无线传感器网络密钥分配协议研究*)

李志军　秦志光　王佳昊

(电子科技大学计算机科学与工程学院　成都 610054)

摘　要　密钥分配协议对于无线传感器网络的安全起着基础性作用。由于传感器网络大规模、节点资源非常受限、分布式等特点,传统的基于公钥和可信任的密钥分配中心等方式不能实用。本文系统针对传感器网络特点,提出密钥管理协议的需求与性能指标,系统阐述了几种当前比较典型的密钥预分配协议:基于初始信任、随机密钥预分配以及各种改进方案等,分析比较其优缺点,并提出了进一步研究的方向。

关键词　传感器网络,密钥分配,密钥管理,安全协议

Key Distribution Protocols in Sensor Networks

LI Zhi-Jun　QIN Zhi-Guang　WANG Jia-Hao

(Institute of Computer Science and Engineering, UEST of China, Chengdu 610054)

Abstract　Key management is one of the fundamental building blocks of security services. As sensor networks are very resource-constrained and large scale, traditional key management techniques, such as public key cryptography or key distribution center, are often not effective. We discuss the characteristics of sensor networks, and give the performance issues of key distribution protocols. Several key distribution protocols based on initial trust and random graph theory are reviewed. We analyze their performance in especial and give their overhead and payoff. The paper also points out the future research issues.

Keywords　Sensor networks, Key distribution, Key management, Security Protocol

1　引言

无线传感器网络(Wireless Sensor Networks,以下简称传感器网络)通过大规模的各类集成化的微型传感器协作地实时监测、感知和采集各种环境或监测对象的信息,利用嵌入式系统对信息进行处理,并通过自组织无线通信网络以多跳中继方式通讯,集数据采集、处理、通信等能力于一身,是当前国际上备受关注的、由多学科高度交叉的新兴前沿研究热点领域[1]。传感器网络具有十分广阔的应用前景,在军事国防、工农业、城市管理、生物医疗、环境监测、抢险救灾、反恐、危险区域远程控制等许多领域都有重要的科研价值和巨大实用价值,已经引起了世界许多国家军界、学术界和工业界的高度重视。2003 年 2 月,美国麻省理工学院的《技术评论》评出对人类未来生活产生深远影响的十大新兴技术,传感器网络即位于这十种新技术之首[2]。

由于传感器网络在很多关键应用上的应用,如军事、监控系统中,安全成为传感器网络大规模应用前必须解决的问题。为提供机密性、鉴别、完整性等安全特性,实现一个安全的密钥管理协议是前提条件,也是传感器网络安全研究的主要问题。

由于传感器网络的特殊性,传统的密钥交换管理协议(如基于公钥密码体系和可信任的密钥分配中心等)不能有效用在传感器网络上,当前有一系列的协议提出。本文综述传感器网络的主要密钥分配协议,分析其优缺点,给出以后研究的方向。

2　传感器网络特点与密钥分配协议性能评价

2.1　传感器网络特点

传感器网络与传统无线有线网络相比,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)通讯能力有限,节点只是与邻居节点直接通讯,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[3]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)、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。本文主要阐述的也就是对偶密钥的的分配协议。

(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[4],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。

(5)网络动态性大,经常有新的节点加入或者旧的节点失效。

*)国家自然科学基金资助项目(60473090)。**李志军**　博士研究生,主要研究方向:传感器网络与 Ad Hoc 网络安全;**秦志光**　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,**王佳昊**　博士研究生,主要研究方向:计算机安全与传感器网络。

(6)节点往往是随机布置的,很难依靠节点的布置信息来优化密钥分配协议。

2.2 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)能源消耗。能源消耗主要由协议所需的计算量和通讯量组成。

(2)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。我们一个重要假设就是敌人可以监控传感器节点所有的通讯,然后可以捕获一些节点,并可以提出它捕获的节点的全部信息(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。由于单个传感器节点要求成本非常低廉,所以在传感器网络没有什么实用性。而且文[5]表明此技术很不可靠。

毫无疑问,被捕获节点所建立的链路全部不安全了。如果剩下未捕获节点之间的安全链路的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,一个关键性能指标就是这些被捕获节点泄漏的信息对其他未捕获节点之间的安全链路的影响,我们称之为节点捕获的免疫能力。我们用一个二维坐标图来形象化表示此性能,横坐标是敌人捕获的节点数,纵坐标是剩余的任意一个安全连接被破解的概率;对于一个密钥管理协议,相同条件下,安全链路被破解的概率越低,节点捕获的免疫能力越好。

(3)是否防止节点复制、支持鉴别。敌人可以利用捕获的节点伪造出新的节点,进一步破坏传感器网络的功能;支持鉴别是为了可以准确定位传感器节点,发现异常后可以把此节点排除出去。

(4)可扩展性,即密钥协议所支持的最大网络规模以及所需存储器与网络规模的关系。

(5)是否能支持节点的动态加入、多次部署。由于传感器节点可能失效等原因,为保证网络功能,需要多次布置传感器节点;密钥分配协议应该支持节点的多次布置、动态加入。

2.3 预分配密钥管理协议

节点在部署之前,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。

3 符号约定

为了下面清晰地说明相关协议和算法,我们给出所用主要英文符号的含义:

n: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}:要求的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 重合方案中的 q

λ:安全门限阈值

u,v:传感器节点 ID,用来代表单个节点

$u \| v$:代表串 u 与串 v 的串接

K_{uv}:节点 u、v 通过协议建立的对偶密钥

S:密钥池,即全部密钥的集合,同时表示密钥池的大小

H_k:使用密钥 k 的单向散列函数

4 基于初始信任的密钥管理协议

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。Zhu、Setia、Jajodia 等根据传感器网络部署的特点,提出初始信任假设,让传感器网络以自治的方式来建立各个邻居节点之间的对偶密钥[3]。

所谓初始信任,就是认为传感器节点刚开始部署在目标区域附近时,有一个短暂的安全时间 T_{min}(一般为几秒钟),敌人至少要在 T_{min} 时间之后才能捕获传感器节点并提取出其中的密钥信息,而传感器各节点之间建立密钥的时间 T_{est} 要小于 T_{min}。依据此假设,设计了一个密钥分配协议,要求所有节点都有一个公开的带密钥的单向散列函数 H,并共享一个主密钥 K。在节点部署好后,设置定时器 T_{min},同时利用初始化时候的可信任阶段,快速建立各个邻居节点的对偶密钥;所有节点之间的对偶密钥根据主密钥 K 和函数 H 推导出来,例如对于节点 u、v(假设 $u<v$),它们可以通过 $H_{H_K(u)}(v)$ 或者 $H_K(u \| v)$ 来产生相互间的密钥 K_{uv};最后在定时 T_{min},所有节点删除主密钥。这样,只要初始信任假定成立,那么无论后面敌人捕获多少节点,只能得到该被捕获节点与其他邻居节点的对偶密钥。而由于函数 H 的单向性,他无法推出主密钥 K,也就没有办法得到其他未捕获节点相互之间的对偶密钥,故安全性高;同时,建立对偶密钥的时候,无需节点之间进行通讯,能源性能很好。

此协议的主要缺陷是它不支持节点的多次部署。另外,如何选取一个合适的初始密钥生命期 T_{min},对此协议的成败非常关键。可依据具体的应用,对此问题做进一步研究。

文[6]增强了初始信任的密钥管理,支持节点多次部署。它不是所有节点共享一个主密钥,而是所有第 i 次部署的节点共享一个批次主密码 K_i。同次节点之间的对偶密钥建立协议同前。而不同批次节点之间建立对偶密钥,对于前次部署的节点 u,它保存了根据所有后面批次主密钥对它的 ID 值进行单向散列运算的值 $H_{Ki}(u)$,这样它就可以与所有第 i 次部署节点建立对偶密钥,而就算被捕获了也不会泄漏相关信息。以两次为例,假设第一次布置的一个节点 u(保存次初始密钥 K_1 以及 $H_{K_2}(u)$),第二次布置的节点 v(保存次初始密钥 K_2),它们之间可以通过 $H_{H_{K_2}(u)}(v)$ 建立安全的对偶私有密钥。但是有了批次的概念之后,敌人只要捕获一个前次的节点,就可以复制出很多恶意的节点,照样能同后面所有部署的节点建立连接,破坏传感器网络的功能。这是此协议的一个主要缺点。

文[7]依据另一种信任关系提出一种极端的密钥管理协议,它认为由于传感器节点布置的随机性,敌人只能监控很小一部分区域的无线通讯,所以在节点部署的时候,完全可以用明文交换来快速建立对偶密钥。

5 随机密钥预分配协议

5.1 E-G 协议

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。Eschenauer、Gligor 引入随机图理论[8],首先提出了基本的随机密钥预分配协议(以下简

称 E-G 协议)[9],引出后续一系列研究,是当前传感器网络密钥协议的重点研究方向。

根据随机图理论,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。

E-G 协议的建立由 3 个阶段构成:

(1)密钥初始化。首先随机产生一个非常大的密钥池 S,每一个密钥都有其编号;对于每一个节点,随机地从密钥池 S 中选取 m 个密钥,保存在其存储器中,$m << S$。

(2)建立安全链路。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密钥发现,来确定它们是否共享至少一个密钥;如果是,它们就可以利用其中编号最小的密钥作为它们的对偶密钥,我们就称之为它们之间建立了安全链路。这种共享密钥发现可以通过每个节点以明文的形式广播自己拥有的全部密钥的编号来实现。如果要更高的安全性,可以通过挑战/应答方式:每一个节点用它的所有密码加密一个挑战随机数 a,并广播出去,而邻居节点用自己所有的密钥来尝试解密这些广播数据。如果能解密出 a,就确认双方共享此密钥。但是这样加解密的计算消耗比较大。

(3)建立间接对偶密钥。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。前一阶段只能保证一定比例的邻居节点之间能建立对偶密钥,其他的邻居节点之间可以通过这个安全连接图,找到一条安全路径,通过它建立相互的对偶密钥。

根据随机图理论,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:

$$d=(\frac{n-1}{n})[\ln(N)-\ln(-\ln(P_r)]$$

d 与 n 以及 Pr 的关系如图 1 所示。

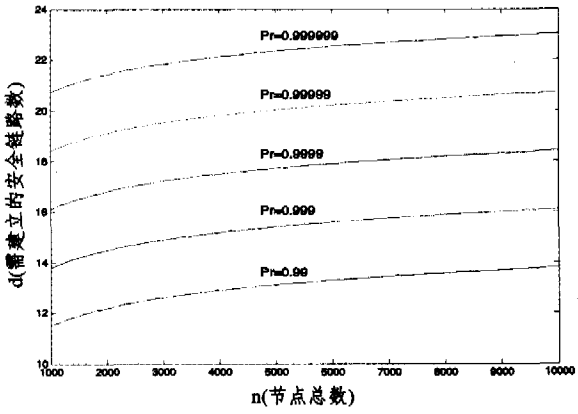

图 1 不同网络规模、互连度下的安全链路需求

假设每个传感器节点的有 n' 个邻居节点,为保证能建立 d 个安全链路,必须保证任意两个传感器节点之间以不低于概率 $P_{low}=\frac{d}{n'}$ 的可能至少共享一个随机密钥。

假设密钥池总共有 S 个密钥,每个节点从中随机选 m 个密钥,则任意两个节点至少共享一个密钥的概率为:

$$P_{est}=1-\frac{((S-m)!)^2}{S!\ (S-2m)!}\approx 1-\frac{(1-\frac{m}{S})^{2(S-m+0.5)}}{(1-\frac{2m}{S})^{(S-2m+0.5)}}$$

此式采用阶乘的简化公式,当 n 非常大的时,$n!\approx\sqrt{2\pi}\,n^{n+\frac{1}{2}}e^{-n}$。

参数的选取: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 $P_{est}\geqslant P_{low}$。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,选取最大的 S,满足 $P_{est}\geqslant P_{low}$,计算出 S 为 65017。

5.2 性能改进

各个协议在相同条件下来比较其安全性能: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。

5.2.1 q 复合模式

Chan、Perrig、Song 在 E-G 协议基础上,提出了 q 复合模式、多路增强模式,以一定代价有效地改进 E-G 协议安全性能[10]。q 复合模式[10]主要对共享密钥发现有两点改进:要求节点间必须至少共享 q 个密钥才能建立安全链路;如果不少于 q,则采用它们之间所有的密钥来建立对偶密钥。

任意两个节点之间恰好共享 i 个密钥的概率为:

$$p(i)=\frac{\binom{S}{i}\binom{S-i}{2(m-i)}\binom{2(m-i)}{m-i}}{\binom{S}{m}^2}$$

对于 q 复合模式,则两个节点之间能建立安全链路的概率为:

$$P_{est}=1-p(0)-p(1)-\cdots-p(q-1)$$

参数的选取:对于给定的 m、P_{low},我们选取最大的 S,使计算出的 $P_{est}\geqslant P_{low}$。例如,假定 $P_{low}=0.33$、$m=200$,E-G 协议与 $q=1$ 模式下,$S=100080$;$q=2$ 时,$S=33938$;$q=3$ 时,$S=19758$。很显然,q 越大,S 越小。

安全性能比较:

对于 E-G 协议,安全链路被破解的概率为(x 为被捕获节点数):

$$p_{EG\_BeCracked}=1-(1-\frac{m}{S})^x$$

对于 q 复合模式,安全链路被破解的概率为:

$$p_{QC\_BeCracked}=\sum_{i=q}^{m}(1-(1-\frac{m}{S})^x)^i\frac{p(i)}{P_{est}}$$

其性能比较如图 2 所示。

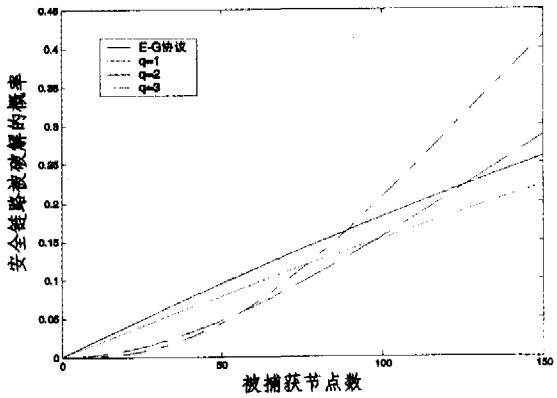

图 2 q 复合模式的安全性能比较($m=200$, $P_{low}=0.33$)

分析: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。$q=1$ 与 E-G 协议差不多，但是安全性能始终要好一些，这是因为 E-G 协议只用一个共享密钥来建立安全链路，而 q 复合模式用全部共享密钥来建立安全链路。q 复合模式以额外的计算负载为代价，提高安全性能，但是只适合只有少数节点被捕获的场合。

5.2.2 多路增强

多路增强[10]与文[11]提出的秘密共享密钥建立协议的主要思想基本相同。E-G 协议是两个邻居节点通过 1-hop(也就是直接通讯)进行共享密钥发现，但是在这两个节点之间存在着多条多跳路径互连，可以利用这些路径来加强安全性。假设两个节点 u、v 已经通过共享密钥发现阶段建立直接密钥 K_{direct}，同时它们之间有 j 个互相独立的路径(就是相互之间没有公共的安全链路)，u 随机产生 j 个随机数 $R_1, R_2, \cdots, R_j$，分别通过 j 个独立路径传送到节点 v。最终两节点的对偶密钥为 $K_{uv}=K_{direct}\oplus R_1\oplus R_2\oplus\cdots\oplus R_j$。这样，敌人必须得到所有 $j+1$ 个数据，才能破解此安全链路。

但是，如何在两个节点之间找到 j 条多跳的互相独立的路径，是 NP 完全问题。比较实用的是 2-hop 的情况，也就是通过一个邻居节点来增强安全性，实现非常方便。

假设原始模式下，任意一个安全链路被破解的概率为 p，两个节点间存在着 a 条 2-hop 安全路径，则 2-hop 多路增强后，安全链路被破解的概率为：

$$p'=p(2p-p^2)^a$$

文[10]计算出平均有 0.5865 $\frac{d^2}{n}$ 个 2-hop 节点可以用于多路增强。假设 $d=20, n'=60(P_{low}=0.33)$，则 $a=3.83$。2-hop 多路增强安全性能对比如图 3 所示。

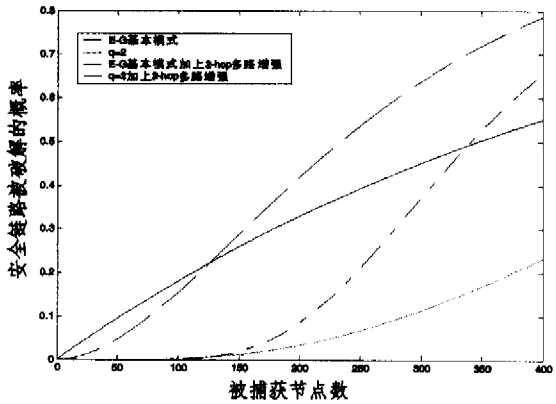

图 3 多路增强安全性能比较($m=200, d=20, n'=60$)

分析：多路增强以额外的通讯负载为代价，比较好地提高了安全性能。由图 3 看出，安全性能最好的是 E-G 协议加上多路增强。同时采用 q 复合与多路增强，反而降低安全性能。这是因为在较少节点被捕获的情况下，多路增强起的作用与 q 复合模式基本相同，再加上 q 复合也不能增强安全性能；而当被捕获节点增多时，q 复合模式导致更小的密钥池，反而降低了安全性能。

5.2.3 共享密钥发现

共享密钥如何发现，对于随机密钥预分配协议的性能是一种影响因素。文[11]提出可以利用伪随机数函数来提高共享密钥发现阶段能源性能，降低通讯消耗。每个节点使用它的 ID 作为伪随机数函数的种子，产生 m 个密钥编号，把相应的密钥保存到存储器中。这样，在共享密钥发现阶段，无需广播每个节点的所有密钥编号，只需要知道邻居节点的编号，就可以计算出相互间拥有多少共同的密钥，能源性能好。

前面提出的节点捕获攻击是假设敌人随机捕获节点的，如果采用上述伪随机数编号或者明文广播密钥编号的方式来进行共享密钥发现，那么敌人可以从中获得有用的信息，有选择地捕获相应的节点，可以更快地推导出全部密钥，大大提高其他安全链路被破解的概率。而挑战/应答方式可以避免此缺点，但是通讯/计算消耗非常大，能源有效性差。文[12]提出一种密钥产生与共享密钥发现协议，基于伪随机数函数，满足一定约束条件的密钥才能分配到相应节点中，以可用的密钥数降低以及部分节点存储器空间浪费为代价，以接近明文广播密钥编号的能源消耗，实现近似于挑战/应答方式的安全性能。

5.3 缺陷

对于随机密钥预分配协议，由于是从一个公共的密钥池来选取密钥，所以节点间的对偶密钥并不为其私有，不能采用这些对偶密钥作为鉴别用。同时，由于安全链路被破解的概率只与被捕获的节点数有关，而与网络规模无关，一定数量的节点被捕获将导致一定比例的安全链路被破解，那么对于大规模的传感器网络就非常不利。假设 $n=100000, m=200$，$P_{low}=0.33$，被捕获 0.1%(100 个)的节点，以 E-G 协议基本模式为例，将导致剩余的 18.13%安全链路被破解，差异达到 100 多倍。

针对这些缺陷，文[10]还提出了成对密钥分配协议，不是从一个公共的密钥池取，而是对于每个节点随机地生成与其他 m 个节点相对应的 m 个密钥，每一个密钥只为两个节点所私有。这样，安全性能非常好，捕获节点不会影响其他的安全链路。但是，为保证邻居节点之间不低于 p_t 概率建立安全链路，传感器网络的规模 n 不能大于 $\frac{m}{P_{low}}$。典型的 $m=200, P_{low}=0.33$，则 n 最大为 600，非常不实用，只能用于小规模网络。

6 多重空间密钥预分配协议

本节所有运算都是在有限域 GF(q_{req})内，q_{req} 为大素数。如果密钥都是 64bit，要保证计算安全性，q_{req} 取大于 2^{64} 的最小素数即可。

6.1 Blom 密钥预分配协议

Blom 密钥预分配协议[13]可以使传感器网络中任意两个节点建立私有的对偶密钥，它具有 λ 门限安全特性：只要被捕获的节点不超过 λ 个，则对节点捕获完全免疫；如果超过 λ，则所有安全链路全部被破解。

在节点布置之前，由离线的服务器产生一个 $(\lambda+1)\times n$ 的线性无关矩阵 G 和 $(\lambda+1)\times(\lambda+1)$ 的对称矩阵 D，就是 $D^T=D$。G 是公开的，D 必须保密。计算出 $N\times(\lambda+1)$ 矩阵 $A=(D\cdot G)^T$，定义 $K=A\cdot G$，则有 $K^T=K$，所以 $K_{uv}=K_{vu}$。使用 K_{uv} 作为节点 u、v 的对偶密钥。

为节约节点存储器，在满足 $n<q_{req}$ 的情况下，可以通过一个素数 t 来产生整个线性无关的 G：

$$G=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ t & t^2 & t^3 & \cdots & t^n \\ t^2 & (t^2)^2 & (t^3)^2 & \cdots & (t^n)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t^\lambda & (t^2)^\lambda & (t^3)^\lambda & \cdots & (t^n)^\lambda \end{bmatrix}$$

对于每一个节点 u，只需在存储器中保存矩阵 A 的第 u

行 A_u 与 t，存储器消耗为 $\lambda+2$。

节点布置好后，两个邻居节点 u、v 只需知道对方的 ID，无需额外通讯就可以分别计算出对偶密钥：u 根据 t 计算出 G 的第 v 列，然后就可以计算对偶密钥 $K_{uv}=\sum_{i=1}^{\lambda+1}(A_{ui}\times G_{iv})$；同样 v 可以计算出 $K_{vu}=\sum_{i=1}^{\lambda+1}(A_{vi}\times G_{iu})$。$K_{uv}=K_{vu}$。

只要敌人捕获的节点不超过 λ，就不能恢复出 D，那么也就无法得到安全链路的保密信息，对节点捕获完全免疫。如果超过 λ，就可以通过解方程组算出 D，所有安全链路被破解。

6.2 多重空间密钥预分配协议

Du、Deng 等结合 Blom 协议与 E-G 协议，提出多重空间密钥预分配协议[14]。与 E-G 协议相同，分为 3 个阶段：

在密钥初始化阶段，选取合适的 λ；由离线服务器产生唯一的 G，同样地可以用一个素数 t 生成整个 G，但是产生 ω 个（相当于 E-G 协议中的 S）不同 D^i，定义每一对 $\langle D^i,G\rangle$ 为一个密钥空间；计算出相应的 A^i。对于每一个节点 u，随机从 ω 个密钥空间中选取 τ 个，保存相应的 A^i 中的第 u 行及 t。在安全链路建立阶段，只要两个节点至少选取了一个相同的密钥空间，就可以计算出相应的对偶密钥。λ、ω、τ 为可调的安全参数，受节点存储空间 m 和邻居节点安全链路概率下限值 P_{low} 限制：

$$(\lambda+1)\tau+1\leqslant m;1-\frac{((\omega-\tau)!)^2}{\omega!\ (\omega-2\tau)!}\geqslant P_{low}$$

非常类似于 Blom 协议，Blundo 提出的基于多项式的密钥预分配协议[15]也可以应用于传感器网络，同样有 λ 门限安全特性。在节点布置之前，由离线服务器产生二元多项式 $f(x,y)=\sum_{i,j=0}^{\lambda}a_{ij}x^iy^j$，其中 $a_{ij}=a_{ji}$，所以有 $f(x,y)=f(y,x)$。对于节点 u，在存储器里面保存多项式 $f(u,y)$。当节点布置之后，两个节点 u、v 无需额外通讯，只需分别计算出 $f(u,v)=f(v,u)$，将它作为对偶密钥。

Liu、Ning 结合多项式和 E-G 协议，设计了另外一种多重空间密钥预分配协议[16]。各项性能与 Du-Deng 协议基本一致。

此类协议的安全性能比较好，但是计算消耗比较大。前面各种性能提高方式（如多路增强等）都可以应用到此类协议上，提高相应性能。

7 基于布置信息的密钥分配协议

传感器网络虽然不能准确地获得节点的准确布置信息，但是在有些时候能获得相对的布置信息，可以利用信息来优化密钥分配协议。关键是如何建立准确可靠的节点布置信息模型。文[17]提出一种基于节点布置绝对坐标的模型，假设每个节点有一个目的点，以此点为中心，节点的实际布置点按照一定概率密度函数分布。文[18]提出的是基于节点布置相对位置的模型，认为节点布置是成组的，组内各个节点更有可能成为邻居。以上两模型，结合随机密钥预分配协议，取得了良好的安全性能，这是理所当然的。但关键是这些模型真的符合实际情况吗？就算是，那么取得正确的概率密度函数也是一件非常困难的事情，所以这问题还需要更进一步研究。

结论 密钥分配协议是传感器网络安全的基础。传感器网络的灵活性、容错性、高感知性能、无基础设置、低费用、高灵活性、快速布置等特点决定它的应用领域极为广泛，但正是上述特征使得传统的密钥分配技术不能有效地应用到传感器网络中。我们针对传感器网络特点，提出密钥分配协议的性能指标，归纳和总结了主要的传感器网络密钥分配协议，分析其前提、性能、负载、应用，并对一些可能的改进和研究方向进行了简要阐述。

参 考 文 献

1 任丰原，黄海宁，林闯. 无线传感器网络. 软件学报，2003，14(7)：1282～1291

2 Ten emerging technologies that will change the world. Technology Review，2003，106(1)：22～49

3 Zhu S，Setia S，Jajodia S. LEAP：efficient security mechanisms for large-scale distributed sensor networks. In：Proceedings of the 10th ACM conference on Computer and Communication Security (CCS' 03)，Washington D C，2003

4 Akyildiz I F，Su W，Sankarasubramaniam Y，et al. A survey on sensor networks. IEEE Communications Magazine，2002，40(8)：102～114

5 Anderson R，Kuhn M. Tamper Resistance - a Cautionary Note. In：Proceedings of the Second USENIX Workshop on Electronic Commerce. Oakland，California，1996

6 Dutertre B，Cheung S，Levy J. Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust：[SRI SDL Technical Report SRI-SDL-04-02]. 2004

7 Anderson R，Chan H，Perrig A. Key Infection：Smart Trust for Smart Dust. In：Proceedings of the Network Protocols，12th IEEE International Conference on (ICNP'04)，2004

8 Spencer J. The Strange Logic of Random Graphs. Algorithms and Combinatorics. Springer-Verlag，Vol. 22，2000

9 Eschenauer L，Gligor V D. A key-management scheme for distributed sensor networks. In：Proceedings of the 9th ACM conference on Computer and Communications Security，Washington，DC，USA，2002

10 Chan H，Perrig A，Song D. Random key predistribution schemes for sensor networks. In：Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy，Berkeley，CA，United States，2003

11 Zhu S，Xu S，Setia S，et al. Establishing Pairwise Keys for Secure Communication in Ad Hoc Networks：A Probabilistic Approach. In：Proceedings of the 11th IEEE International Conference on Network Protocols，2003

12 Pietro R D，Mancini L V，Mei A. Efficient and resilient key discovery based on pseudo-random key pre-deployment. In：Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04)，2004

13 Blom R. An optimal class of symmetric key generation systems. In：Proc. of the EUROCRYPT 84 workshop on Advances in cryptology：theory and application of cryptographic techniques，Paris，France，1985

14 Du W，Deng J，Han Y S，et al. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. ACM Transactions on Information and System Security (TISSEC)，2005

15 Blundo C，Santis A D，Herzberg A，et al. Perfectly-Secure Key Distribution for Dynamic Conferences. Information and Computation，1998，164(1)：1～23

16 Liu D，Ning P，Li R. Establishing Pairwise Keys in Distributed Sensor Networks. ACM Transactions on Information and System Security (TISSEC)，2004

17 Liu D，Ning P. LocationBased Pairwise Key Establishments for Static Sensor Networks. In：Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. Fairfax，Virginia，2003

18 Du W，Deng J，Han Y S，et al. A key management scheme for wireless sensor networks using deployment knowledge. In：Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies，2004