

文章编号:1001-9081(2006)08-1802-05

## 传感器网络的多重单向散列随机密钥预分配协议

李志军, 耿 技, 王佳昊, 秦志光

(电子科技大学 计算机科学与工程学院, 四川 成都 610054)

(leezj@uestc.edu.cn)

**摘 要:**首先借鉴 Leighton Micali 协议中的多重单向散列建立密钥思想,设计了一种基本的多重单向散列密钥分配协议。该协议能确保所有邻居节点能建立安全链路,但是安全性能差。然后结合多重单向散列与随机密钥预分配,提出了多重单向散列随机密钥预分配协议,并详细分析了性能。与现有的协议相比,该协议只需很少的单向散列运算,计算负载小,安全性能高,非常适用于传感器网络。

**关键词:**传感器网络; 密钥管理; 随机密钥分配; 多重单向散列

**中图分类号:** TP309.7; TP393.08 **文献标识码:** A

## Multiple one-way hash random key pre-distribution protocol in sensor networks

LI Zhi-jun, GENG Ji, WANG Jia-hao, QIN Zhi-guang

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan 610054, China)

**Abstract:** Firstly, a basic multiple one-way hash key distribution protocol was developed based on Leighton Micali protocol. It ensures that all neighbors' nodes can establish secure links, but has poor safety performance. Then a novel key distribution protocol integrating multiple one-way hash with random key pre-distribution was presented. Only one-way hash function is requirement for sensor node, which is very suitable for sensor networks. Compared with other protocols, this one has better performance, which need less computing overhead and can enhance the security.

**Key words:** sensor networks; key management; random key distribution; multiple one-way hash

### 1 无线传感器网络的特点与性能评价

密钥分配协议对于无线传感器网络(Wireless Sensor Networks, 以下简称传感器网络)的安全起着基础性作用。由于传感器网络资源非常受限且容易被物理捕获,传统的基于公钥和可信任的密钥分配中心等方式不能有效应用到传感器网络。近年相关研究主要集中在基于随机图论的随机密钥预分配协议。

#### 1.1 传感器网络特点

传感器网络与传统网络相比,有其鲜明的特点。这些特点对于传感器网络的密钥分配协议提出了相应的挑战:

(1) 通信能力有限,节点只是与邻居节点直接通信,典型的是以多跳的方式进行通信。同时为了优化网络性能,往往采用很多技术在支持数据融合等网络内处理。为此,针对传感器网络特点,文献[1]提出了一种通用的层次密钥体系,每个节点保存以下四类密码:个体密码(此节点与基站的单独密钥),群密钥(所有传感器节点共享的密钥),簇密钥(此节点与它的所有邻居节点共享的密钥)和对偶密钥(此节点与它每一个邻居节点的单独密钥)。个体密钥预先产生,簇密钥利用对偶密钥产生和更新,群密钥利用簇密钥产生和更新。所以关键就是建立和更新对偶密钥。本文主要阐述的就是对偶密钥的分配协议。

(2) 电源能力极其有限。网络中的传感器由于电源能量的原因经常失效或废弃,所以为了保证传感器网络的有效性,密钥分配协议不能增加太多的电源消耗。传感器传输信息要比

执行计算更消耗电能,传感器传输 1 位信息所需要的电源足以执行 3000 条计算指令<sup>[2]</sup>,所以密钥分配协议要尽量优化,减少数据的传输。这使得基于可信任的密钥分配中心的密钥分配协议(例如 Kerberos 协议等)不实用。

(3) 计算能力、存储器非常受限。这使得传统的基于公钥密码体系的密钥分配协议(例如 Diffie-Hellman 协议)不能有效地应用于传感器网络中。

(4) 传感器节点数量大,分布广泛,所以主要依靠各个节点自组织来完成密钥分配。

#### 1.2 性能评价

密钥分配协议的性能直接影响其可用性,我们提出几个传感器网络条件下评价其性能的标准:

(1) 能源性能。能源消耗主要由协议所需的计算量和通信量组成。

(2) 安全性能,即节点捕获的免疫能力。由于传感器网络布置在检测区域,敌人可轻易捕获传感器节点,传感器网络安全协议的一个重要假设就是敌人可以监控传感器节点所有的通信,然后可以捕获一些节点,并可以提取出它所捕获节点的全部信息(包括密钥),再利用这些信息来推导出其他剩余安全链路的密钥。虽然可以采用一些技术来抵御节点信息提取,但是成本很高,而单个传感器节点要求成本非常低廉,所以在传感器网络中没有什么实用性。

毫无疑问,被捕获节点所建立的链路均不再安全。如果剩下未捕获节点之间安全链路的对偶密钥被敌人用捕获的信息推导出来,我们称它被破解。对于密钥分配协议,一个关键

收稿日期:2006-02-13 基金项目:国家自然科学基金资助项目(60473090)

作者简介:李志军(1977-),男,安徽宿松人,博士研究生,主要研究方向:传感器网络与 Ad Hoc 网络安全;耿技(1963-),男,安徽合肥人,副教授,博士研究生,主要研究方向:分布并行处理与计算机操作系统;王佳昊(1978-),男,河北陇尧人,博士研究生,主要研究方向:计算机安全与传感器网络;秦志光(1956-),男,四川隆昌人,教授,博士生导师,主要研究方向:网络与信息系统安全,群件技术。

的安全性能指标就是这些被捕获节点泄漏的信息对于其他未捕获节点之间安全链路的影响,我们称之为节点捕获的免疫能力。安全链路被破解的概率越低,协议对节点捕获的免疫能力越好。

### 1.3 相关协议

在节点部署之前,由离线的服务器将密钥或者能产生密钥的信息预先配置在节点中,这种密钥管理的方法叫做预分配密钥管理。当前主要的传感器密钥分配协议都可以认为属于预分配密钥管理协议,传感器各个节点之间利用预先保存在其节点的秘密信息,自组织、分布式建立密钥。由于节点存储和能量的限制,预分配密钥管理协议必须考虑节省存储空间和减少通信开销。

最简单的密钥分配协议就是所有传感器节点共享一个密钥,但是如果一个节点被捕获并取出密码,安全将不复存在。最安全的密钥分配协议是预先给每两个节点生成一个对偶密钥,把这些密钥保存在节点中,但是由于网络规模巨大,节点存储器非常受限,每个节点需保存  $n-1$  个密钥,可扩展性非常差,只能用于小规模网络。文献[3]引入随机图理论<sup>[4]</sup>,提出了基本的随机密钥预分配协议(简称 EG 协议),在布置之前每个节点从一个大的密钥池中选取少数的密钥保存在存储器中,节点布置好后只要两个邻居节点至少共享一个密钥,就采用这个密钥作为对偶密钥。文献[5]在 EG 协议基础上,提出了  $q$  复合模式和多路增强模式,在一定条件下,有效地改进了 EG 协议安全性能:如果敌人捕获很少的节点,  $q$  复合模式体现出更好的安全性能,但是随着被捕获节点的增多,  $q$  越大,性能反而变差;多路增强以额外的通信负载为代价,较好地提高了安全性能。在 EG 协议基础上,文献[6]结合 Blom 协议,文献[7]结合 Blundo 的多项式密钥分配,分别提出两种非常类似的多重空间密钥预分配协议。但是这两种协议都需要大素数的模余运算,对节点要求高,计算负载很大。

## 2 符号约定

为了清晰地说明相关协议和算法,我们给出本文所用主要英文符号的含义:

$n$ : 传感器网络大小,即全部节点数;

$n'$ : 单个节点的邻居节点数;

$d$ : 单个节点的所有邻居节点中建立安全链路的节点数;

$m$ : 单个节点用于密钥的存储器限制;

$P_r$ : 随机密钥分配时的全网互连度;

$P_{low}$ : 邻居节点建立安全链路概率下限值;

$P_{est}$ : 邻居节点能建立安全链路的实际概率;

$q$ :  $q$  重合模式中的  $q$ ;

$t$ : 散列度;

$u, v$ : 传感器节点 ID, 用来代表单个节点;

$x \parallel y$ : 代表串  $x$  与串  $y$  的串接;

$K_w$ : 节点  $u, v$  通过协议建立的对偶密钥;

$S$ : 源密钥池,即全部源密钥的集合;同时用它表示源密钥池的大小;

$H$ : 单向散列函数。

## 3 多重单向散列密钥分配协议

文献[8]提出了三种不采用公钥体系的密钥分配协议,分别简称为 LM-1、LM-2、LM-3。LM-1 协议每个节点的存储器

消耗为  $O(B^2 \log(n))$  到  $O(B^3 \log(n))$  之间,  $n$  为网络规模,  $B$  为最大非法用户数量,存储要求非常大; LM-2 要求节点能抵御节点捕获; LM-3 协议依靠在线的可靠服务器,基本思想非常类似于 Needham-Schroeder 协议。所以它们都不能有效地应用于传感器网络。我们采用其中的多重单向散列建立密钥的思想,首先设计一种基本的多重单向散列密钥协议(简称 MH 协议)应用到传感器网络中,并研究其性能。

### 3.1 协议算法

由离线的服务器产生  $m$  个公共的原始密钥  $(X_1, X_2, \dots, X_m)$ , 我们定义这些密钥为源密钥。对于每一个节点,在布置之前,产生  $m$  个随机数  $(\alpha_1, \alpha_2, \dots, \alpha_m)$ , 取值范围为  $[0, t-1]$ ,  $t$  定义为散列度,把这些随机数  $\alpha_i$  定义为散列种子;然后分别计算出  $m$  个  $Y_i = H^{\alpha_i}(X_i)$ , 这些  $Y_i$  定义为散列密钥。将每一个节点独立的  $m$  个散列种子及对应的散列密钥保存在节点的存储器中。这里  $H$  代表单向散列函数,  $H^{\alpha_i}(X_i)$  代表对  $X$  连续进行  $\alpha_i$  次单向散列操作:

$$H^{\alpha_i}(X) = \overbrace{H(\dots H(H(X)) \dots)}^{\alpha_i}$$

节点布置好后,通过以下方式建立各个邻居节点之间的对偶密钥:假设节点  $u$  的散列种子为  $(\alpha_1, \alpha_2, \dots, \alpha_m)$  及对应散列密钥为  $(Y_1, Y_2, \dots, Y_m)$ , 节点  $v$  的散列种子为  $(\beta_1, \beta_2, \dots, \beta_m)$ , 每个节点通过明文广播它的全部散列种子,则  $u$  可以计算出它与  $v$  的对偶密钥:

$$K_w = H(H^{\delta_1}(Y_1) \parallel H^{\delta_2}(Y_2) \parallel \dots \parallel H^{\delta_m}(Y_m))$$

其中:

$$s_i = \begin{cases} 0 & \text{当 } \alpha_i \geq \beta_i \\ \beta_i - \alpha_i & \text{当 } \alpha_i < \beta_i \end{cases} \quad i = 1, 2, \dots, m$$

也就是:

$$K_w = H(H^{\delta_1}(X_1) \parallel H^{\delta_2}(X_2) \parallel \dots \parallel H^{\delta_m}(X_m))$$

其中,  $\delta_i = \max(\alpha_i, \beta_i)$ ,  $i = 1, 2, \dots, m$ 。

同样的,节点  $v$  也可以计算出  $K_w$ , 并等于  $K_w$ 。

可以采用伪随机数函数,减少存储需求及通信负载,提高协议性能。每个节点使用它的 ID 作为伪随机数函数的种子,连续产生  $m$  个数,模  $t$ , 作为它的散列种子  $(\alpha_1, \alpha_2, \dots, \alpha_m)$ , 这样在节点布置好后,无需再明文广播,只要知道邻居节点的 ID, 就可以计算出对偶密钥。

### 3.2 安全性能分析

假设有  $x$  个节点被敌人捕获并提出其中信息,而对于剩余的任一个假设为节点  $u, v$  间的安全链路,它们的散列种子分别为  $(\alpha_1, \alpha_2, \dots, \alpha_m)$ 、 $(\beta_1, \beta_2, \dots, \beta_m)$ , 对于每一对  $\langle \alpha_i, \beta_i \rangle$ , 由于单向散列函数的单向性,只要所有被捕获的节点中有一个对应编号的散列种子  $\gamma_i$  且满足  $\gamma_i \leq \max(\alpha_i, \beta_i)$ , 则由这一对  $\langle \alpha_i, \beta_i \rangle$  所决定的秘密信息  $H^{\max(\alpha_i, \beta_i)}(K_i)$  将暴露,我们就称这一对  $\langle \alpha_i, \beta_i \rangle$  被破解;当所有  $m$  对  $\langle \alpha_i, \beta_i \rangle$  都被破解,敌人就能计算出它们的对偶密钥  $K_w$ , 安全链路被破解。

对于两个取值范围为  $[0, t-1]$  的随机整数  $\alpha_i$  与  $\gamma_i$ ,  $\gamma_i > \alpha_i$  的概率为:  $\sum_{i=0}^{t-1} \frac{1}{t} \sum_{j=i+1}^{t-1} \frac{1}{t} = \frac{t-1}{2t}$ , 则任意一对  $\langle \alpha_i, \beta_i \rangle$  不被破解的概率为  $\left(\frac{t-1}{2t}\right)^{2x}$ , 它被破解的概率就为  $1 - \left(\frac{t-1}{2t}\right)^{2x}$ 。所以 MH 协议安全链路被破解的概率为:

$$P_{MH\_BeCracked} = \left(1 - \left(\frac{t-1}{2t}\right)^{2x}\right)^m \quad (1)$$

MH 协议在不同  $m, t$  的安全性能如图 1 所示。由图 1 可以看出, MH 协议的安全性能比较差, 当被捕获节点达到并超过 8 个时, 基本上绝大部分安全链路被破解。同时可以看出, 取大的  $t$  没有太大意义, 不会增强多少安全性能, 反而大大提高了计算负载。但是此协议的研究为后面性能良好的多重散列随机密钥预分配协议打下了基础。

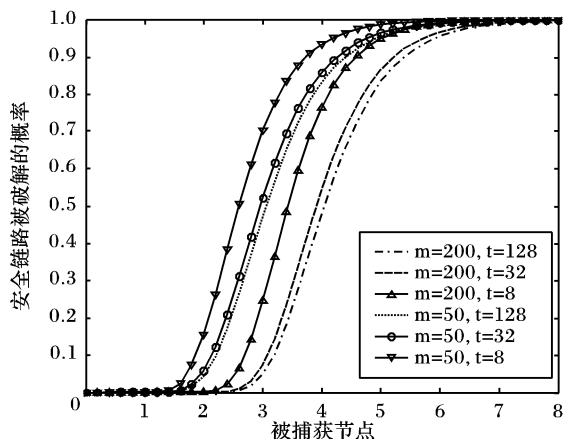


图 1 多重散列密钥分配协议安全性能

#### 4 多重单向散列随机密钥预分配协议

为提高对节点捕获的免疫能力, 提出了一种新的多重单向散列随机密钥预分配协议 (简称 HR 协议)。前面 MH 协议保证所有邻居节点之间能计算出对偶密钥, 建立安全链路, 但是这样导致敌人只需捕获很少的节点, 就可以破解绝大多数安全链路。根据随机图理论<sup>[4]</sup>, 对于一个随机图  $G(n, P_r)$ ,  $n$  是节点总数, 如果要保证全图互连度  $P_r$  为一个很高的值 (比如 0.9999), 每个节点无需确保跟它的所有邻居节点建立安全链路, 而只需要以不低于  $P_{low}$  的概率能建立安全链路, 通过其他多跳安全路径来建立与其他邻居节点的间接对偶密钥。根据此理论, 结合多重单向散列思想, 我们设计了性能良好的多重单向散列随机密钥预分配协议。

##### 4.1 协议内容

###### 4.1.1 密钥初始化

离线的服务器产生一个全局的非常大的源密钥池  $S$ , 每一个源密钥都有其编号。

在每一个节点布置之前, 由离线的服务器对节点进行密钥初始化: 假设节点其编号为  $u$ , 首先生成  $m$  个随机数 ( $u_1, u_2, \dots, u_m$ ) 作为源密钥编号, 对应的从密钥池  $S$  中选取  $m$  个源密钥 ( $K_{u_1}, K_{u_2}, \dots, K_{u_m}$ ), 并类似 MH 协议, 再产生  $m$  个随机数 ( $\alpha_{u_1}, \alpha_{u_2}, \dots, \alpha_{u_m}$ ) 作为散列种子, 取值范围为  $[0, t-1]$ ,  $t$  为散列度, 然后分别计算出  $m$  个对应的散列密钥  $Y_{u_i} = H^{\alpha_{u_i}}(K_{u_i})$  ( $i = 1, \dots, m$ )。把它的  $m$  个源密钥编号、对应的散列种子以及散列密钥保存在其存储器中。这里  $m \ll S$ 。源密钥编号和散列种子的随机性必须独立无关。

###### 4.1.2 安全链路建立

当传感器节点被布置到目标区域后, 各个节点与它的每一个邻居节点通过共享源密钥发现, 来确定它们是否共享至少一个源密钥编号; 如果是, 它们就可以利用其中编号最小的源密钥, 通过类似 MH 协议的方式, 建立它们的对偶密钥, 我们就称之为它们之间建立了安全链路。例如, 假设节点  $u, v$  共享的最小源密钥编号为  $j$ , 对应散列种子对为  $\langle \alpha_j, \beta_j \rangle$ , 则它

们互相向对方传输自己的散列种子, 利用各自的散列种子和散列密钥, 最后都可以计算出它们的共享密钥为  $K_{uv} = H^{\max(\alpha_j, \beta_j)}(K_j)$ ; 其中一个节点需进行  $|\alpha_j - \beta_j|$  次散列运算, 另一节点无需进行任何散列运算。

这种共享源密钥发现可以通过每个节点以明文的形式广播自己的全部源密钥编号实现。为尽量节约通信消耗, 文献 [9] 提出可以利用伪随机数函数提高能源性能。每个节点使用它的 ID 作为伪随机数函数的种子, 产生  $m$  个源密钥编号, 这样在邻居节点只要知道对方的 ID, 就可以确定是否共享源密钥。同 MH 类似,  $m$  个散列种子也可以通过伪随机数函数产生, 但是这两个随机数函数必须不同并且无关, 才能真正保证这些随机事件的独立性。

可以采用类似于文献 [5] 的  $q$  复合方案来改进协议安全性能。与上述基本模式相比,  $q$  复合 (简记为 QC) 有两点不同:

(1) 节点间必须至少共享  $q$  个源密钥编号才能建立安全链路,  $q$  的具体取值由应用环境决定。当敌人捕获的节点比较少时, 此特性加大了敌人破解剩余安全链路的难度; 但是随着被捕获节点的增多, 反而安全性能变差, 而且  $q$  越大, 性能越差。

(2) 如果两个邻居节点  $u, v$  之间实际共享的源密钥编号数量  $j$  不少于  $q$ , 对应的源密钥编号为  $(R_1, \dots, R_j)$ , 散列种子对为  $(\langle \alpha_{R_1}, \beta_{R_1} \rangle, \dots, \langle \alpha_{R_j}, \beta_{R_j} \rangle)$ , 则采用它们之间所有的源密钥来通过多重单向散列, 建立对偶密钥  $K_{uv} = H(H^{\max(\alpha_{R_1}, \beta_{R_1})}(K_{R_1}) \parallel \dots \parallel H^{\max(\alpha_{R_j}, \beta_{R_j})}(K_{R_j}))$ 。此特性以很小的计算负载为代价, 始终提高节点捕获的免疫能力。

我们把前面的叫 HR 协议基本模式, 而把采用  $q$  复合方案的称为 HR 协议  $q$  复合模式。

###### 4.1.3 间接对偶密钥建立

通过前一阶段, 绝大多数节点通过安全链路组成了一个安全连接图  $G_{sec}$ 。对于未能直接建立对偶密钥的邻居节点  $u, v$ , 利用传感器网络的相关路由协议, 可以在安全连接图  $G_{sec}$  内找到至少一条多跳的安全路径  $SecPath_{uv}$ , 节点  $u$  产生一个随机数  $K_{uv}$ , 利用安全路径  $SecPath_{uv}$  传输到  $v$ , 就可以  $K_{uv}$  用作为它们的对偶密钥。

##### 4.2 协议参数

###### 4.2.1 安全链路需求

根据文献 [3], 对于一个有  $n$  个节点的网络, 要保证全网的互连度为  $P_r$ , 需要每个节点必须保证有  $d$  个邻居节点可以建立安全链路:

$$d = \left( \frac{n-1}{n} \right) (\ln(N) - \ln(-\ln(P_r))) \quad (2)$$

$d$  与  $n$  以及  $P_r$  的关系如图 2 所示。

###### 4.2.2 概率要求

假设每个传感器节点有  $n'$  个邻居节点, 为保证能建立  $d$  个安全链路, 那么必须保证任意两个传感器节点之间以不低于概率  $P_{low} = \frac{d}{n'}$  建立安全链路。

假设密钥池总共有  $S$  个源密钥, 每个节点从中随机选  $m$  个源密钥, 则任意两个节点之间恰好共享  $i$  个 ( $m \geq i \geq 0$ ) 源密钥编号的概率为:

$$P(i) = \frac{\binom{S}{i} \binom{S-i}{2(m-i)} \binom{2(m-i)}{m-i}}{\binom{S}{m}^2} \quad (3)$$

用  $P_{est}$  表示两个节点之间能建立安全链路的概率,则  $P_{est}$  等于 1 减去两个节点共享不超过  $q-1$  个源密钥编号的概率:

$$P_{est} = 1 - p(0) - p(1) - \dots - p(q-1) \quad (4)$$

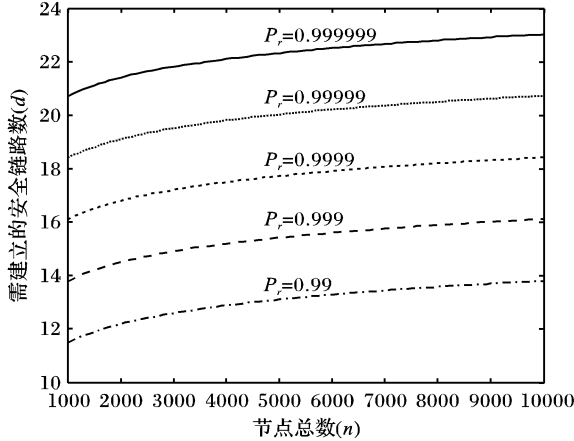


图2 不同网络规模、互连度下的安全链路需求

#### 4.2.3 参数计算

$n, n'$  等由传感器网络的特性决定,而  $P_r$  由设计者选择,然后计算出  $d, P_{low}$ ;  $m$  由节点硬件限制决定,最后选取最大的  $S$  满足  $P_{est} \geq P_{low}$ 。例如,假设有 10000 个节点的传感器网络,需要达到  $P_r = 0.9999$  的全网互连度,则  $d = 18.42$ ;假设  $n'$  为 40,则  $P_{low}$  为 0.4605;假设受硬件限制  $m$  为 200。对于 HR 协议基本模式以及  $q = 1$  模式,计算出  $S$  为 65017;  $q = 2$  模式时,  $S = 25789$ ;  $q = 3$  模式时,  $S = 15933$ 。

#### 4.3 性能分析

假设敌人随机的捕获  $x$  个节点并提出其中信息,用剩余安全链路被破解的概率来衡量安全性能。用节点建立一次安全链路所需的散列运算次数来衡量 HR 协议的计算负载。不失一般性,假设要破解的是任选的节点  $u, v$  之间的安全链路。

##### 4.3.1 HR 协议基本模式

在 HR 协议基本模式下,节点  $u, v$  共享的最小源密钥编号为  $j$ ,对应的散列种子对为  $\langle \alpha_j, \beta_j \rangle$ ,则它们的对偶密钥为  $K_w = H^{\max(\alpha_j, \beta_j)}(K_j)$ 。

敌人要破解此安全链路必须同时满足:首先被捕获的  $x$  个节点中包含  $i$  个编号为  $j$  的源密钥编号,  $i$  肯定不大于  $x$ ,要求  $i \geq 1$ ;其次这  $i$  个的随机数种子中至少有一个不大于  $\max(\alpha_j, \beta_j)$ 。

被捕获的  $x$  个节点中恰好有  $i$  个节点包含编号为  $j$  的源密钥编号的概率为:

$$\binom{x}{i} \left(\frac{m}{S}\right)^i \left(1 - \frac{m}{S}\right)^{x-i} \quad (5)$$

由前面 MH 协议性能分析可知,  $i$  个随机数种子中至少有一个不大于  $\max(\alpha_j, \beta_j)$  的概率为  $1 - \left(\frac{t-1}{2t}\right)^{2i}$ 。

HR 协议基本模式,安全链路被破解的概率:

$$P_{HR\_BeCracked} = \sum_{i=1}^x \binom{x}{i} \left(\frac{m}{S}\right)^i \left(1 - \frac{m}{S}\right)^{x-i} \left(1 - \left(\frac{t-1}{2t}\right)^{2i}\right) \quad (6)$$

$\alpha_j, \beta_j$  取值范围为  $[0, t-1]$  之间的所有整数,每一种取值

的概率为  $\frac{1}{t}$ 。为建立它与节点  $v$  的对偶密钥,只有当  $\beta_j > \alpha_j$  时,节点  $u$  才需要进行  $\beta_j - \alpha_j$  次散列运算。

HR 协议基本模式的计算负载为:

$$Q_{HR\_Hash}(t) = \sum_{i=0}^{t-1} \frac{1}{t} \sum_{j=i+1}^{t-1} \frac{1}{t} (j-i) = \frac{t^2-1}{6t} \quad (7)$$

##### 4.3.2 HR 协议 $q$ 复合模式

对于 HR 协议  $q$  复合模式,节点  $u, v$  共享  $i$  个源密钥编号,这里  $i$  的取值范围为  $[q, m]$  之间的所有整数,取一个具体  $i$  值的概率为  $\frac{p(i)}{P_{est}}$ 。对于每一个  $i$  的具体取值,只有当所有  $i$  对散列种子都被破解,安全链路才会被破解。一对随机的散列种子破解的概率正好就是以上计算出的 HR 协议基本模式安全链路被破解概率  $P_{HR\_BeCracked}$ ;由于这  $i$  对散列种子都是独立的,所以所有  $i$  对散列种子都被破解的概率为  $(P_{HR\_BeCracked}(x, m, S, t))^i$ 。

由以上分析,可以计算出 HR 协议  $q$  复合模式安全链路被破解的概率:

$$P_{HR\_BeCracked} = \sum_{i=q}^m (P_{LQW\_BeCracked}(x, m, S, t))^i \frac{p(i)}{P_{est}} \quad (8)$$

对于每一个  $i$  的具体取值,对于节点  $u$ ,为计算出对偶密钥,需进行  $O_{HR\_Hash}(t) * i$  次散列运算。所以 HR 协议  $q$  复合模式计算负载:

$$O_{HR\_QC\_Hash} = \sum_{i=q}^m O_{LQW\_Hash}(t) * i * \frac{p(i)}{P_{est}} \quad (9)$$

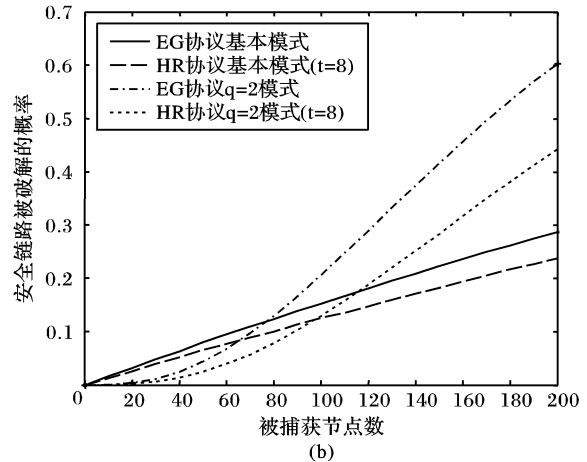
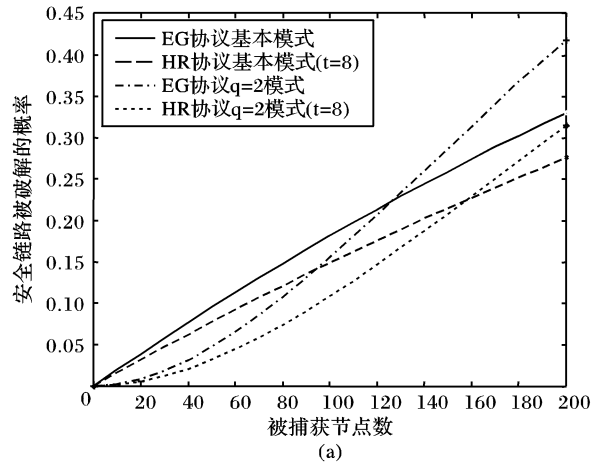


图3 HR 协议与 EG 协议安全性能比较 ( $m = 200, P_{low} = 0.33$ )

##### 4.3.3 性能比较

我们在相同条件下比较 HR 协议与 EG 协议的安全性能:节点有相同的密钥存储器限制  $m$ ;要求各个节点间能按照相

同的概率  $P_{low}$  建立安全链路。以  $m = 200, P_{low} = 0.33$  为例, 其安全性能比较如图 3 所示。HR 协议在不同散列度下的计算负载如图 4 所示。

由图 3、图 4 可以看出, 与 EG 协议相比, 只需数次散列运算为代价, HR 协议取得更好的安全性能。在很小的散列度 ( $t = 8$ ) 条件下, 对于基本模式、 $q = 1$ 、 $q = 2$ 、 $q = 3$  模式, 分别平均将安全链路被破解概率降低到 82.3%、81.8%、70.1%、63.2%。各个模式之间, 如果敌人捕获很少的节点,  $q$  复合模式比基本模式表现出更好的安全性能; 但是随着被捕节点的增多,  $q$  越大, 性能越差。这是因为  $q$  越大, 为达到同样的  $P_{low}$ ,  $S$  就越小; 而捕获的节点一多, 就更容易恢复出  $S$  的内容。同时大的  $q$  会增大计算负载。散列度  $t$  越大, 计算负载越大, 但是安全性能只能取得很小的提高。所以综合起来, 取小散列度  $t$  (例如 8) 的 HR 协议  $q = 1$  模式的性能最好。

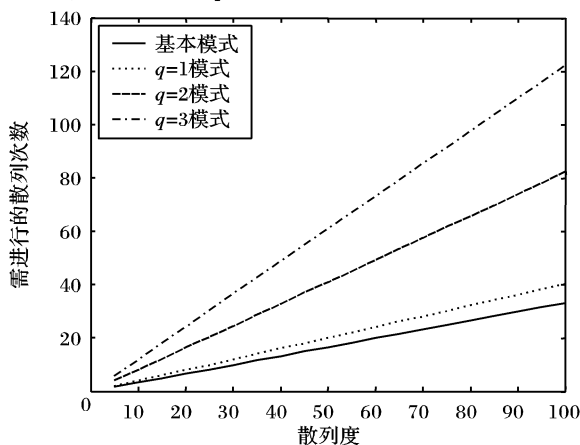


图 4 HR 协议计算负载 ( $m = 200, P_{low} = 0.33$ )

## 5 结语

密钥分配协议是传感器网络安全的热点研究问题。本文主要提出了一种新的多重单向散列随机密钥预分配协议, 只

要求每个节点能进行单向散列操作, 非常适合传感器网络。全面的分析表明, 与现有协议相比, 只需要很小的计算负载为代价, 就可以较好地提高安全性能。

### 参考文献:

- [1] ZHU S, SETIA S, JAJODIA S. LEAP: efficient security mechanisms for large-scale distributed sensor networks [A]. Proceedings of the 10th ACM conference on Computer and Communication Security (CCS'03) [C]. Washington DC, 2003.
- [2] AKYILDIZ IF, SU W, SANKARASUBRAMANIAM Y, et al. A survey on sensor networks [J]. IEEE Communications Magazine, 2002, 40(8): 102 - 114.
- [3] ESCHENAUER L, GLIGOR VD. A key-management scheme for distributed sensor networks [A]. Proceedings of the 9th ACM conference on Computer and Communications Security [C]. Washington, DC, 2002.
- [4] SPENCER J. The Strange Logic of Random Graphs [M]. Number 22 in Algorithms and Combinatorics, Berlin: Springer-Verlag, 2000.
- [5] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks [A]. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy [C]. Berkeley, CA, USA, 2003.
- [6] DU W, DENG J, HAN YS, et al. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks [J]. ACM Transactions on Information and System Security, 2005, 8(2): 228 - 258.
- [7] LIU DG, NING P, LI RF. Establishing Pairwise Keys in Distributed Sensor Networks [J]. ACM Transactions on Information and System Security, 2005, 8(2): 41 - 77.
- [8] LEIGHTON T, MICALI S. Secret-Key Agreement without Public-Key Cryptography [A]. Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology [C]. Santa Barbara, California, USA, 1993.
- [9] ZHU S, XU S, SETIA S, et al. Establishing Pairwise Keys for Secure Communication in Ad Hoc Networks: A Probabilistic Approach [A]. Proceedings of the 11th IEEE International Conference on Network Protocols [C]. 2003.

(上接第 1801 页)

## 5 结语

本文从信息论的角度研究 MIMO 系统各态历经信道容量, 在瑞利平衰落信道下, 当输入为循环对称复高斯向量, 且发射天线采用等功率分配条件, 并假定接收机已知信道状态信息, 而发射机未知时, MIMO 系统信道容量的公式, 并进行了仿真, 得到了不同信噪比下各态历经信道容量与收发天线间的关系图; 以此为基础, 利用 Laguerre 多项式 ( $L_k^{n-m}(\lambda)$ ) 在  $k = 0$  时的特殊值, 分别详细推导了 SIMO 和 MISO 系统的各态历经信道容量的公式, 当收发天线数为有限数时, SIMO 和 MISO 系统的容量可以表示为有限个指数积分和的形式, 从而弄清楚了对以上两个系统每增加一个接收天线或一个发射天线, 其信道容量增加量的确切数值, 为系统设计提供了理论基础; 对于等收发天线的 MIMO 系统各态历经信道容量, 在小信噪比下, 本文给出了一个比较精确简洁的近似公式, 并介绍了文献 [1] 中大信噪比下的一个近似公式作为补充。大量仿真结果表明, 采用本文给出的三种典型 MIMO 系统的各态历经信道容量公式及近似公式, 其理论计算结果与仿真值比较吻合。

### 参考文献:

- [1] TELATAR IE. Capacity of multi-antenna Gaussian channels [J]. Eu-

ropean Transactions on Telecommunications, 1999, 10(6): 586 - 595.

- [2] DOHLER M, AGHVA H. On the Approximation of MIMO Capacity [J]. IEEE Transactions on Wireless Communications, 2005, 4(1): 30 - 34.
- [3] DOHLER M, AGHVA H. A closed Form Expression of MIMO capacity over Ergodic Narrowband Channels [J]. IEEE Communications Letter, 2004, 8(6): 365 - 367.
- [4] SHIN H, LEE H. Closed-form Formulas for Ergodic Capacity of MIMO Rayleigh Fading Channels [A]. IEEE ICC [C]. 2003. 2996 - 3000.
- [5] SHIN H, LEE JH. On the Capacity of MIMO Wireless Channels [J]. IEICE Transactions on Communications, 2004, E87-B(3).
- [6] ALOUINI M, GOLDSMITH J. Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques [J]. IEEE Transactions on Vehicular Technology, 1999, 48(4).
- [7] KHAN E, HENEGHAN C. A Closed Form Expression for the Ergodic Capacity of MIMO Systems [J]. Информационные Том 5, 2005, (1): 47 - 57.
- [8] 王超, 李治安, 吴德伟, 等. 两种典型的 MIMO 系统信道容量分析与仿真 [J]. 电子学报, 2004, 32(12).