无线传感器网络中一种基于公钥的密钥分配方案

黄杰，黄蓓
（东南大学 信息科学与工程学院，江苏 南京 210096）

摘 要：针对基于对称密钥的密钥分配技术无法彻底解决无线传感器网络中密钥分配的安全问题，提出了一种基于公钥的密钥预分配方案，基站利用一系列原始公钥和单向散列函数产生公钥集合，并为每个节点随机分配公私钥对和公钥集合的子集。由于私钥的唯一性，采用该方案不仅能够提高网络的安全性能，而且可以改善网络的存储开销。利用随机图论的相关原理证明，该方案与传统的密钥预分配方案相比，既保证了网络的安全，又兼顾了网络和节点资源有限的实际，在连通性不变的前提下，其网络安全性和网络的扩展性大幅度提高。

关键词：无线传感器网络；公开密钥算法；对称密钥算法；连通性；扩展性
中图分类号：TP393.1 **文献标识码**：A **文章编号**：1000-436X(2011)10-0052-07

Public key based key distribution scheme for wireless sensor networks

HUANG Jie[1,2], HUANG Bei[1]
(School of Information Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: Since key pre-distribution schemes based on symmetric key can not completely solve security problems of keys distribution in WSN, a new public key based key distribution scheme was proposed . In the scheme, public key set was generated by an initial public key set and a hash function in base station. Each sensor device was pre-distributed one public/private pair-wise key from public key set and a public key subset from the initial public keys set. Owing to uniqueness of private key, not only the communication security problems could be improved for WSN. but also the sensor-memory cost could be decreased. With the theorem of random-graph theory, the connectivity and scalability were illustrated. The results showed that the scheme was superior to the traditional key pre-distribution schemes.

Key words: wireless sensor network; asymmetric key algorithm; symmetric key algorithm; connectivity; scalability

1 引言

无线传感器网络（WSN）是由大量体积小、低成本、低功耗、低能量、低容量、可移动，具有通信、感测及计算能力的微型传感器节点通过自组织方式构成的测控网络。WSN 广泛应用于军事、环境监测、农业、医疗卫生、工业、智能交通、建筑物检测和空间探测等领域。

由于 WSN 往往部署在敌战区或无人区，其网络节点和通信链路处于不受保护的开放状态，因此如何保证网络安全和数据安全是直接关系到 WSN 能否被广泛应用的关键技术之一。由于 WSN 中各节点的资源限制，在传统网络中所采用的安全算法、机制和协议不能直接移植到 WSN 中，因此，

收稿日期：2010-09-21；**修回日期**：2011-04-11
基金项目：国家高技术研究发展计划（“863 计划”）基金资助项目（2009AA01Z427）；江苏省产学研联合创新基金项目支持（BY2009149）；信息网络安全公安部重点实验室开放课题
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2009AA01Z427); The Joint Innovation Project for Industry-University-Institute in Jiangsu Province(BY2009149); Key Lab of Information Network Security, Ministry of Public Security

必须研究适合 WSN 特点的安全技术。

与传统的有线网络和无线网络相比，无线传感器网络的安全需求更侧重于以下几个方面。

1) 抗物理攻击。WSN 的节点遭受物理攻击（如：节点捕获）的概率是非常高的，但入侵者无法获悉节点保存的秘密信息，或获取的秘密信息对整个网络的安全性影响尽可能小。

2) 机密性。未授权用户不能访问 WSN 中的信息。由于 WSN 采用无线信道传送数据，入侵者很容易监听到节点之间传输的信息，因此，必须采取相应的措施（如：加密）预防 WSN 中的机密信息被窃听，或者即使被窃听，入侵者也无法了解信息的相关内容。

3) 可认证性。WSN 的链路建立是在传感器节点随机部署之后，因此需要通过认证的方式识别各节点是否属于合法单元，同时进行会话密钥的交换。

4) 可扩展性。WSN 中的节点寿命是有限的（由电池的能量决定），一旦某个节点失效，可以更换新的节点，或者根据应用的需要随时扩大网络的规模，增加新的节点，而保持整个网络的特性不发生改变。

基于以上几点，WSN 的安全机制必须满足以下几个条件。

1) 适度的安全性。由于 WSN 的寿命一般不会太长，因此采用的安全机制只需要在其生命期内有效即可。如：密钥的长度不需要太长。

2) 资源占用率低。采用的安全机制占用的内存资源少，计算量小，计算的复杂度低。

3) 消耗的能量少。对于传感器节点而言，无线传输消耗的能量远远大于内部运算所消耗的能量，以 SPINs 安全协议为例[1]，完成安全协议进行必要的射频收发所消耗的能量超过所有安全机制能耗的 97%，而加密运算所消耗的能量不到 3%，因此必须尽量减少 WSN 初始化阶段节点之间信息交换的次数和时间。

公钥密码系统由于计算复杂度高和计算量大，在密钥分配时需要协议参与，因此大多数学者认为其不适合 WSN。为此，产生了大量以对称密码技术为基础的研究成果[2~7]，但这些成果无法回避的事实是：没有公钥体制的密钥分配无论怎样精密都无法最终解决密钥分配的安全问题。而在基于公钥的 WSN 安全机制的研究方面进展比较缓慢，相关的研究文献也不是很多[8~12]，这些文献一个共同的特点是回避了传感器节点资源有限的问题，认为随着技术的发展，WSN 资源有限的问题将迟早会解决，显然这类研究成果在目前的条件下是没有实用价值的。本文利用随机图论的相关理论，在 WSN 中实现了一种基于公钥的密钥分配方案，在保证节点资源消耗最低的前提下，既解决密钥的安全分配问题，又解决网络的可扩展性问题。

本文的相关内容分配如下：第 2 节对相关的研究工作进行了描述，第 3 节阐述了一种适合于 WSN 的基于公钥的密钥分配方案。该方案中，每个节点随机保存部分原始公钥信息，网络部署后，利用密钥发现机制实现 WSN 的连通，第 4 节分析本方案网络的连通性，利用概率统计的方法证明即使每个节点保存部分原始公钥信息，其网络的连通性也可以达到非常高的水平，从而满足应用的要求，第 5 节分析了网络的可扩展性，即，适当的增加新的节点不会影响网络的安全性，第 6 节是结束语。

2　相关工作

密钥分配与管理是 WSN 关键安全问题之一，由于 WSN 的资源限制，一直以来，基于对称密钥的预分配方案是重点研究内容，并产生了大量标志性的研究成果。

基于对称密钥的预分配方案有两种最直接的策略。一种是主密钥方案[13]，所有节点在部署之前预先分配一个主密钥，节点部署后，任意两节点之间利用主密钥产生会话密钥，实现节点之间的安全通信。这种方案的好处在于节点的存储负担非常小，WSN 资源的消耗小，但显而易见的问题是一旦某个节点被捕获，整个 WSN 网络将受到安全威胁，其安全性能非常差。另一种是对密钥方案，在 n 个节点组成的 WSN 中，每个节点将保存 $n-1$ 个节点的对称密钥，一个节点被捕获，它影响的只是与该节点通信的链路，对其他链路的安全性不构成威胁，但 WSN 规模比较大时，该方案将使节点的内存超载，同时网络没有任何扩展能力。这 2 种方案是对称密钥预分配方案的极端情况，从这 2 种方案可以看出，基于对称密钥的预分配方案必须在网络安全和存储量之间寻求一种平衡。为此产生了 3 种类型的对称密钥预分配方案：随机密钥预分配方案[2,3]，多项式的密钥预分配方案[4, 6,14]和基于网络部署知识的密钥预分配方案[15,16]。

随机密钥预分配方案最早是由 Eschenauer 和

Gligor[2]开始研究的，他们提出了一种基于密钥池的方案。该方案在每个节点被配置之前，随机从一个密钥池 P 中抽取 k 个密钥，组成密钥环，使任意 2 个节点有一定的概率共享至少一个密钥。如果 2 个节点的密钥环有交集，那么这 2 个节点之间就能够直接建立链路，否则需要借助路径建立过程在 2 个节点之间建立安全链路。实验证明，即使密钥环中密钥的数量远远小于构造 WSN 的节点数量，网络同样能够达到很高的连通性。但这种方法没有对所有节点的密钥环构成的集合在密钥池 P 中的占比进行约束，因此，一个密钥可能用于不同节点对之间的比例会非常高，从而降低整个网络抗物理攻击的能力。为了改善 WSN 抗物理攻击的能力，Chan 等[3]提出了 q-composite 方案，该方案指出 2 个节点之间共享密钥的数量达到 $q(q \geqslant 2)$ 时，它们之间才能建立安全链路，此时节点之间的会话密钥是所有共享密钥组合的结果，入侵者即使获取了某个节点的密钥环，他也无法确切的知道哪种组合形式应用于其他节点对之间的通信，因此，在一定程度上提高了 WSN 抗物理攻击的能力。

以上方法虽然能够在网络的安全性和节点存储量之间进行一定的平衡，但每个节点保存的都是密钥的明文，一旦被捕获的节点数量超过一个临界值时，整个网络的安全性能将急剧下降。同时，每个节点密钥环中所有密钥的并集对密钥池的覆盖范围也将直接影响到整个网络的安全性。

多项式密钥预分配方案不同于上述方案，节点保存的是产生密钥的多项式，而多项式可以是一元的[14]，也可以是二元的[4]，这样无论多少个节点被物理捕获，其泄漏的信息也不会对整个 WSN 构成直接的威胁，区别在于二元多项式的安全性更高。但如果要产生不同的对密钥，多项式的数量必须足够多，此时节点内存容量会成为一个瓶颈。正是基于这些考虑，Liu 和 Ning[6]提出了多项式池的密钥预分配方案，其思路是借鉴了随机密钥池的思想，构建多项式池，每个节点从中选择若干个多项式组成多项式环。采用这种方法可以在不降低网络抗物理攻击能力的前提下，减少节点存储开销，但这种方法需要借助 WSN 中簇头或基站，而这将成为整个网络的安全瓶颈。由于节点中存储的是产生密钥的多项式，因此在密钥建立过程中，节点之间通信量和计算量都比较大，对 WSN 寿命的影响较严重。

基于网络部署知识的密钥预分配方案，该方案是基于如下假设：节点部署后的位置关系与节点部署前的位置关系非常密切，如果一个节点与另一个节点在部署前是邻居，那么部署后这 2 个节点成为邻居的可能性将非常大。该方案在实施过程中利用了文献[2]中的相关知识，提高了网络连通性的同时，改善了网络抵抗物理攻击的能力和节点的存储量。与随机密钥预分配方案相比，该方案中各节点在建立密钥环时，对密钥的选择更有针对性，节点部署后相邻节点之间能够建立安全链路的可能性将更大，但这种方案分配机制比较复杂，所有密钥共享的计算是在部署前完成，其可操作性不强。

以上研究成果全部是利用对称密码技术完成密钥分配，在整个过程中他们回避了一个关键问题，即：所有这些方案能够实施，必须建立在对通信节点的身份认证基础上。如果没有这个前提，所有的方案都没有价值。而解决认证的问题必须借助公钥密码体制或第三方可信实体，显然，在 WSN 中引入第三方可信实体是不现实的，如果借助公钥密码体制，必须解决以下问题。

1) 如何在节点中存储其他节点的公钥信息，既保证了网络的连通性，又不会使内存超载。

2) 如何降低节点之间信息交换的次数，从而降低 WSN 的能量消耗。节点之间信息交换的次数和交换的信息量不得超过文献[1]中的方案。

3) 如何保证整个网络的可扩展性。即：新节点可以随时增加到网络中，不会影响整个网络的安全性能。

针对上述公钥密码体制需要解决的 3 个问题，本文提出了基于公钥的密钥分配方案。

3 基于公钥的密钥分配方案

假设 WSN 是一种扁平结构，其节点分为 2 种类型：基站和节点。其中基站的资源不受任何限制，而节点的资源受限。基站的独有信息包括：基站 ID_{A}，基站的公钥 UK_{A} 和基站的私钥 RK_{A}。每个节点的独有信息包括：节点的 ID，节点公钥 UK，节点的私钥 RK 和单向散列函数 H。该方案分为 2 个阶段：公钥集合建立阶段，邻居发现阶段。

公钥集合建立阶段。假设待部署的 WSN 中节点数量为 n，节点配置前，基站首先产生一个公钥集合 S：

$$\begin{bmatrix} ID_{11}UK_{11} & ID_{12}UK_{12}\cdots ID_{1N}UK_{1N} \\ ID_{21}UK_{21} & ID_{22}UK_{22}\cdots ID_{2N}UK_{2N} \\ \vdots & \vdots \quad\quad \vdots \\ ID_{N1}UK_{N1} & ID_{N2}UK_{N2}\cdots ID_{NN}UK_{NN} \end{bmatrix}$$

该集合是一个 $N\times N$ 的矩阵，$UK_{i,j}$ 表示公钥，$ID_{i,j}$ 表示对应公钥的身份或序列号。公钥集合 S 产生的方法如下。

1) 基站首先构造一个原始公钥集合 $\boldsymbol{F}=[UK_{10},UK_{20},\cdots UK_{N0}]$；

2) 利用单向散列函数 H 分别计算 F 中的每个元素得到对应行的公钥值，即：$UK_{i1}=H(UK_{i0})$，$UK_{i,j+1}=H(UK_{i,j})$

3) 利用集合 S 中的公钥产生对应的私钥。

基站从集合 S 中选择一个元素 $[ID_{ij}UK_{ij}]$ 及其对应的私钥 RK_{ij} 分配给节点 n_f，所选元素不会重复，分配完成后，所有的节点都将拥有唯一的 ID，公钥和对应的私钥。每个节点从集合 F 中随机选择 m（$m<N$）个元素，组成公钥集合 F 的子集 T，子集 T 之间可能存在元素的重叠。在这个过程中，注意到，对于集合 F 和 S 中的每个元素并没有利用基站的私钥 RK_{A} 对其签名。如果签名，在使用这些公钥时要验证签名，这不仅增加了节点的存储开销，而且增加了节点的能耗。在本方案中，利用基站的私钥 RK_{A} 签名节点的公钥是完全没有必要的，原因在于：本方案中节点公私钥分配过程与 Internet 上的公私钥分配过程不同。第一，本方案中，基站可信的假设是合理的，节点部署前其自身的公私钥对是由基站统一离线分配的，因此，节点无需利用基站的公钥验证基站分配的公私钥对的合法性。第二，如果 2 个节点之间能够建立安全的通信链路，则其中一个节点的公钥 UK 一定是另一个节点中保存的集合 T 中元素所对应的集合 S 行向量中的一个。由于这些公钥都包含在预先产生的集合 S 中，没有另外产生新的公私钥对，这些公钥都是由基站分配的，因此节点认为这些公钥的身份是合法有效的假设是合理的。

邻居发现阶段。在 WSN 中，节点的通讯距离是有限的，因此一个节点的邻居节点数量也是有限的，一般远远小于 n。邻居发现的方法是：节点 i 将自己的 ID 号以明文的形式广播出去，接收到该信号的节点 j 查询其保存的集合 T_j，如果属于该集合，则节点 i 是 j 的邻居，节点 j 可以将数据加密后发送给节点 i，反之不一定，即：节点 i 是节点 j 的邻居，但节点 j 不一定是节点 i 的邻居。这时，节点 j 需要根据节点 i 的 ID 号计算其相应的公钥 UK。所有的节点成功广播了 ID 号之后，WSN 将构成一个随机有向图，如果任意 2 个节点都存在通路，则构成有向连通图。在这个过程中，入侵者即使截获了节点的 ID 号或捕获了某个节点，也无法威胁到整个网络的安全。其原因在于：节点的 ID 号仅用于辨别节点的身份和识别该节点的公钥 UK 是集合 F 中哪个元素派生出来的，以及该节点公钥在集合 S 中的位置，因此没有其他信息，入侵者是无法假冒其他节点的。如果入侵者捕获了某个节点，他除了获取该节点的公私钥对外，还可以获得产生其他节点公钥的集合 T 和单向散列函数 H。因为从公钥无法推导出私钥，因此入侵者尽管可以假冒该节点参与网络链路的建立，但无法威胁到其他节点的安全。如果在 WSN 中增加其他的安全措施，是完全可以发现变质节点的，本文不就该问题展开讨论。

在密钥分配阶段，节点不产生与邻居节点之间通信的会话密钥 K_{s}，会话密钥 K_{s} 是在第一次数据传输过程中产生，即：节点 i 准备将数据发送给邻居节点 j 时，节点首先利用会话密钥 K_{s} 加密待发送的信息，然后利用节点 j 的公钥 UK_j 加密会话密钥 K_{s}，将组合后的数据 $\{E_{K_{\mathrm{s}}}(M),E_{UK_j}(K_{\mathrm{s}})\}$ 发送给节点 j，下次通信时就可以直接利用 K_{s} 了，这样做可以减少一次节点之间的通信过程。由于 K_{s} 的长度非常短，因此用公私钥加解密和对称密钥加解密在能耗上差别不大。

公钥算法的选择。在相同安全强度下椭圆曲线加密算法（ECC）比 RSA 的密钥长度小得多，以 1 024bit 的 RSA 密钥为例[17,18]，同等强度的 ECC 密钥长度只需要 160bit，虽然在 8bit CPU 中，ECC 的计算时长稍高于 RSA 算法，但 ECC 所需要的内存空间要小得多，传输所用的带宽要求更低，综合内存容量、传输时间和计算量，选择 ECC 算法作为文本的公钥算法。

对称密钥的选择。本文采用轻量级的 DES 算法（DESL）[19]，该算法是针对 RFID 开发的，考虑到 WSN 资源有限的特点，同样适合于 WSN 的节点应用，其能耗只有 DES 能耗的 75%。

4　网络连通性分析

由于 WSN 中节点无线信号的传输距离有限，一

个节点只能接收周围节点发送的信号，如图 1 所示（虚线表示邻居发现阶段的通信链路，实线表示邻居之间的数据传输链路），节点 A 接收其周围节点 B-G 的信号。在邻居发现阶段，节点 B-G 将其 *ID* 号以明文的方式广播给节点 A，节点 A 接收到这些 *ID* 号后与其集合 *T* 进行比较，如果 *T* 中包含产生该节点公钥的原始公钥，则 A 将相应的节点划归为邻居。图 1 中，节点 B，D 和 F 是 A 的邻居，A 可以将收集到的数据发送给节点 B，D 或 F，但反之不一定。邻居发现阶段完成后，WSN 将构成一个随机有向图。

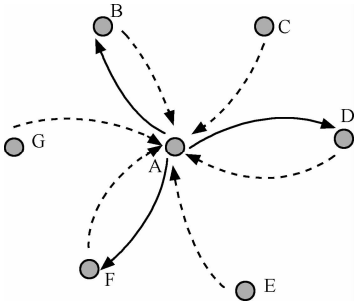

图 1 邻居节点的有向链路

在 WSN 中，假设节点的数量为 n，基站产生的公钥集合 S 中密钥的数量为 $|\boldsymbol{S}|=N\times N$，节点保存的原始公钥集合 T 中密钥的数量为 m，一个节点存储产生另一个节点公钥的原始公钥的概率为 p，那么该节点的出度为 $d^-=(n-1)p$，WSN 抽象成一个随机有向图 $G_{n,p}$。当 $p=0$ 时，任何一个节点都没有邻居，每个节点都是孤立的；当 $p=1$ 时，任何一个节点都有 $n-1$ 个邻居，此时 $G_{n,p}$ 变化成无向连通图。本节和第 5 节将解决第 2 节中的问题 1)和问题 3)，为此，必须回答以下问题。

1) 一个节点的 d^- 达到多少时，才能保证整个网络的连通性，即：任何一个节点成为孤岛的概率非常小。

2) 在保证网络连通性的前提下，m 值的大小如何选择，它与 N 的关系，即：网络的扩展性与 m 的关系。

本节将回答上述的问题 1），而第 5 节将回答问题 2）。

Erdos 和 Renyi[20]曾对随机图的相关性质做过深入的研究，并给出了很多非常有用的结论：当 $n\to\infty$ 时，随机图 $G_{n,p}$ 中没有孤立点的概率为

$$\lim_{n\to\infty}\Pr[G_{n,p}\text{没有孤立点}]=\mathrm{e}^{-\mathrm{e}^{-c}} \tag{1}$$

此时，$\lim\limits_{n\to\infty}p=\dfrac{\ln(n)}{n}+\dfrac{c}{n}$，其中 c 是任意一个常实数。

由此可得：

$$d^-=\frac{n-1}{n}[\ln n-\ln(-\ln Pr)] \tag{2}$$

图 2 描述了 WSN 不同连通等级下的 d^- 和节点数量 n 之间的关系。网络的连通性提高一个等级，节点的出度大约增加 2。对于同一等级连通性的网络，随着节点数量的增加，每个节点出度值增加并不明显，如：Pr＝0.999 99，当 n＝2 000 时，$d^-\approx19$，而当 n＝10 000 时，$d^-\approx21$。因此节点数量对节点的出度值的影响不是很明显，而主要与其连通的等级有关。

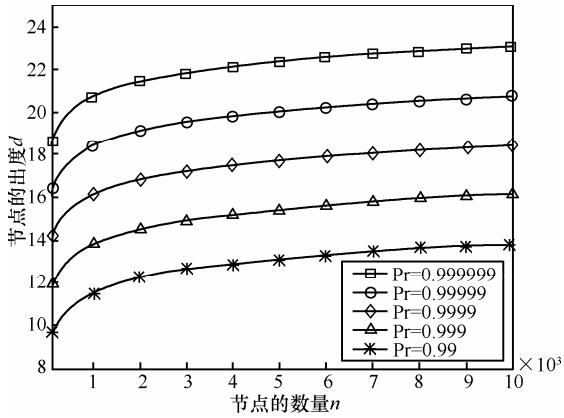

图 2 WSN 不同连通概率下 n 和 d^- 的关系

在 WSN 中，每个节点的通信距离是有限的，它只可能与其信号覆盖范围内的节点建立联系，信号范围内的节点数量 $t\ll n$。如果要保证整个网络的连通性，每个节点的 d^- 值是不会改变的，那么每个节点包含产生周围节点公钥的原始公钥的概率 p'将增加，即 $p'=\dfrac{d^-}{t-1}\gg p$。如：假设一个 WSN 网络，$n=10\,000$，$Pr=0.999\,99$，若 $t=40$，则 $p'=0.53$；若 $t=60$，则 $p'=0.35$。

5 网络的扩展性分析

当网络增加新节点时，基站首先从公钥集合 S 从选择一个从未使用过的元素以及其对应的私钥分配给该节点，然后从 F 中随机选择 m 个元素组成子集 T。一个显而易见的结论是：集合 S 中包含的元素越多，网络的扩展性越好，但在 m 不变的情况下，一个节点成为另一个节点邻居的概率 p 必然会

下降，从而降低网络的连通概率。

节点 i 从集合 F 中选择 m 个元素组成子集 T_i，此时，节点 j 在节点 i 的无线覆盖范围内。如果节点 j 从集合 S 中任意选择一个公私钥对作为自己的身份密钥，那么共有 $|\boldsymbol{S}|$ 种选择。如果节点 j 的公钥是由集合 T_i 中某个元素派生出来的，那么共有 $m\times N$ 种选择。因此，节点 j 是 i 邻居的概率为

$$p'=\frac{d^-}{t-1}=\frac{m\times N}{N\times N}=\frac{m}{N} \tag{3}$$

从式(3)可以发现，当 p'一定时，m 和集合 S 的数量 $|\boldsymbol{S}|$ 成正比，但 $m\ll|\boldsymbol{S}|$，此时不仅保证了 WSN 的安全，同时大大减轻了节点的存储开销。WSN 的扩展性取决于 $|\boldsymbol{S}|$ 的大小，但 $|\boldsymbol{S}|$ 增大会增加 m 的大小，即：增大了节点存储开销。因此，在利用本方案设计 WSN 时，必须兼顾网络的规模和节点的存储空间。

现在来比较本方案与传统的随机密钥预分配方案在网络扩展性方面的优劣。比较的对象选择 E-G 方案[2]，其他的随机密钥预分配方案[3~7]都是基于 E-G 方案的改进，其目的是增加 WSN 抗物理攻击能力，但网络的扩展性比 E-G 方案差。

假设：集合 S 中包含的密钥数量为 255×255=65 025，如图 3 所示，2 种方案中节点保存的密钥与节点成为邻居的概率之间的关系。

从图 3 可以看出，在一个节点成为另一个节点邻居的概率相同的情况下，本方案需要保存的密钥数量小于 E-G 方案保存的密钥数量，即：当节点的规模增大时，要保证网络连通性的概率，每个节点的度数必然增大，此时 p'将增大，这必然导致节点存储密钥的数量增加。本方案与 E-G 方案相比，其网络扩展性更强。

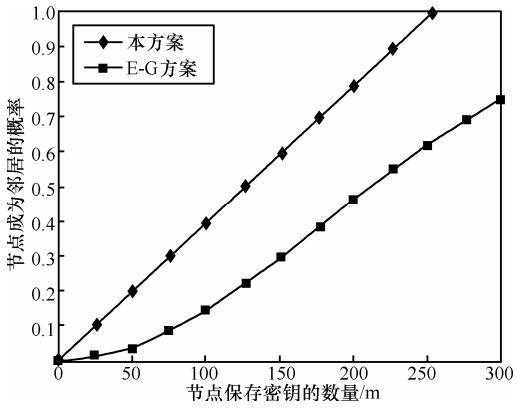

图 3　节点保存密钥的数量与节点成为邻居的关系

6　结束语

与基于对称密钥的预分配方案相比，本文给出的利用公开密钥系统实现 WSN 中密钥预分配的方案具有更高的安全性，任何一个节点被攻击，受影响的仅仅是该节点及其对应的链路，对网络中其他链路和节点均不产生影响。而在扩展性方面，通过相应的分析和比较，本方案比传统密钥预分配方案优越，节点规模相同的情况下，本方案对内存的要求低。

参考文献：

[1] HWANG D D, LAI B C, VERBAUWHEDE I. Energy- memory-security tradeoffs in distributed sensor networks[A]. 3rd International Conference on Ad-Hoc Networks and Wireless (ADHOC-NOW)[C]. 2004.70-81.

[2] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[A]. Proc of the 9th ACM Conf on Computer and Communications Security[C]. 2002.41-47.

[3] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[A]. IEEE Symposium on Research in Security and Privacy[C]. 2003. 197-213.

[4] CHENG Y, AGRAWAL D P. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks[J]. Ad Hoc Networks, 2007,(v5): 35-48.

[5] CHENG Y, AGRAWAL D P. Efficient pairwise key establishmentand management in static wireless sensor networks[A]. Proceedings of the Second IEEE International Conference on Mobile ad hoc and Sensor Systems[C]. Washington, DC, 2005. 7-10.

[6] LIU D, NING P. Establishing pairwise keys in distributed sensor networks[A]. Proceedings of the Conference on Computer and Communications Security'03[C]. ACM Press, Washington DC 2003. 52-61.

[7] DU W, DENG J, HAN Y S, *et al*. A key predistribution scheme for wireless sensor networks using deployment knowledge[J]. IEEE Transaction on Dependable and Secure Computing, 2006,3(1): 62-77.

[8] DU W, WANG R, NING P. An efficient scheme for authenticating public keys in sensor networks[A]. 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing[C]. 2005.

[9] GAO J, SION R, LEDERER S. Collaborative location certification for networks[A]. ACM Transactions on Sensor Networks[C]. 2010.30-55

[10] WANG H, LI Q. Efficient Implementation of Public Key Cryptosystems on MICAz and TelosB Motes[R]. Technical Report WM-CS-2006-07, College of William & Mary (2006), 2006.

[11] ROMAN R, ALCARAZ C. Applicability of public key infrastructures in wireless sensor networks[J]. Lecture Notes in Computer Science, 2007, 4582: 313-320.

[12] WATRO R, KONG D, CUTI S, *et al*. TinyPK: Securing sensor networks with public key technology[A]. Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks[C]. 2004. 59-64.

[13] LAI B, KIM S, VERBAUWHEDE I. Scalable session key construction protocol for wireless sensor networks[A]. IEEE Workshop on Large Scale Real-Time and Embedded Systems[C]. 2002.

[14] BLUNDO C, SANTIS A D, HERZBERG A, *et al*. Perfectly-secure key distribution for dynamic conferences[A]. Advances in Cryptology-CRYPTO ’92[C]. LNCS 740, 1993.471-486.

[15] LIU D, NING P. Location-based pairwise key establishments for relatively static sensor networks[A]. Proceedings of 2003 ACM Workshop on Security of Ad hoc and Sensor Networks (SASN’ 03)[C]. George W.Johnson Center at George Mason University, Fairfax, VA, USA,2003.

[16] LIU D, NING P. Improving key pre-distribution with deployment knowledge in static sensor networks[A]. ACM Transactions on Sensor Networks (TOSN)[C].2005.

[17] GURA N, PATEL A, WANDER A, *et al*. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[A]. Cryptographic Hardware and Embedded Systems: 6th International Workshop Cambridge[C]. MA, USA. 2004. 119-132.

[18] WANG H, SHENG B, TAN C, *et al*. WM- ECC: an Elliptic Curve Cryptography Suite on Sensor Motes[R]. Technical Report of Department of Computer Science, in College of William & Mary, WM-CS-2007-11, 2007.

[19] POSCHMANN A, LEANDER G, SCHRAMM K, *et al*. New light-weight crypto algorithms for RFID[A]. IEEE International Symposium on Circuits and Systems[C]. ISCAS 2007:1843:1846

[20] SPENCER J, THOMA L. On the limit values of probabilities for the first order properties of graphs[A]. R.L.Graham, J. Kratochvil, J. Nesetril, and F.S.Roberts, editors, Contemporary Trends in Discrete Mathematics[C]. volume 49 of DIAMACS, American Mathematical Society, 1999.317-336.

作者简介：

黄杰（1970-），男，湖北武汉人，博士，东南大学副教授、硕士生导师，主要研究方向为移动通信网安全和无线传感器网络安全。

黄蓓（1970-），女，湖北武汉人，东南大学讲师，主要研究方向为水下通信系统和信号处理。