第35卷 第18期 计 算 机 工 程 2009年9月
Vol.35 No.18 Computer Engineering September 2009
·安全技术· 文章编号：1000—3428(2009)18—0139—03 文献标识码：A 中图分类号：TP393

WSNs中多项式密钥预分配改进方案

周集良，吕庆聪，李彩霞，曹奇英
(东华大学信息科学与技术学院，上海 201620)

摘 要：针对密钥管理与路由信息脱离的现象，提出一种基于按需路由协议的多项式密钥预分配改进方案。该方案利用网络路由的拓扑信息和基站功能，使基站集中存储重要安全信息并承担大量计算负荷，普通节点仅保存其邻居的多项式份额。该机制能有效防止密钥泄漏，增强网络的安全性，节省节点的能量资源。

关键词：无线传感器网络；网络安全；密钥预分配；多项式份额

Improved Scheme of Polynomial Key Pre-distribution in Wireless Sensor Networks

ZHOU Ji-liang, LV Qing-cong, LI Cai-xia, CAO Qi-ying
(College of Information Science and Technology, Donghua University, Shanghai 201620)

【Abstract】 To solve the limitation of combination between traditional key management and routing information, this paper presents an improved scheme of polynomial key pre-distribution based on on-demand routing protocol according to the security requirement. The scheme makes full use of the topology information of routing and the function of the base station, which gathers the important security information and the computing loads, to insure the sensor only stores the polynomial quantum of neighbors. The mechanism can effectively prevent the key from giving away, improves the network secure performance, and save the energy resource.

【Key words】 Wireless Sensor Network(WSN); network security; key pre-distribution; polynomial quantum

1 概述

无线传感器网络具有开放的体系结构，由于网络自身特性，任何潜在的敌手都可以很容易地截取、窃听和伪造信息，因此安全性对无线传感器网络非常重要[1]。

在无线传感器网络的安全机制中，最重要的是在节点之间、节点与基站之间进行通信时，对信息进行加密和身份认证，其中，密钥的安全性是所有安全的基础。针对无线传感器网络的特点，近来已提出很多密钥管理方案，但这些方案都有自己不同的侧重点和优缺点。无线传感器网络应用范围十分广泛，由于应用环境、应用要求的不同，对节点资源和安全性的要求都有很大不同，并没有一种能适应所有应用环境的密钥管理方案，而安全性和资源开销是一对矛盾，因此需要针对不同的应用进行取舍。

无线传感器网络所有节点都是潜在的路由节点，每个节点兼备路由器和主机2种功能。路由信息是非常重要的资源，如何融合路由信息和密钥分发、管理是一个值得深入研究的课题[2]。

本文结合执行按需路由协议得到的拓扑信息资源，改进和融合传统的预共享密钥分发和多项式密钥预分配方案，提出了基于按需路由协议的多项式密钥预分配改进方案。

2 相关研究

2.1 传感器网络安全需求

无线传感器网络不但存在传统网络的安全问题，而且因网络的特殊性还存在一些额外的安全问题[1-2]：无线连接问题；网络内外的恶意攻击问题；网络的动态扩展性问题；网络的入侵检测和安全维护。针对这些问题，需要有完整的安全解决方案，密钥管理无疑是这些安全解决方案的基础，目前，已经提出了各种密钥管理方案。

2.2 密钥管理方案

在针对无线传感器网络结构提出的许多密钥管理方案中，比较典型的有预共享密钥、基本随机密钥分发和基于多项式的预配置密钥分发等方案。

2.2.1 预共享密钥分发方案

预共享密钥分发方案是一种最基本的密钥管理方案，所有的传感器节点在拓扑前预配置一个相同的密钥，所有的节点均利用该密钥进行加密、解密、认证以及密钥的协商和更新。这种方案的优点是：设计简单，计算复杂度低，易于扩展新节点。不足之处是是一旦一个节点被攻破，网络中所有的节点都将被攻破，整个网络就失去了安全防护[3]。

2.2.2 随机密钥预分配方案

随机密钥预分配方案在部署传感器节点之前，首先用密钥算法产生一个包含 S 个密钥的密钥池，并将 S 个密钥排序，分别分配一个密钥 ID，然后随机抽取 m 个密钥(包括相应的密钥 ID)分配给节点的密钥环(存储密钥的地方)。网络部署后，每个节点向邻居节点广播其所有密钥 ID，接收到的节点和自己的密钥 ID 进行对比，若有共同的密钥，就用这些密钥进行加密通信。否则，节点通过与其他存在共享密钥的邻居

基金项目：教育部基金资助重点项目(104086)
作者简介：周集良(1970－)，男，高级工程师、博士研究生，主研方向：路由技术，网络安全；吕庆聪、李彩霞，讲师、博士；曹奇英，教授、博士生导师
收稿日期：2009-03-15 **E-mail：**hnzhoujl@126.com

节点，经过若干跳后建立双方的一条密钥路径[4]。

可见，要达到网络高连通概率，每个节点要存储大量的密钥和密钥 *ID*。这对资源有限的节点来说是不现实的，而且存储大量密钥将使系统变得脆弱。

2.2.3 基于多项式的密钥预分配方案

基于多项式的密钥预分配方案在密钥产生过程中并不直接把密钥分配到传感器节点上，而是分配用于产生安全会话密钥的多项式，密钥则由这些多项式产生。这一方法避免了直接分配密钥易造成的泄漏问题，多项式动态生成节点间的密钥对，在一定程度上提高了安全性[5]。

采用基于多项式的密钥分配方案后，网络的安全性能有所提高，能够有效地抵御节点被捕获，但与密钥预分配方案相比，增加了额外的通信成本，节点的存储成本和计算开销都相应增加，耗费了大量宝贵的能量资源。

2.2.4 其他预配置密钥方案

其他预配置密钥方案有可扩展密钥管理(Scalable Cryptographic Key Management, SCKM)方案、低能量密钥管理协议(Low-Energy Key Management Protocol, LEKMP)等。这些方案虽然扩展性好、耗能低，但安全性较差[4-5]。

3 多项式密钥预分配改进方案

上述密钥管理方案均考虑了网络安全需求和节点的能量限制，提高了网络安全性能，但这些方案没能根据具体的网络拓扑结构充分利用路由信息资源实施安全的密钥管理。因此，需要根据按需路由协议的网络结构和路由信息，对现有多项式密钥预分配方案进行改进。

3.1 方案概述

对无线传感网络模型作如下假设：网络区域为 *A*，共有 *N* 个传感节点均匀分布其中，这些传感节点在 *A* 中独立地自由移动，有一个基站位于网络中心位置；网络是不安全的，可能受到各种攻击，但基站是安全的，并有足够的能量和一定的入侵检测能力；基站运行基于查询的按需路由协议(即查询驱动的路由协议)。

本文采用基站预共享密钥与多项式密钥预分配改进方案相结合的模型，设计了如下模型：在网络拓扑发现阶段，采用基站预共享密钥，建立安全的网络邻居表；然后，将邻居表位置信息引入改进的多项式密钥预分配的方案中。基站集中存储重要安全信息并承担大量计算负荷、通信负荷，普通节点保存其邻居的多项式份额和部署时的主密钥。

3.2 方案的具体实现

方案采用基于二元 *t* 次多项式和位置信息的安全引导模型。基于二元 *t* 次多项式的密钥对模型是 Blundo 等 1993 年提出的，该方法本是解决组密钥预分布模型的算法，计算开销太大，不适合传感器网络，但是其密钥对分配模型部分可以被传感器网络所利用。其模型的一般形式为

$$f(x,y)=\sum_{i=o}^{i=t}\sum_{i=0}^{i=t}a_{i,j}x^i y^j \bmod p$$

$$f(x,y)=f(y,x)$$

$$g_u(x)=f(x,r_u) \bmod p=\sum_{i=0}^{i=t}a_{u,i}x^j$$

该模型需要节点保存一个与自身 *ID*(记为 r_u)相关的多项式份额(polynomial share) $g_u(x)$，并与邻近节点通过该多项式份额建立共享密钥对。以 t=1 为例，每个节点有一个唯一的身份标识，属于有限域 F_P，其中，p 是比密钥空间尺寸大的最小质数。首先，从 F_P 中选择 a, b, c 3 个元素生成多项式：

$$f(x,y)=(a+b(x+y)+cxy) \bmod p$$

然后为每个节点计算一个多项式份额：

$$g_u(x)=(a_n+b_n x) \bmod p$$

$$a_n=(a+br_u) \bmod p,\quad b_n=(b+cr_u) \bmod p$$

最后，节点 *u* 和节点 *v* 通过在其多项式份额中代入另一节点的 *ID* 计算共享密钥对，即节点 *u* 计算 $K_{u,v}=g_u(r_v)$，节点 *v* 计算 $K_{v,u}=g_v(r_u)$。

引入位置信息后，节点的部署需要一个部署服务器辅助完成，设计这个部署服务器由基站担任。为了预分布密钥对，基站随机产生一个定义在有限域 F_p 上的二元 *t* 次多项式 $f(x,y)$，其中，p 是一个足够大的质数以容纳加密密钥；$f(x,y)$ 满足对称特性即 $f(x,y)=f(y,x)$。

假定每个节点都有一个唯一的 *ID*，对于每一个节点 *i*，部署服务器计算多项式 $f(x,y)$ 的一个份额 $f(i,y)$。对于任意 2 个节点 *i* 和 *j*，节点 *i* 可以通过在节点 *j* 对 $f(i,y)$ 求值计算共同密钥 $f(i,j)$，节点 *j* 可以通过对 $f(j,y)$ 在 *i* 点求值得到共同密钥 $f(j,i)$，因为 $f(j,i)=f(i,j)$。理论上该模型在被俘节点个数不超过 *t* 的前提下不会泄漏任何信息。利用这种思想，根据位置信息将目标区域划分为小的单元(cell)，每个单元与一个唯一的随机二元 *t* 次多项式相关。为简单起见，假定目标区域是一个能被划分为等大小单元的矩形区域，其预分布过程如下：

在路由协议的路由发现阶段，基站已经得到了全网节点的邻居信息，设为矩阵{***C***}。

设 $G=(V,E)$是具有 *n* 个传感节点的网络图，则 *G* 的邻接矩阵是具有如下性质的 *n* 阶方阵：

$$\boldsymbol{A}[i,j]=\begin{cases}1 & \text{若}(v_i,v_j)\text{或}<v_i,v_j>\text{是}E(G)\text{中的边}\\ 0 & \text{否则}\end{cases}.$$

可以得知，节点 *i* 的邻居数为

$$n_i=\sum_{j=1}^{j=n}a_{ij}<<n$$

将传感节点的目标区域做如下划分：以每个传感节点为中心，以该节点和其对应的邻居组成一个逻辑区域。

节点 *i* 的邻居节点集合设为

$$\{ID_j \mid a_{ij}=1,\ j=1,2,\cdots,n\}$$

节点 *i* 的逻辑区域设为

$$\{ID_i\}\cup\{ID_j \mid a_{ij}=1,\ j=1,2,\cdots,n\}$$

这样，每一个逻辑区域都是一个单元，所有逻辑区域又组成一个部署矩阵，坐标为 (p_i,q_i) 表示第 *i* 个逻辑区域位于部署矩阵的第 *p* 行 *q* 列。

为便于描述，用 $n=M\times N$ 表示总的单元数。基站随机产生 *s* 个二元 *t* 次多项式 $\{f_{p_iq_i}(x,y)\}_{p_i=0,1,\cdots,M-1;q_i=0,1,\cdots,N-1}$，并将 $f_{p_iq_i}(x,y)$ 分配给 $C_{p,q}$ 单元。

图 1 是目标区域划分的一个例子。对于每个节点，部署服务器首先确定它的主单元，即节点期望定位的单元；然后部署服务器找到与节点的主单元相邻的 4 个单元；最后部署服务器将节点的主单元的坐标和多项式份额以及与它邻近的 4 个单元的多项式份额放在节点中，并布置到目标区域。例如，节点 *u* 期望部署到 $C_{2,1}$ 单元中，显然，$C_{2,1}$ 单元是它的主单元，且 $C_{2,0}$, $C_{1,1}$, $C_{2,2}$, $C_{3,1}$ 是与主单元相邻的 4 个单元。这样，基站将坐标(2, 1)及多项式份额 $f_{2,1}(u,y)$，$f_{2,0}(u,y)$，$f_{1,1}(u,y)$，$f_{2,2}(u,y)$ 和 $f_{3,1}(u,y)$ 存放到节点 *u* 中。

$C_{0,0}$	$C_{0,1}$	$C_{0,2}$	…	$C_{0,y-1}$
$C_{1,0}$	$C_{1,1}$	$C_{1,2}$	…	$C_{1,y-1}$
$C_{2,0}$	$C_{2,1}$	$C2_{,2}$	…	$C_{2,y-1}$
$C_{3,0}$	$C_{3,1}$	$C_{3,2}$	…	$C_{3,y-1}$
…	…	…	…	…
$C_{m-1,0}$	$C_{m-1,1}$	$C_{m-1,2}$	…	$C_{m-1,y-1}$

图 1　目标区域的划分

3.3　新节点的加入与撤消

密钥建立好后，普通节点仍保留存储在节点中的 *ID* 和共享密钥，由于基站广播密钥前使节点间的主共享密钥失效，因此节点间不能再用共享密钥进行会话，而只能使用建立后的密钥，这样就可以保证节点的安全性，即使节点被捕获或者共享密钥被泄露，攻击者也不能够用共享密钥对其他节点进行重放攻击。而保留 *ID* 和共享密钥的目的是为了新节点的加入。假如有一个新节点 *C* 预加入已有的网络，那么它的加入过程如下：

(1)节点 *C* 首先预配置自身的身份 *ID* 和基站共享密钥；

(2)基站广播拓扑发现消息；

(3)基站检测新加入的节点是否为合法节点；

(4)若是，基站根据该节点的邻居信息，计算该节点和其邻居节点的多项式份额；否则，拒绝节点加入；

(5)基站打包上一步计算得到的多项式份额消息，并发送到该节点和其邻居。这样新节点 *C* 就安全加入到网络中。

如果某个节点被捕获或能量耗尽，根据前面假设，基站通过检测机制发现后，更改网络拓扑信息表，更新该节点有关的多项式份额，执行步骤(4)。这样，该节点即从这个网络中删除。

3.4　密钥的更新

在许多分布式传感器网络中，通常每 2 个节点共享密钥的生命周期会超过 2 个节点的生命周期。但在有些情况下(如恶意攻击、密钥被破解)，密钥将失效或过期，因此，共享密钥需要随时进行更新。密钥的更新过程如下：

(1)基站向所有节点或被攻击节点的邻居节点发送一条密钥更新指令；

(2)节点接收到更新指令后，销毁现在使用的多项式份额，然后基站再启用密钥建立过程，如执行上述步骤(1)～步骤(5)，计算相应多项式份额，并发送到对应节点中。

4　性能分析

4.1　安全性分析

本方案虽然使用了节点与基站的共享主密钥，但该主密钥只是在网络建立或节点加入时才有效，其他时间该密钥无效，因此，该方案比传统的预共享密钥分发方案更安全。

即使某些节点被捕获，也只能得到多项式份额，无法从节点中获得密钥，攻击者也不能通过这些多项式攻击网络中的其他节点。这样确保了网络的安全性。通信双方建立唯一的会话密钥后，该会话密钥具有身份认证功能，接收者可以通过数据源认证确信消息是从正确的节点处发送过来的，从而确保了消息的真实性。如果在信息中使用消息认证码，可以将会话密钥和待检验的消息连接在一起进行运算，从而能够有效防止攻击者对截获的信息进行篡改，保证了消息的完整性。如果将计数器信息包含在待加密消息中，邻居之间会话密钥加密确保了攻击者无法获知和篡改计数器的信息，计数器的内容又能使接收者确信收到的数据是在最近时间内生成的最新数据，即消息是新鲜的。因此，本方案为身份验证、消息安全通信等诸多安全功能提供了安全基石。

4.2　效率分析

和其他密钥方案相比，本方案效率得到了较大提高：基站存储了重要的安全信息，普通节点只保存了邻居节点的多项式份额和本身的 *ID*，节省了普通节点宝贵的存储空间；大量的计算负荷和通信负荷由基站承担，普通节点只需完成邻居节点的多项式份额计算和与邻居节点建立会话密钥的通信费用；改进方案的连通概率为 1，高于随机密钥分配方案。

表 1 对几种常见的密钥分配方案和多项式密钥预分配改进方案(表中称“新方案”)的几个效率参数进行了比较。其中，*P* 为密钥池的大小；*d* 为节点的度；*k* 为节点密钥环大小；*T* 为搜寻共享密钥；*N* 为节点的邻居数，一般 $N<<T$。

表 1　4 种方案比较

解决方案	扩展性	内存需求	通信开销	连通概率
预共享密钥	比较好	1	1	1
随机密钥	一般	$2k$	$K+dk$	$1-\frac{((P-k)!)^2}{(P-2k)!P!}$
多项式	差	$T+1$	T	1
新方案	一般	$N+1$	N	1

5　结束语

针对当前密钥分配与网络拓扑结构、路由信息资源相脱离现象，本文提出能确保传输消息的机密性、完整性、新鲜性的方案，能够有效抵制包括节点俘获在内的多种网络攻击，为传感器网络安全体系结构的建立提供了基础性保障。

参考文献

[1] Adrian P, John S, David W. Security in Wireless Sensor Networks[J]. Communication ACM, 2004, 47(4): 53-57.

[2] Akkaya K, Younis M. A Survey on Routing Protocols for Wireless Sensor Networks[J]. Ad Hoc Networks, 2005, 3(3): 325-349.

[3] Eschenauer L, Gligor V D. A Key-management Scheme for Distributed Sensor Networks[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. Washington, DC, USA: ACM Press, 2002.

[4] Haowen C, Perrig A, Dawn S. Random Key Pre-distribution Schemes for Sensor Networks[C]//Proceedings of IEEE Symposium on Security and Privacy. Berkeley, California, USA: IEEE Press, 2003.

[5] Didier F, Yann L C. Finding Low-weight Polynomial Multiples Using Discrete Logarithm[C]//Proc. of IEEE International Symposium on Information Theory. Nice, France: IEEE Press, 2007.

编辑　张正兴