文章编号:1001 - 9081(2009)11 - 2980 - 03

一种无线传感器网络预分配密钥管理方案的改进

陈航哲,王晓明
(暨南大学 信息科学技术学院,广州 510632)
(elite910@163.com)

摘 要:无线传感器网络在应用二元多项式密钥预分配协议时,通常容易遭受到敌方的合谋攻击。为了更好地解决这一问题,通过减少普通节点共享的密钥个数,改变簇首间建立共享密钥的方式,改进了一种无线传感器网络的密钥预分配管理方案。分析表明,改进后的方案保留了原方案的网络高安全性等优点,而且进一步节省了普通节点的内存空间,减少了节点间的通信量,延长了网络的生存周期,能够有效地抵御敌方的合谋攻击。

关键词:网络安全;二元对称多项式;门限;分簇
中图分类号: TP393.08 **文献标志码**:A

Improved Pre-distribution key management scheme for WSN

CHEN Hang-zhe, WANG Xiao-ming
(*College of Information Science and Technology, Jinan University, Guangzhou Guangdong* 510632, *China*)

Abstract: Wireless Sensor Network (WSN) was usually vulnerable to conspiracy attack from its adversaries when using bivariate polynomial key pre-distribution protocol. In order to solve this problem, a pre-distribution key management scheme for WSN was improved by reducing the amount of pairwise keys sharing between sensor nodes and changing the means of establishing pairwise keys between clusters. Analysis shows that the improved scheme not only maintains the advantages such as higher security of the original scheme, but also saves the limited memory storage of sensor nodes further, reduces the communication overhead of sensor nodes, extends the lifespan of the networks and can withstand conspiracy attack effectively.

Key words: network security; bivariate symmetric polynomial; threshold; clustering

0 引言

无线传感器网络作为计算机、通信和传感器这三项技术相结合的产物,是一种全新的信息获取和处理技术。目前它已经被广泛应用在军事侦查、城市管理、环境和交通监测、森林防火等方面[1]。由于无线传感器网络一般部署在恶劣的自然环境中或敌方阵地里,加上网络规模庞大、节点数目众多等特性使得任何潜在的敌方都可以轻易地截取、窃听和伪造信息。为了提高其安全性,无线传感器网络的密钥分配研究日益受到人们的重视。

一般而言,传感器节点计算能力不强,存储空间有限,能量储备和通信能力较低。针对这些特点,目前主要使用的密钥分配方法之一是预分配密钥技术,即在传感器部署之前,向其内存中装载入一定量的密钥信息,通信双方可以通过这些信息直接得到或者经计算得出它们之间的通信密钥。最简单的方法是在整个网络中使用同一个密钥 K;又或是给每一对传感器都分配一个通信密钥,那么在有 n 个传感器节点的网络中一共需要 $n(n-1)/2$ 个密钥。然而前一种方法在敌方破获 K 之后,就可以控制整个网络;后一种方法则需要保存很多的密钥,对传感器的内存要求很高[2],且网络扩展性差,均不适用于资源受限的传感器网络。

最近,不少学者提出了基于二元多项式的密钥预分配管理方案[3-5]。本文首先介绍文献[3]中提出的方案(以下简称 Yi 方案),然后指出其不足之处,提出改进的方案,并从网络的安全性等方面对改进后的方案进行分析评估。

1 Yi 方案简介

1.1 网络模型及假设

在文献[3]中,无线传感器网络被当作是一种分层的网络,称之为基于分簇的无线传感器网络。网络共分为三层,有三种不同的节点:基站、簇首节点和普通节点。

1)基站:无线传感器网络中性能最强的节点,无线电射程覆盖整个网络范围。基站是整个无线传感器网络与外界网络的接口,将接收来自无线传感器网络中的节点发送过来的所有数据。基站一般作为无线传感器网络的控制中心,部署在有人值守的可控制的环境下,不易被敌方俘获,而且数据处理能力、内存容量都不受限制。

2)簇首节点:具有较高能量储备,足够的存储能力,很强的数据处理能力,无线电射程足够远,簇首节点之间在建立了对称密钥后可以直接通信。簇首节点负责对簇内数据进行预处理,剔除冗余信息并对数据进行压缩,再把处理好的数据发送到基站。

3)普通节点:能量储备有限,存储能力也有限,数据处理能力较弱,无线电射程短,部署好后保持静止。普通节点之间不通信,它们只需采集周围环境的数据,然后发往所在簇的簇首节点即可。

根据该网络模型,在无线传感器网络中存在着两个通信层。第一层是基站与簇首节点之间的通信;第二层是簇首节点与簇内普通节点之间的通信。

收稿日期:2009 - 05 - 19;**修回日期**:2009 - 07 - 10。
基金项目:国家自然科学基金资助项目(60773083);广东省自然科学基金资助项目(8151063201000022)。
作者简介:陈航哲(1980 -),男,广东茂名人,硕士,主要研究方向:网络信息安全、无线传感器网络; 王晓明(1960 -),女,重庆人,教授,博士,主要研究方向:计算机网络安全、现代密码学。

1.2　文中主要符号约定

假设无线传感器网络在部署好之后有 n 个普通节点,有 m 个簇首节点。对本文所使用符号作如下约定:BS 表示基站;CH_i 表示簇首 i;S_i 表示普通节点;K_{A-B} 表示节点 A 和 B 之间的密钥;$E_K(data)$ 表示用密钥 K 加密数据;$f_{CH}(x,y)$ 表示 t 阶二元对称多项式,用以建立簇首之间的密钥;$f_{CH_i}(x,y)$ 表示 t 阶二元对称多项式,用以建立簇首与普通节点之间的密钥;⊕表示异或运算;K_{CH_i-BS} 表示表示簇首 CH_i 与基站 BS 之间的对称密钥;KDS 表示离线密钥分配服务器。

1.3　二元对称多项式预分配协议

二元 t 阶对称多项式一般定义如下:

$$f(x,y) = \sum_{0\leqslant i,j\leqslant t} A_{i,j}x^i y^j$$

在预分配对称密钥之前,离线密钥分配服务器(Key Distributing Server, KDS)会在有限域 F_q 上随机选择一个 t 阶二元对称多项式,其中 q 是一个足够大的素数。KDS 还会在部署网络之前分配一个独一无二的 ID 号(比如,u)给每一个传感器节点,然后把每个传感器的 ID 号代入 $f(x,y)$ 中计算出一个一元多项式,并把该多项式的所有系数都装入传感器内存中。一般地,对于 ID 号为 u 的传感器节点,所装载的一元多项式为 $f(u,y) = \sum_{j=0}^{t} B_{u,j}y^j$,其中 $B_{u,j} = \sum_{i=0}^{t} A_{i,j}u^i$。对于任何两个传感器节点 u、v,节点 u 都可以计算出它们之间共享的密钥 $f(u,v)$,方法是计算当 $y = v$ 时 $f(u,y)$ 的值。同样地,节点 v 可以用类似的方法计算出 $f(v,u)$。由于 $f(x,y)$ 是二元对称多项式,所以有等式 $f(u,v) = f(v,u)$ 成立。从而,节点 u 和 v 可以建立它们之间通信用的密钥。以上过程可以用图 1 来简单地表示[4]。

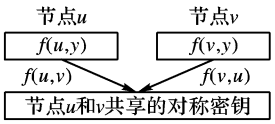

图 1　基于二元对称多项式的密钥分配原理

针对该协议存在的 t 门限性质,即难以抵挡多于 t 个节点的合谋攻击问题,文献[3]提出了一个改进方案——Yi 方案。

1.4　Yi 方案及分析

Yi 方案中,密钥分配及建立共分为三个不同的阶段,即预分配阶段、簇首之间建立密钥阶段、簇首与簇内普通节点之间建立密钥阶段。

在预分配阶段,基站被分配了 $m+n$ 个密钥,其中 n 个密钥用于基站与普通节点之间加密信息,存储的 m 个密钥 $K_{CH_i-BS}(1\leqslant i\leqslant m)$ 用于基站分别与每一个簇首节点 CH_i 之间的通信加解密。普通节点也存储了一个与基站共享的密钥。簇首中预存储的信息则包括一个与基站通信的对称密钥 K_{CH_i-BS} 及两个一元多项式 $g_{CH}(y)$ 和 $g_{CH_i}(y)$。在簇首之间建立密钥阶段,m 个簇首需要两两之间交换信息建立密钥。在簇首与簇内的普通节点建立密钥的阶段,簇首通过与其他某两个簇首之间通信,得到建立簇首与簇内普通节点的密钥所需要的信息,从而计算出密钥。

根据网络模型假设以及原方案的思想,至少有两个地方可以改进。1)基站与普通节点之间不需要共享密钥,这样可以节省普通节点的内存空间。因为簇首需要把普通节点收集到的信息进行过滤、整理,再转发给基站。假如普通节点利用与基站共享的密钥加密了收集到的信息后再发给簇首,那么簇首就无法对收到的信息进行必要的处理。而且,普通节点由于无线电射程短,一般与基站没有直接的通信,所以没有必要与基站共享一个通信密钥。2)把簇首之间两两建立共享密钥单独安排在第二个阶段是不必要的。由于簇首的计算能力比较强以及能量充足,所以完全可以在需要的时候再建立密钥,这样可以有效地减少网络中的通信开销。

2　改进后的密钥分配和建立方案

网络模型假设及用到的符号等基本与 Yi 方案相同。

2.1　密钥预分配阶段

在部署无线传感器网络节点之前,需要把一些密钥的相关信息装载入传感器节点中。为实现数据的保密性、可靠性和完整性,网络不同层的节点所装载的密钥信息是不尽相同的[3]。下面是改进方案中每层节点所装载密钥信息的具体情况。

1)基站:存储 m 个密钥 $K_{CH_i-BS}(1\leqslant i\leqslant m)$,分别用于与每一个簇首节点 CH_i 的通信加解密。

2)簇首节点:存储一个与基站通信的对称密钥 K_{CH_i-BS} 和两个一元多项式,即 $g_{CH}(y)$ 和 $g_{CH_i}(y)$。两个一元多项式分别由以下两式计算得到:

$$g_{CH}(y) = f_{CH}(CH_i,y)$$

$$g_{CH_i}(y) = f_{CH_i}(CH_i,y)$$

此外,每一个簇首都内置一个逻辑数组 $con[m]$,用以标志自己与其他簇首是否建立了安全的通信密钥,初始化全部为 false。

3)普通节点:预存储一个对称密钥 K_{S_i-CH}。K_{S_i-CH},用于 S_i 和它所在簇的簇首之间通信的密钥。

K_{S_i-CH} 的具体产生过程如下:

1)KDS 从 m 个多项式 $f_{CH_i}(x,y)$ 中随机选择 $l(l\geqslant 1)$ 个多项式,此处取 $l=2$,假设选取 $f_{CH_a}(x,y)$ 和 $f_{CH_b}(x,y)$;

2)KDS 计算出 $f_{CH_a}(CH_a,S_i)$ 和 $f_{CH_b}(CH_b,S_i)$,分别赋值给 k_1 和 k_2:

$$k_1 = f_{CH_a}(CH_a,S_i)$$

$$k_2 = f_{CH_b}(CH_b,S_i)$$

3)KDS 计算密钥 $K_{S_i-CH} = k_1 \oplus k_2$;

4)KDS 把 K_{S_i-CH} 及两个簇首的 ID,即 CH_a 和 CH_b 装载到传感器节点 S_i 内存中。K_{S_i-CH} 将作为网络部署好之后,S_i 和它所在簇的簇首之间通信的密钥。

2.2　簇首与簇内普通节点对密钥的形成阶段

假设部署好整个网络后,节点 S_i 所在簇的簇首是 CH_j。以下是 S_i 和 CH_j 之间建立通信密钥的详细过程。

1)S_i 把其 ID 号 S_i,以及它存储的两个簇首节点的 ID 号 CH_a 和 CH_b 包含在消息 M 中,发送到它所在的簇首节点 CH_j。

2)CH_j 收到簇内节点 S_i 发过来的消息 M 后,查看自己是否已经计算了 $K_{CH_j-CH_a}$ 以及 $K_{CH_j-CH_b}$,即查看 $con[CH_a]$ 及 $con[CH_b]$ 是否为 true。若至少有一个值为 false,比如前者的值为 false,则首先根据 $K_{CH_j-CH_a} = f_{CH}(CH_j,CH_a)$ 计算出 CH_a 与 CH_j 之间的通信密钥,然后用 $K_{CH_j-CH_a}$ 加密 S_i 发送到 CH_a。类似地,用 $K_{CH_j-CH_b}$ 加密 S_i 发送到 CH_b。

3)收到请求信息后,CH_a 查看自己是否已经计算了 $K_{CH_a-CH_j}$。如果没有,则计算出来,然后解密消息,得到 S_i 的 ID 值,从而计算出 $k_1 = f_{CH_a}(CH_a,S_i)$。CH_a 把 $E_{K_{CH_a-CH_j}}(k_1)$ 发送给 CH_j。

4)CH_j 收到来自 CH_a 的回应消息后,用 $K_{CH_j-CH_a}$ 解密消息,从而得到 k_1。

5)同样地,CH_j 可以从 CH_b 处得到 k_2。

6）最后 CH_j 通过 k_1 和 k_2 的异或运算得到 $K_{S_i-CH_j}$，即：

$K_{S_i-CH_j} = k_1 \oplus k_2$

至此，簇首 CH_j 与其簇内的普通节点 S_i 之间建立了对称密钥，即 $K_{CH_j-S_i}$。

当这一阶段完成后，每一个簇首都与其簇内的普通节点建立了安全的通信密钥。其中一部分的簇首之间也建立了相互之间的通信密钥。由于模型中假设簇首的无线电射程足够远，能够与基站进行直接的通信，因此，簇首之间两两预先全部建立密钥没有必要。完全可以在需要的时候再建立，这是基于簇首的计算能力很强以及能量充足的假设。

3 网络性能评价

3.1 安全性分析

本方案中，普通节点之间没有通信，每个普通节点都只保存一个对称密钥，提高了网络在遭受敌方节点俘获攻击后的自我恢复能力。在网络初始化阶段，每个簇首节点都只保存了两个一元多项式，簇首对于其簇内的普通节点的密钥信息毫不知情。即使所有簇首的信息都泄露，普通节点中的预分配密钥信息也不会泄露。方案中没有组密钥[6]，簇首之间传递交换信息时，要预先建立好对称密钥，再进行通信。任何一个簇首被敌方俘获，都不会影响到其他未被俘获的簇首之间的安全通信。

至于前面提及的 t 阶二元对称多项式存在的 t 门限性质[3]，由于本文方案中假设簇首有相当充足的能量和很大的内存容量，所以可以选择一个足够高阶的二元对称多项式用以产生簇首间的通信密钥。假如多项式的阶 t 大于网络中簇首的个数 m [3]，那么即使敌方俘获了所有的簇首节点，也不能破解出这个多项式的系数，从而确保了网络的通信安全。

3.2 网络表现评价

1）扩展性能：由于无论网络的规模有多大，普通节点都只存储一个密钥，因此网络规模的大小只取决于簇首节点的个数。由于方案中假设簇首具有相当大的内存，足够的能量和较强的数据处理能力，因此，从理论上讲，只要选取合适的二元对称多项式和成簇算法，那么本方案就适用于任何大规模的无线传感器网络[3]。从而，本方案具有较佳的网络扩展性。

2）存储开销：无论网络规模有多大，普通节点都只需要存储一个密钥，极大地节省了内存空间。而基站和簇首的存储能力都很强，所以它们的存储开销可以忽略不计。

3）通信开销：对于一般密钥预分配方案来说，由于每个传感器节点都需要和它的邻居节点交换密钥信息，所以通信开销较大。而本方案中，每个普通节点仅预先存储一个对称密钥，无须与其他普通节点交换信息建立密钥。当有新的普通节点加入网络时，无须额外重新分配密钥，只要在部署前按照前面的方法分配一个密钥，然后再根据某种规则加入到某一个簇即可。基站也无须与所有簇首重新交换密钥信息[3]。所有这些都大大降低了节点间的通信开销，延长了网络的生存周期。

4 结语

由于无线传感器网络及其节点所独有的特性使得其要达到较高的安全性能变得相当困难，而且还需要面对来自多方面的攻击。因此，为了实现传感器节点间的安全通信，通常需要在节点部署之前，进行密钥的预分配。二元 t 次多项式密钥预分配协议[6]便是在已有的密钥预分配协议上发展起来的，针对无线传感器网络节点的存储空间、能量和计算能力有限的特性，减少了节点间的通信开销[3]。

与其他已有的预分配密钥方案[7]和基于簇的无线传感器网络密钥管理协议[8]相比，可以使网络在遭受节点俘获攻击后有更强的自我恢复能力，从而具有良好的抗毁性，能有效抵御节点的合谋攻击。通信开销也比随机密钥预分配等方案要低。而普通节点只存储一个密钥，极大地节省了存储空间，更加适用于大规模的无线传感器网络。当然，本文只是在理论上对改进后的方案做了评估，下一步的工作将是进行仿真，从实验上验证理论的可行性。

参考文献：

[1] 黄鑫阳，扬明. 无线传感器网络密钥管理研究综述[J]. 计算机应用研究，2007，24(1)：10－15.

[2] 刘良，邓亚平，李钦. 一种基于ID的传感器网络密钥管理方案[J]. 计算机应用，2006，26(10)：2347－2350.

[3] CHENG YI，AGRAWAL D P. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks [J]. Ad Hoc Networks，2007，16(5)：35－48.

[4] ZHANG WEN-SHENG，TRAN M，ZHU SEN-CUN. A random perturbation-based scheme for pairwise key establishment in sensor networks [J]. MobiHoc，2007，32(8)：90－99.

[5] 李军，李录明. 多项式密钥预分配协议在传感器网络上的实现[J]. 计算机工程，2007，33(15)：149－151.

[6] 周贤伟，孙晓辉，覃伯平. 无线传感器网络密钥管理方案的研究[J]. 计算机应用研究，2007，24 (1)：144－147.

[7] 赵治平，林亚平. 传感器网络中基于簇的组密钥管理方案[J]. 计算机工程，2008，34(5)：153－157.

[8] 魏楚元，郝莹，吕橙. 基于簇的无线传感器网络密钥管理协议[J]. 计算机工程与设计，2007，28(20)：4901－4904.

（上接第2979页）

参考文献：

[1] 周成虎，骆剑承，刘庆生，等. 遥感影像地学理解与分析[M]. 北京：科学出版社，1999.

[2] 张红英. 数字图像修复技术的研究与应用[D]. 成都：电子科技大学，2006.

[3] CRIMINISI A，PEREZ P，TOYAMA K. Region filling and object removal by exemplar-based image inpainting [J]. IEEE Transactions on Image Processing，2004，13(9)：1200－1212.

[4] 彭宏京，侯文秀，宫宁生. 改进的基于样例修补的目标移除方法[J]. 计算机辅助设计与图形学学报，2006，18(9)：1345－1349.

[5] 戴磊，魏宝刚. 图像复原的算法研究[J]. 计算机工程与设计，2006，27(2)：184－187.

[6] 袁金国. 遥感图像数字处理[M]. 北京：中国环境科学出版社，2006.

[7] 王贤敏，关泽群，吴沉寒. 遥感影像高逼真度二维信息隐藏盲算法[J]. 计算机工程与应用，2004，40(13)：3－5.

[8] 王贤敏，王乘，周建中等. 一种新的遥感影像不同权限信息隐藏技术[J]. 计算机工程，2006，32(1)：28－30.

[9] 胡英，陈辉，房世波. 数字水印技术在遥感图像版权保护中应用[J]. 计算机仿真，2005，22(3)：200－202.

[10] 陈辉. 数字水印技术及其在遥感图像中的应用研究[D]. 成都：成都理工大学，2005.

[11] 曹荣，王颖，李象霖. 一种自适应的DFT域数字水印算法[J]. 计算机工程与应用，2006，42(10)：77－78.

[12] 王向阳，杨红颖，邬俊. 基于内容的离散余弦变换域自适应遥感图像数字水印算法[J]. 测绘学报，2005，34(4)：324－330.

[13] 党安荣，王晓栋，陈晓峰，等. ERDAS imagine 遥感图像处理方法[M]. 北京：清华大学出版社，2003.