥预分发方案不同的是,普通节点并没有从密钥池里选取任何链密钥.

每一个辅助节点选取以下机密信息:(1)从密钥池随机选取的  $q_a$  个不同的链密钥,这里对每一个散列链被选取的链密钥数并没有任何限制;(2)若某一个散列链  $C_i$  的一个或多个链密钥被选取,则辅助节点预分发对应的散列映像  $F(commitment_i)$  及其生成因子  $G_i$ .例如,若链密钥  $k_{3,4}$  被辅助节点选取,则辅助节点同时保存  $F(commitment_3)$  和生成因子  $G_3$ .  $F(commitment)$  为辅助节点的广播通信密钥.

所有普通节点和辅助节点预分发各自的机密信息后就随机部署在指定的区域里.

### 4.2 直接对偶密钥建立

所有节点部署后,辅助节点开始广播其预分发的链密钥以及其标识.若辅助节点包含了多个散列链的链密钥,则它广播多个数据包.每一个数据包包含 3 部分内容:(1)同一散列链的所有链密钥以及其索引;(2)该散列链的生成因子;(3)辅助节点的标识,数据包使用相应的  $F(commitment)$  加密.例如,如果辅助节点  $A_w$  从散列链  $C_i$  里预分发了  $\tau$  个链密钥,则所广播的数据包格式如下:

$i, E(F(commitment_i), ID_{A_w} | k_{i,j_1} | \dots | k_{i,j_\tau} | j_1 | \dots | j_\tau | G_i), ID_{A_w}$  是辅助节点  $A_w$  的标识,  $i$  为密钥链标识.参数  $\tau$  必须大于等于 1 并且小于等于  $M$ .  $E(K, m)$  表示使用密钥  $k$  对信息  $m$  进行加密.

若普通节点与其相邻辅助节点共享公共散列链,则该节点可以解密接收到的相应的广播数据包.数据包解密后,节点就可以使用对应的  $commitment$  和生成因子,利用式(5)对链密钥进行认证.若链密钥  $k_{i,j}$  认证通过,节点则使用该链密钥和辅助节点的标识生成一个派生密钥  $k_{i,j,w}$  如下:

$$k_{i,j,w} = F(k_{i,j} \parallel ID_{A_w}) \quad (6)$$

注意:若链密钥  $k_{i,j}$  无法通过认证,或参数  $j$  的取值范围不在 1 与  $M$  之间,该链密钥将被丢弃,因为该链密钥有可能是被攻击者伪造的.

对数据包链密钥认证过程完成后,无论有多少个链密钥通过认证,普通节点都将删除所接收的所有辅助节点标识和生成因子.

尽管普通节点可能与其他辅助节点共享相同的散列链,但由于各个辅助节点的标识不相同,所以生成的派生密钥是不相同的. 每一个普通节点所生成的派生密钥总数,与其相邻的辅助节点数量相关. 因此,不同的普通节点,其派生密钥的总数可能是不相同的.

一旦普通节点生成了所有的派生密钥,它们将发送广播数据包,标明各自所包含的派生密钥. 但广播数据包并不包含真正的派生密钥,而是仅仅包含派生密钥的索引. 例如,索引  $\langle i, j, w \rangle$  表示派生密钥  $k_{i,j,w}$  是由链密钥  $k_{i,j}$  和辅助节点  $A_w$  的标识生成的,若两个普通节点有相同的派生密钥索引,则它们共享同一派生密钥. 若两个普通节点之间共享的派生密钥数为  $t$ ,即  $\{k_1, k_2, \dots, k_t\}$ ,超过阈值  $q$ ,即  $t \geq q$ ,它们就可以分别使用这  $t$  个派生密钥生成对偶密钥如下:

$$k_{uv} = k_1 \oplus k_2 \oplus \dots \oplus k_t \quad (7)$$

上式中,  $\oplus$  表示“异或”操作.

一旦生成对偶密钥,普通节点将删除所有的派生密钥.

#### 4.3 路径密钥建立

如果两个相邻普通节点共享的派生密钥数达不到阈值  $q$ ,则意味着它们之间无法直接建立对偶密钥. 在这种情况下,有两种选择: (1) 使用与 Eschenauer 方案相类似的方法去建立对偶密钥; (2) 不建立对偶密钥,若网络部署密度大足以保证以非常高的概率进行信息传送,一些相邻普通节点之间不建立安全通信链路是可以接受的.

### 5 性能分析

在这一部分,主要分析我们提出方案的性能,并与典型的随机密钥预分发方案<sup>[10-11]</sup>进行比较.

#### 5.1 网络安全连通性分析

网络安全连通性被定义为 WSN 建立安全通信链路的概率. 如果两个相邻普通节点共享足够数量的派生密钥,则它们可以建立安全的通信链路.

对于相邻普通节点  $u$  和  $v$ ,若下述两个条件之一满足,则它们之间无法共享派生密钥: (1) 它们之间不共享任何散列链; (2) 它们与公共辅助节点不共享任何散列链. 若上述两个条件不成立,则  $u$  和  $v$  可能共享派生密钥.

设  $m_i$  为两个相邻普通节点  $u$  和  $v$  通过它们的一个公共相邻辅助节点而生成的派生密钥数,  $m$  为

通过所有  $g$  个公共相邻辅助节点生成的派生密钥总数,则有  $m = m_1 + m_2 + \dots + m_g$ . 下面首先证明一个引理和一个定理.

**引理 1.** 假设两个相邻普通节点  $u$  和  $v$  仅有一个公共的相邻辅助节点,若  $u$  与  $v$  共享的 *commitment* 数为  $l$ ,则它们之间共享的派生密钥数不超过  $l \times M$ .

证明. 同一个散列链的 *commitment*,连同生成因子,可以对该散列链的所有链密钥进行认证,所以每一个 *commitment* 至多可认证  $M$  个链密钥. 由于  $u$  和  $v$  之间共享的派生密钥所使用的链密钥必须通过它们之间共享的 *commitments* 进行认证,而  $u$  和  $v$  共享的 *commitment* 数为  $l$ ,即使这  $l$  个 *commitments* 所对应的散列链的所有链密钥均被  $u$  和  $v$  的公共相邻辅助节点所选取,  $u$  和  $v$  之间共享的派生密钥数也不过为  $l \times M$ ,一旦其中有一个或多个链密钥未被选取,则  $u$  和  $v$  之间的共享派生密钥数不超过  $l \times M$ .

证毕.

**定理 1.** 假设相邻普通节点  $u$  和  $v$  之间有  $g$  个公共的相邻辅助节点,并且通过各公共辅助节点而生成的派生密钥数分别为  $m_1, m_2, \dots, m_g$  ( $\forall i, m_i \leq q_n$ ). 则  $u$  和  $v$  之间共享的 *commitment* 数至少应为  $\left\lceil \frac{\max(m_1, m_2, \dots, m_g)}{M} \right\rceil$ .

证明. 若两个相邻普通节点  $u$  和  $v$  共享的 *commitment* 数为  $l$ ,根据引理 1,它们通过其中任何一个公共相邻辅助节点所生成的派生密钥数在  $0$  与  $l \times M$  之间. 反过来说,若它们通过公共辅助节点  $A_i$  生成  $m_i$  个派生密钥,则它们必须共享的 *commitment* 数至少为  $\left\lceil \frac{m_i}{M} \right\rceil$ . 对于所有的  $m_i$  ( $i = 1, 2, \dots, g$ ),若  $u$  和  $v$  共享足够的 *commitment* 数来确保能够生成最大数量的派生密钥,则它们一定也能够通过其他公共辅助节点生成其他数量的派生密钥,因此,  $u$  和  $v$  之间共享的 *commitment* 数至少为  $\left\lceil \frac{\max(m_1, m_2, \dots, m_g)}{M} \right\rceil$ .

证毕.

假设  $u$  与  $v$  共享的 *commitment* 数为  $l$ ,对于它们之间任意的一个公共辅助节点,如  $A_w$ ,若  $u$  和  $v$  通过  $A_w$  可以生成  $s$  个派生密钥,则  $A_w$  预分发  $q_a$  个链密钥的方法如下: 首先从  $u$  和  $v$  共享的  $l$  个 *commitments* 所对应的  $l$  个散列链里随机选取  $s$  个链密钥,共有  $\binom{l \times M}{s}$  种选取方法; 然后从剩余的

$(L-l)$  个散列链里随机选取  $(q_a-s)$  个链密钥, 共有  $\binom{(L-l) \times M}{q_a-s}$  种选取方法. 因此,  $A_w$  预分发  $q_a$  个链密钥的方法可描述如下:

$$\Omega(l, s) = \binom{l \times M}{s} \binom{(L-l) \times M}{q_a-s} \quad (8)$$

若  $u$  和  $v$  之间有  $g$  个公共相邻辅助节点, 并且通过各个辅助节点可生成的派生密钥数分别为  $m_1, m_2, \dots, m_g$ , 则它们之间共享  $m$  个派生密钥的概率可描述如下: 首先,  $u$  可从  $L$  个散列链随机选取  $q_n$  个 *commitments*, 共有  $\binom{L}{q_n}$  种选取方法, 其次, 一共有

$\sum_{m_1+m_2+\dots+m_g=m}$  种方法让公共服务节点提供共享链密钥. 根据定理 1,  $u$  与  $v$  共享的 *commitments* 将在  $\left\lceil \frac{\max(m_1, m_2, \dots, m_g)}{M} \right\rceil$  和  $q_n$  之间, 假设它们之间共享的 *commitment* 数为  $l$ , 则  $v$  可随机从  $u$  已选取的  $q_n$  个散列链中随机选取  $l$  个 *commitments* 以及从剩余的  $(L-q_n)$  个散列链里随机选取  $(q_n-l)$  个 *commitments*, 因此  $v$  共有  $\binom{q_n}{l} \binom{L-q_n}{q_n-l}$  种选取方法, 而各个公共辅助节点选取方法如同式(8)所示. 因此,  $u$  和  $v$  通过  $g$  个公共相邻辅助节点生成  $m$  个派生密钥的概率可描述如下:

$$p(m) = \left[ \sum_{m_1+m_2+\dots+m_g=m} \sum_{i=\left\lceil \frac{\max(m_1, m_2, \dots, m_g)}{M} \right\rceil}^{q_n} \binom{q_n}{i} \binom{L-q_n}{q_n-i} \Omega(i, m_1) \dots \Omega(i, m_g) \right] / \left( \binom{L}{q_n} \binom{L \times M}{q_a}^g \right) \quad (9)$$

显然, 两个相邻普通节点  $u$  和  $v$  之间共享少于  $q$  个派生密钥的概率为  $\sum_{i=0}^{q-1} p(i)$ , 其中  $p(i)$  定义如式(9). 因此,  $u$  和  $v$  之间至少共享  $q$  个派生密钥的概率可描述如下:

$$p_{\text{connect}} = 1 - (p(0) + p(1) + \dots + p(q-1)) \\ = 1 - \left[ \sum_{m_1=0}^{q-1} \sum_{m_2=0}^{q-m_1-1} \dots \sum_{m_g=0}^{q-m_1-\dots-m_{g-1}-1} \sum_{l=\left\lceil \frac{\max(m_1, m_2, \dots, m_g)}{M} \right\rceil}^{q_n} \binom{q_n}{l} \binom{L-q_n}{q_n-l} \Omega(l, m_1) \dots \Omega(l, m_g) \right] / \left( \binom{L}{q_n} \binom{L \times M}{q_a}^g \right) \quad (10)$$

## 5.2 参数分析

从式(10)可以看出, 一些系统参数, 如散列链的

长度  $M$ 、散列链的数量  $L$ 、公共相邻辅助节点数  $g$  等, 都将影响网络的安全连通性. 下面将详细讨论这些参数以及将本方案与典型的随机密钥预分发方案进行比较. 下面所有分析, 都将在达到 99.99% 的网络安全连通性的情况下进行.

### 5.2.1 公共相邻辅助节点的影响

相邻普通节点所拥有的公共派生密钥数量取决于它们之间的公共相邻辅助节点的数量. 因此, 公共辅助节点的数量越多, 两个相邻普通节点之间共享派生密钥的概率就越大. 图 4 显示在公共辅助节点的数量分别为 1, 2 和 3 时, 每一个普通节点所需预分发的 *commitment* 数与每一个辅助节点预分发的链密钥数之间的对比关系.

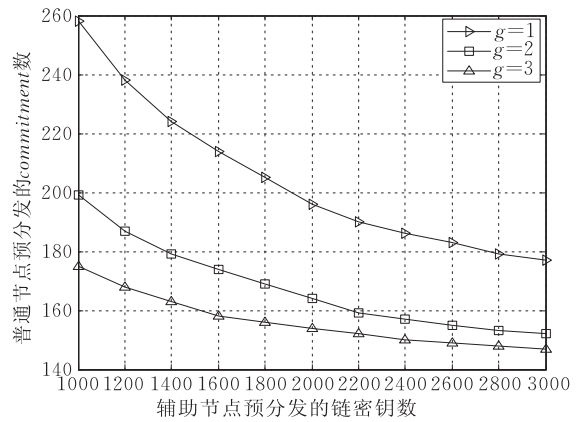


图 4 普通节点预分发的 *commitment* 数与辅助节点预分发的链密钥数的对比关系 (其中,  $M=8, L=2500, q=1$ )

图 4 提供了与上述观察相吻合的结果, 即公共辅助节点越多, 普通节点所需预分发的 *commitment* 数就越少. 同时也揭示了一个十分有趣的现象, 那就是公共辅助节点数量的提高并不能显著降低辅助节点所需预分发的链密钥数. 例如, 当辅助节点预分发的链密钥数为 3000 时, 公共辅助节点的数量从 2 增加到 3 时, 辅助节点所需预分发的 *commitment* 数仅仅降低了 3.29%, 即从 152 降低到 147.

### 5.2.2 散列链长度的影响

在同一个散列链里的每一个链密钥都可被所对应的 *commitment* 和生成因子所认证. 因此, 散列链的长度越长, 则可认证的链密钥则越多, 也就是, 普通节点所需预分发的 *commitment* 数就越少. 图 5 显示了散列链的长度如何影响普通节点所需预分发的链密钥数.

值得注意的是, 在图 5 中, 散列链的长度越长, 曲线将变得越平滑. 这意味着所需预分发的 *commitment* 数的衰减速率将放缓. 例如, 当辅助节点预分

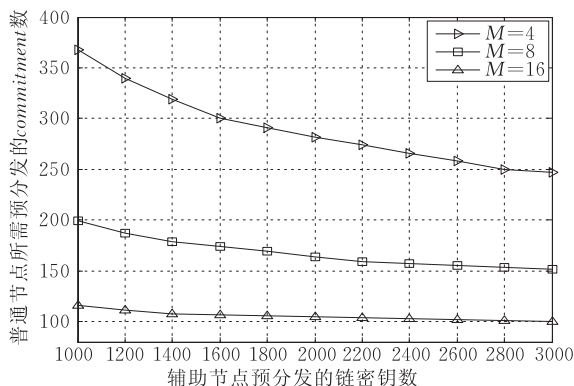


图 5 不同的散列链长度对普通节点所需预分发的 *commitment* 数的影响(其中,  $L \times M = 20000$ ,  $g=2$ ,  $q=1$ )

发的链密钥数从 1000 增加到 3000 时,散列链的长度为 4 时,普通节点所需预分发的 *commitment* 数将减少 32.8%(从 368 降至 247),而当散列链的长度为 16 时,所需预分发的 *commitment* 数仅仅减少 13.8%(从 116 降至 100)。因此,若散列链的长度足够长,增加辅助节点预分发的链密钥数并不能显著影响网络的安全连通性。同时这也表明:散列链的长度是影响网络连通性能的一个重要因素,也显著影响着普通节点所需预分发的 *commitment* 数。

### 5.3 与典型随机密钥管理方案比较

#### 5.3.1 与 Eschenauer 方案的比较

在 Eschenauer 方案里,当密钥池的密钥总数增多时,为了确保达到较高的安全连通性,节点也必须预分发更多的密钥数。但由于节点资源受限的特点,节点预分发的密钥数不宜过多。但从安全的角度来看,密钥池的密钥总数越多,将使得攻击者必须俘获更多的节点才能获得更多的密钥,因此密钥总数越多,或预分发的密钥数越少,网络的抗毁性相对就越强。

图 6 显示了在不同的密钥池总数大小和不同的散列链数量的情况下,本方案与 Eschenauer 方案的

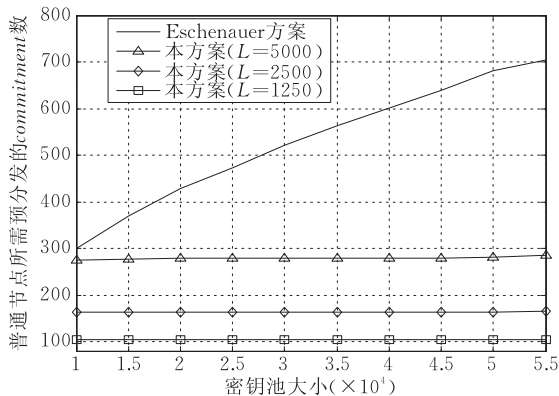


图 6 本方案与 Eschenauer 方案的比较

普通节点所需预分发的密钥或 *commitment* 数。在本方案里,辅助节点预分发的链密钥数为 2000,公共辅助节点数为 1。

从图 6 看出,本方案不仅仅是普通节点所需预分发的 *commitment* 数要小于 Eschenauer 方案里节点所需预分发的密钥数,而且,在不同的散列链数量情况下,不管密钥池的密钥总数如何,只要散列链的数量固定,本方案里的节点所需预分发的 *commitment* 数就基本不变。因此,本方案具有一个非常显著的特点,那就是不管密钥池大小如何,只要适当调整散列链的数量,就使得普通节点所需预分发的 *commitment* 数保持很低,而且基本不变。这表明,本方案在密钥池相对较大时将是非常有效的。

#### 5.3.2 与 $q$ -composite 方案的比较

$q$ -composite 方案通过提高共享密钥的阈值来提高网络的抗毁性,然而,这也意味着,节点必须预分发更多的密钥,或者密钥池的密钥总数需降低。图 7 显示在不同的散列链长度的情况下,本方案与  $q$ -composite 方案的比较。在本方案里,辅助节点预分发的链密钥数为 2000,公共辅助节点数为 1。

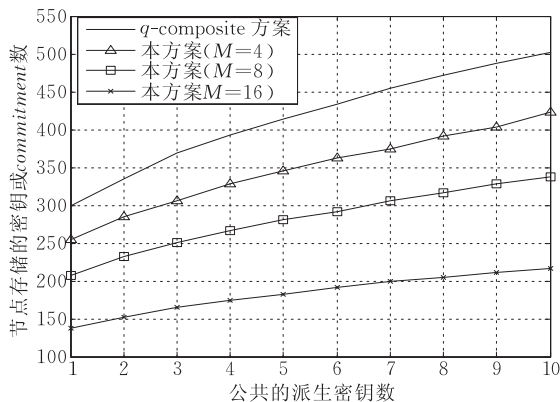


图 7 本方案与  $q$ -composite 方案的比较

图 7 的结果显示,本方案里普通节点所需预分发的 *commitment* 数要比  $q$ -composite 方案里节点预分发的密钥数要少。而且,当散列链的长度稍微增长时,普通节点所需预分发的 *commitment* 数将显著降低,这就意味着,在本方案里只要散列链的长度足够大,普通节点只要稍微提高一下预分发的 *commitment* 数,就将能够极大地提高网络的安全连通性。

### 5.4 理论分析与模拟实验的结果比较

为了验证式(10)推导的正确性,本文运行了一个模拟实验,共有 1000 个普通节点和辅助节点,设置了 4 个场景,验证在不同的散列链数量、散列链长度以及不同的派生密钥阈值情况下理想链路与实际



链路之间的差异. 对于两个相邻普通节点, 若它们至少存在一个公共辅助节点, 则存在一条理想链路; 若它们之间至少存在一个仅供辅助节点, 并且与公共辅助节点至少共享一个散列链, 则存在一条实际链路. 表 1 显示了模拟实验的条件设置, 其中, 各个场景里的 *commitment* 数值, 是根据式 (10) 所能达到 99.99% 的安全连通概率而设定的, 而 *curkeys* 表示辅助节点预分发的链密钥数.

表 1 模拟实验里不同场景的参数设置	
场景	参数设置
场景 1	$M=4, L=5000, g=2, curkeys=1000, m=1, commitments=368$
场景 2	$M=8, L=2500, g=3, curkeys=3000, m=1, commitments=146$
场景 3	$M=4, L=5000, g=1, curkeys=2000, m=3, commitments=437$
场景 4	$M=8, L=2500, g=1, curkeys=2000, m=8, commitments=293$

图 8 显示了模拟实验的结果.

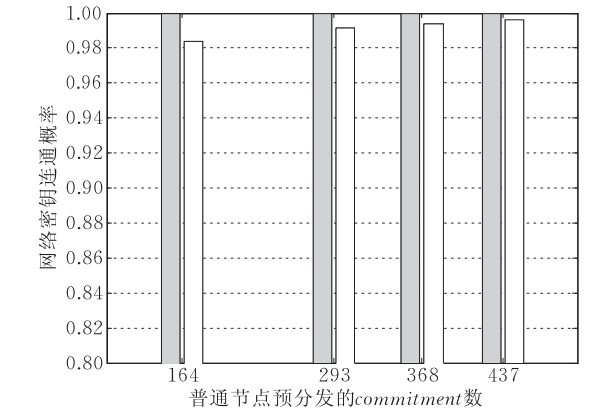


图 8 模拟结果与理论结果的比较

图 8 显示了模拟结果所得到的实际链路与理想链路的比率. 从结果可以看出, 当普通节点预分发的 *commitment* 数分别为 164, 293, 368 和 437 时, 这个比率分别为 98.16%, 99.13%, 99.41% 和 99.64%, 这说明模拟结果与实际分析结果至多存在着 1.84% 的差异, 从而证明式 (10) 的推导正确性.

从以上分析可以看出, 与其他典型的随机密钥预分发方案相比, 本方案极大地提高了网络安全连通性. 其原因是归结于散列链的链密钥关联性以及公共辅助节点的作用. 散列链能够使得链密钥之间的相关性得到提高, 从而使得普通节点仅需保存少量特殊的秘密信息 (即 *commitments*), 就能够借助辅助节点来生成众多的派生密钥. 从而能够以较小的存储开销获取较高的网络安全连通性.

6 安全分析

本方案可以有效地防御被动攻击. 一方面, 辅助节点广播的每一个数据包都使用  $F(commitment)$  加密, 攻击者无法窃听到该数据包的任何数据; 另一方面, 普通节点之间发送的数据包仅仅包含派生密钥的索引, 攻击者即使能够窃取这些数据包, 也不能由此获取任何派生密钥.

本方案也可以有效防御主动攻击. 例如: 攻击者伪造广播数据包, 对普通节点发起 DoS 攻击, 由于其无法获取  $F(commitment)$ , 因此该广播数据包被普通节点丢弃; 即使攻击者通过俘获辅助节点而获取  $F(commitment)$ , 但也无法伪造链密钥, 因为每一个链密钥都必须经过认证才能被普通节点所接受. 最常见的一种主动攻击方式是攻击者俘获普通节点或辅助节点, 利用受损的节点对网络进行攻击. 下面我们首先证明一个定理, 然后对节点受损情况进行分析.

正常的普通节点之间的对偶密钥的安全性可以表述如下定理 2.

**定理 2.** 对于两个正常普通节点, 即使它们共享的散列链全部受损, 只要存在一个安全的公共辅助节点且至少一个派生密钥通过该节点生成, 攻击者就不可能获取它们之间的对偶密钥.

证明. 若两个正常普通节点的散列链全部受损, 意味着攻击者可能获取相对应散列链的所有链密钥. 然而, 从式 (6) 可以看出, 对于派生密钥  $k_{i,j,w}$  而言, 若辅助节点标识  $ID_{A_w}$  是安全的, 该派生密钥就一定是安全的; 因此, 只要存在一个安全的共享辅助节点且生成相应的派生密钥, 该派生密钥就一定是安全的. 从式 (7) 也可以推出以下结论:  $t$  个共享派生密钥只要有一个是安全的, 则所生成的对偶密钥就肯定是安全的.

证毕.

下面详细分析普通节点受损或辅助节点受损对网络抗毁性的影响. 也就是, 部分普通节点或辅助节点的受损如何影响未受损的相邻普通节点之间通信链路的受损概率, 显然, 这个概率值越小, 网络的抗毁性就越好.

6.1 普通节点受损分析

首先考虑仅有一小部分普通节点受损, 而所有的辅助节点都是安全的情况. 显然, 若一个普通节点受损, 则它所包含的机密信息将全部暴露. 而且, 受损普通节点能够解密所接收到的由辅助节点广播的

部分数据包并获取相应链密钥和生成因子。

当一个普通节点受损时,则一个链密钥属于受损散列链的概率为  $\frac{q_n}{L}$ , 由于每一普通节点平均可拥有  $\lambda$  个相邻辅助节点( $\lambda$  的定义如式(3)), 则一个链密钥被这  $\lambda$  个辅助节点选取的概率为  $\frac{\lambda q_a}{L \times M}$  (假设这  $\lambda$  个辅助节点选取的链密钥各不相同, 这样受损的链密钥数最大)。因此, 一个派生密钥是安全的概率为  $1 - \frac{q_n}{L} \times \frac{\lambda q_a}{L \times M}$ , 假设有  $\alpha$  个受损普通节点, 则在存在着  $\alpha$  个受损普通节点时, 一个派生密钥仍然安全的概率为  $\left(1 - \frac{q_n}{L} \times \frac{\lambda q_a}{L \times M}\right)^\alpha$ 。因此, 一个派生密钥受损的概率为

$$p_{c1} = 1 - \left(1 - \frac{q_n}{L} \times \frac{\lambda q_a}{L \times M}\right)^\alpha \quad (11)$$

若两个普通节点之间的对偶密钥由  $t$  个派生密钥生成, 则一条通信链路受损的概率为  $(p_{c1})^t$ 。因此, 当存在  $\alpha$  个受损普通节点时, 两个正常的相邻普通节点之间的通信链路受损的概率可表述如下:

$$p_{\text{compromised}_1} = \sum_{t=g \times q_a} (p_{c1})^t \frac{p(t)}{p_{\text{connect}}} \quad (12)$$

其中,  $p(t)$  和  $p_{\text{connect}}$  分别定义如式(9)和式(10),  $g$  为公共辅助节点数。

图 9 显示了在网络安全连通概率为 0.5, 公共辅助节点数为 1, 每一个(普通)节点预分发的链密钥或 commitment 数都为 200 时, 不同的受损普通节点数对非受损普通节点的通信链路的影响。

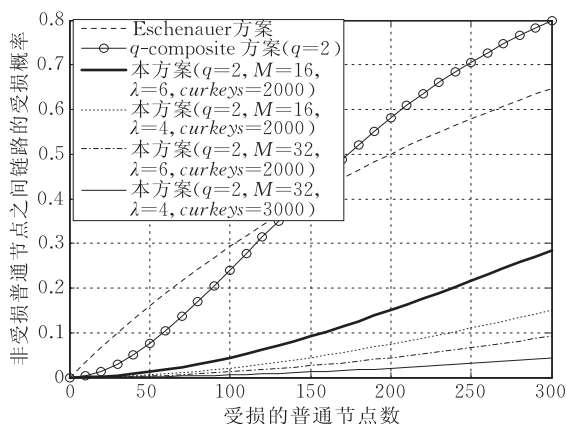


图 9 正常普通节点的通信链路受损的概率

图 9 对本方案、Eschenauer 方案和  $q$ -composite 方案的抗毁性进行了比较。显然, 本方案比其他两个方案提供了更强的抗毁性。例如, 当有 250 个受损普通节点时, Eschenauer 方案和  $q$ -composite 方案分别

有 59% 和 71% 的非受损普通节点之间的通信链路受损, 而本方案在散列链长度为 16 时仅有 21% ( $\lambda=6$ ) 或 11% ( $\lambda=4$ ) 的非受损普通节点之间的通信链路受损。而且, 在本方案里, 适当降低平均公共辅助节点数或提高散列链长度还可以降低通信链路受损的概率。从图 9 可以看出, 当散列链的长度从 16 提高一倍至 32, 通信链路受损的概率则显著降低两倍以上。

## 6.2 辅助节点受损分析

下面考虑仅有部分辅助节点受损而所有的普通节点都未受损的情况。攻击者可以使用受损的辅助节点广播伪造的标识信息, 这样就会导致普通节点可能会使用伪造的标识信息生成派生密钥。然而, 在本方案里, 攻击者因为不能掌握散列函数  $H$  和伪随机函数  $F$  的任何知识而无法生成或伪造任何派生密钥。从派生密钥生成的角度来看, 伪造的标识信息对派生密钥无任何影响, 攻击者显然无法获取任何派生密钥。

但本方案存在一个局限性, 那就是, 如果所有的辅助节点在派生密钥生成阶段都受损了, 普通节点就有可能无法生成对偶密钥了。为了解决这个问题, 可以使辅助节点与普通节点的外表看起来尽量无差异, 由于攻击者无法区分哪一类节点, 就只能随机对节点进行攻击了。而且, 辅助节点的作用仅仅是在部署后广播其标识信息及链密钥, 攻击者不可能在非常短的时间内使得所有的辅助节点受损。因此, 在本方案里, 因全部辅助节点在短时间内同时全部受损而导致无法在相邻普通节点之间建立对偶密钥的情况发生性非常小。

## 6.3 普通节点与辅助节点同时受损分析

显然, 与仅有某一类型的节点受损情况相比, 攻击者更有可能对某一区域内混合数量的普通节点和辅助节点进行攻击, 从而使得在某一区域的部分辅助节点和普通节点有可能受损。在本方案里, 一般而言, 所部署的普通节点的数量要远远多于辅助节点的数量。因此, 若某一区域的部分普通节点和辅助节点受损, 一般情况下, 受损的普通节点数应该多于受损辅助节点的数量。

假定存在着  $\alpha$  个受损普通节点和  $\beta$  个受损辅助节点。可进一步假设  $\alpha > \beta$ 。对于这  $\beta$  个受损辅助节点, 可以分为两部分: 一部分是与  $\alpha$  个受损普通节点相邻的, 称这一部分的辅助节点为相邻的受损辅助节点; 另一部分与任何一个受损普通节点均不相邻, 称这一部分的辅助节点为分离的受损辅助节点。对

于相邻的受损辅助节点,在存在  $\alpha$  个受损普通节点的情况下,一个派生密钥受损的概率为  $p_{c1}$ ,无论相邻的辅助节点数量为多少.另一方面,假设分离的受损辅助节点数为  $\rho\beta$ , ( $0 < \rho < 1$ ),则一个密钥在存在  $\alpha$  个受损普通节点的情况下属于受损散列链的概率为  $1 - \left(1 - \frac{q_n}{L}\right)^\alpha$ ,所以,在存在  $\rho\beta$  个分离的受损辅助节点的情况下,一个派生密钥受损的概率应为

$$p_{c2} = 1 - \left(1 - \left(1 - \left(1 - \frac{q_n}{L}\right)^\alpha\right) \left(\frac{\rho\beta \times q_a}{L \times M}\right)\right)^{\rho\beta} \quad (13)$$

因此,在存在  $\alpha$  个受损普通节点和  $\beta$  个受损辅助节点的情况下,正常普通节点之间的通信链路的受损概率可表述如下:

$$p_{\text{insecure}_2} = \sum_{t=q}^{g \times q_a} (p_{c1} + p_{c2})^t \frac{p(t)}{p_{\text{connect}}} \quad (14)$$

图 10 显示的是在网络连通概率为 0.5,每个普通节点预分发 200 个 *commitments*,辅助节点预分发 2000 个链密钥,散列链长度为 16 的情况下,不同比例和数量的受损普通节点和辅助节点与非受损普通节点之间通信链路受损的对比关系.

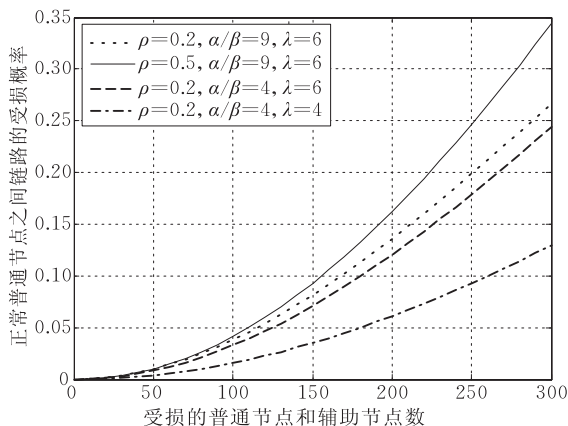


图 10 同时存在受损普通节点和受损辅助节点时非受损普通节点之间通信链路受损的概率

从图 10 可以看出,本方案里普通节点受损仍然是影响通信链路受损的主要因素.甚至在出现大量的分离的受损辅助节点的情况下,本方案仍保持很高的抗毁性.例如,当受损普通节点和受损辅助节点的总数为 300 时,即使受损辅助节点的一半是分离的,通信链路的受损概率才仅为 34%.

## 7 总结与展望

密钥管理是保证 WSN 实现安全通信的重要机制.从目前的研究成果和发展趋势看,随机密钥管理

方案比较符合 WSN 节点资源严格受限的特点,引起了广泛的关注.本文提出的基于散列链的随机密钥预分发方案,通过提高密钥相关性,有效地解决了目前 WSN 同类方案所存在的无法同时满足达到较高的安全连通概率和较强的网络抗毁性的问题.理论分析和模拟实验结果证明本文所提出的方案能够提供理想的安全连通性和抗毁性,为大规模 WSN 的密钥管理研究提供了可行的、有重要参考价值的解决思路.

针对本方案,有一些问题仍值得继续深入研究,例如:系统参数如何组合优化,才能达到最佳的网络安全连通性及网络抗毁性;还有,在存在其他类型的攻击,如 wormhole 攻击、sinkhole 攻击等情况下,网络的抗毁性研究等.

## 参 考 文 献

- [1] Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor network: A survey. *Computer Networks*, 2002, 38(4): 393-422
- [2] Deng J, Han R, Mishra S. INSENS: Intrusion-tolerant routing in wireless sensor networks//*Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems (ICDCS)*. Providence, Rhode Island, USA, 2003: 32-39
- [3] Lazos L, Poovendran R. SeRLoc: Secure range-independent localization for wireless sensor networks//*Proceedings of the ACM Workshop on Wireless Security (WISE)*. Philadelphia, PA, USA, 2004: 21-30
- [4] Przydatek B, Song D, Perrig A. SIA: Secure information aggregation in sensor networks//*Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*. California, USA, 2003: 255-265
- [5] Crossbow Technology, Inc. MICA2: Wireless measurement system.
- [6] Koc K C. High-speed RSA implementation. RSA Laboratories: Technical Report TR201, 1994
- [7] Neuman B C, Tso T. Kerberos: An authentication service for computer networks. *IEEE Communications*, 1994, 32(9): 33-38
- [8] Chan H, Perrig A, PIKE: Peer intermediaries for key establishment in sensor networks//*Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*. Miami, FL, USA, 2005: 524-535
- [9] Camtepe S A, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks//*Proceedings of the Computer Security—ESORICS*. Sophia Antipolis, French Riviera, France, 2004: 293-308

- [10] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks//Proceedings of the 9th ACM Conference on Computer and Communications Security. Washington, USA, 2002: 41-47
- [11] Chan H, Perrig A, Song D. Random key Pre-distribution schemes for sensor networks//Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, California, USA, 2003: 197-213
- [12] Traynor P, Choi H, Cao G, Zhu S, Porta T L. Establishing pairwise keys in heterogeneous sensor networks//Proceedings of the 25th IEEE Conference on Computer Communications (INFOCOM). Barcelona, Catalunya, Spain, 2006: 52-91
- [13] Liu D, Ning P. Location-based pairwise key establishments for static sensor networks//Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. Fairfax, Virginia, USA, 2003: 72-82
- [14] Du W, Deng J, Han Y S, Chen S, Varshney P K. A key management scheme for wireless sensor networks using deployment knowledge//Proceedings of the IEEE INFOCOM. Piscataway, USA, 2004: 586-597
- [15] Malan D J, Welsh M, Smith M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography//Proceedings of the IEEE Sensor and Ad Hoc Communications and Networks (SECON). Santa Clara, Canada, 2004: 71-80
- [16] Uhsadel L, Poschmann A, Paar C. Enabling full-size public-key algorithms on 8-bit sensor nodes//Proceedings of the 4th European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS). Cambridge, UK, 2007: 73-86
- [17] Cressie N. Statistics for Spatial Data. New York: John Wiley & Sons, 1993



**SU Zhong**, born in 1969, Ph. D. candidate. His research interests include network security, wireless sensor network and performance evaluation.

**LIN Chuang**, born in 1948, Ph.D., professor and Ph. D.

supervisor. His current research interests include computer networks, performance evaluation, network security, Petri net theory, trustworthy networks and trustworthy computing.

**REN Feng-Yuan**, born in 1970, Ph. D., associate professor and Ph. D. supervisor. His current research interests include network traffic management and control, wireless sensor networks and performance evaluation.

## Background

This work is supported by the National Natural Science Foundation of China (60673187, 60773138, 60573122), the National High-Tech Research and Development Plan of China (2006AA01Z117), the National Grand Fundamental Research 973 Program of China (2006CB303000) and finished in the QoS Group, Department of Computer Science and Technology, Tsinghua University.

Key management is timely important issue in secure wireless sensor networks and meets many new challenges due to the sensor nodes' stringent resource constraints. Although the deterministic key pre-distribution schemes can ensure that every pair of nodes establish pair-wise key directly, those schemes may induce extreme requirement in term of computation, storage, communication and energy. The ran-

dom key pre-distribution schemes are the most suitable schemes for WSN, however, most of these schemes fail to provide high network connectivity performance and strong resilience against nodes compromised simultaneously. One reason is that the keys which consist of the key pool are less relevant. Hence, the authors try to improve the correlation of keys and propose a hash chain based random key pre-distribution scheme to address the limitation. Theoretical analysis and simulation results demonstrate that the correlation improvement of keys can reach the high network connectivity performance and maintain strong resilience against nodes compromised even though there are a lot of compromised nodes. We believe that the constructions can bring random key pre-distribution technology into the realm of the practical.