基于边密钥的传感器网络动态密钥协商方案 *

郭江鸿[1], 李兴华[2], 武坚强[1]
(1. 嘉应学院 计算机系, 广东 梅州 514015; 2. 西安电子科技大学 网络与信息安全教育部重点实验室, 西安 710071)

摘 要: 由于传感器自身资源受限,目前采用的主要安全技术是对称密钥与密钥预分配策略。在当前基于对称密钥的动态密钥协商方案中,节点预装入密钥材料,部署后与邻居节点通过共享密钥材料建立配对密钥。为提高动态密钥协商中密钥材料的安全性,在一个典型的动态密钥协商方案,即 LBKP 方案的研究基础上,提出了一种新的基于边密钥的传感器网络动态密钥协商方案。与 LBKP 方案相比,该方案有效地减少了内存开销,提高了密钥安全性。

关键词: 传感器网络; 动态密钥; 网络安全; 密钥材料
中图分类号: TP301 **文献标志码**: A **文章编号**: 1001-3695(2010)03-1029-03
doi:10.3969/j.issn.1001-3695.2010.03.061

Edge key-based dynamic keying scheme for wireless sensor network

GUO Jiang-hong[1], LI Xing-hua[2], WU Jian-qiang[1]
(1. *Dept. of Computer Science, Jiaying University, Meizhou Guangdong* 514015, *China*; 2. *Key Laboratory of Computer Networks & Information Security of Ministry of Education, Xidian University, Xi'an* 710071, *China*)

Abstract: For constraint resources of sensor nodes, existing security approaches are symmetric key and key pre-distribution. In most of existing symmetric key based dynamic keying schemes, pairwise key is established by using the shared keying materials preloaded on sensors. For improving the security of keying materials, this paper proposed an edge key-based dynamic keying scheme (EK-DKS) for wireless sensor network based on the study of a typical dynamic keying scheme——LBKP(location based key pre-distribution) scheme. Compared with LBKP scheme, EK-DKS scheme reduced the storage overhead and improved the security effectively.

Key words: sensor network; dynamic keying; network security; keying material

随着无线传感器网络器网络 (wireless sensor network, WSN)的应用领域日益广泛,相应的研究也在不断深入。在无线传感器网络中,由于无线通信的广播特性,节点间的安全通信问题显得更为重要。以提供安全、可靠的保密通信为目标的密钥管理是 WSN 安全研究最为重要、最为基本的内容,也是其他安全机制的基础。同时,传感器节点资源受限,如有限的数据处理能力。有限的存储空间、有限的计算能力及通信范围等特点,使得传统网络密钥管理的许多成果不能直接应用 WSN,如 RSA 等。目前普遍认为可行的方法是采用密钥预分配方案(key pre-distribution scheme, KPS)。

国外关于 WSNs 密钥协商、分配方案的代表性相关研究成果有 Eschenauer 等人[1] 提出的一种概率密钥共享方式以及 Chan 等人[2] 对该方案的改进;Younis 等人[3] 在层次式 WSN 中提出基于位置信息的 EBS 动态密钥管理方案; Liu 等人[4] 和 Du 等人[5] 结合部署知识提出了基于地理信息的密钥分配方案及多矩阵空间密钥分配方案进行动态密钥协商,有效地提高了网络的密钥连通率。国内对 WSNs 密钥协商及密钥建立、分配方案的成果有苏忠等人[6] 对当前传感器网络的密钥管理进行了综合论述;陈克非等人[7] 研究了无线传感器网络中对密钥管理的评估指标问题,对目前比较流行的基于 KDC 和基于预先配置这两种密钥管理方案进行了分析;刘志宏等人[8] 讨论了随机预分配密钥中区域重叠因子对网络连通性及安全性的影响;王佳昊等人[9] 讨论了随机预分配密钥在无线传感器网络跟踪算法中的应用等。

在 Liu 的基于对称密钥的动态密钥协商方案——LBKP 方案(location-based key pre-distribution scheme, LBKP)[6] 中,使用对称多项式作为密钥材料预装入传感器节点中,并在部署后利用邻居间的共享多项式建立配对密钥。同时,利用部署知识得到高的密钥连通率,并利用密钥材料的门限安全提供一定的密钥安全性。本文在 LBKP 方案的基础上提出了一种新的基于边密钥的传感器网络动态密钥协商方案 EK-DKS(edge key-based dynamic keying sheme),提高了安全性。

1 简介 LBKP 方案

Liu 提出了使用基于地理信息的对称二元多项式随机密钥预分配方案[6],简称 LBKP 方案。该方案把部署目标区域划分为若干个大小一致的正方形区域。部署前,部署服务器生成与区域数量相等的对称 t 阶二元多项式,并为每一区域指定惟一的二元多项式。对于每一节点,根据其期望位置来确定其所处区域,部署服务器把与该区域相邻的上、下、左、右四个区域

收稿日期: 2009-06-24; **修回日期**: 2009-07-26 **基金项目**: 国家自然科学基金资助项目(60702059)

作者简介:郭江鸿(1975-),男,山西长治人,讲师,硕士,主要研究方向为无线移动安全等(g_jh@jyu.edu.cn);李兴华(1977-),男,副教授,博士,主要研究方向为网络与信息安全等;武坚强(1975-),男,讲师,主要研究方向为信息安全、图像处理等.

以及节点所在的区域共五个二元多项式共享载入该节点。部署后,两个节点若共享至少一 个二元多项式就可以直接密钥协商。与 E-G 方案[4]和 q-composite 方案[7]相比,LBKP 方案有效地提高了密钥连通率与安全性。

在 LBKP 方案中,每个区域对应分组中的节点存储五个多项式,以保证与任一邻居分组中的节点均可建立安全通信。每个多项式被五个区域对应分组中的所有节点拥有,同时,每个节点存储五个对称多项式对应的秘密分量,如图 1 所示。

2　EK-DKS 简介

2.1　基本思想

现有的大部分基于对称密钥的动态密钥协商方案中,都使用对称多项式或对称矩阵作为密钥材料来提供门限安全。在给定网络规模下,密钥材料的安全性取决于网络中拥有该密钥材料部分信息(如多项式的秘密分量)的节点数目。显然,这部分节点占总节点数比例越大,则敌手随机捕获一个节点含有该密钥材料部分信息的概率越大,即安全性越低。在 LBKP 方案中,主要通过减少节点密度等方式来减少网络中拥有某密钥材料部分信息(如多项式的秘密分量)的节点数目,提高密钥材料的安全性。本文方案则在预分配阶段通过不同的密钥材料的生产及分配方式,从开始就减少拥有某多项式秘密分量的传感器节点数目,来提高安全性。

LBKP 方案中,为每个区域生产一个多项式,称之为区域多项式,该多项式同时被本区域及上、下、左、右四个邻居区域共享。对于每个节点,将存储五个多项式分量;对于每个多项式,网络中共有五个区域的节点拥有该多项式的秘密分量。若部署目标划分为 N 个区域,则对每个多项式而言,含有该多项式秘密分量的节点数目占总节点数的比例为 $5:N$。

与 LBKP 方案不同的是,本文不是为每个区域生产一个多项式,而是为区域中的每条边生成一个多项式,称为边密钥或边多项式,是本文方案中节点间进行动态密钥协商使用的密钥材料,所用本文方案叫做基于边密钥的无线传感器网络动态密钥协商方案。显然,每条边连接两个区域,即每个边密钥被两个区域中的节点共享。这样,对于任意节点,将存储节点所在区域四条边对应的四个边多项式秘密分量;对于每个边多项式,网络中有两个区域的节点拥有该多项式的秘密分量。同样设部署目标划分为 N 个区域,则对每个多项式而言,含有该多项式秘密分量的节点数目占总节点数的比例为 $2:N$。显然,任一被俘节点含有某多项式秘密分量的概率小于 LBKP 方案中的 $5:N$,即为暴露某多项式,敌手需捕获更多的节点,密钥安全性得到了提高,如图 2 所示。

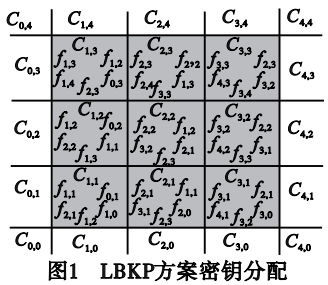

图1　LBKP方案密钥分配

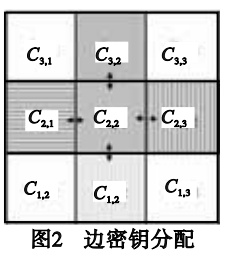

图2　边密钥分配

2.2　EK-KDS 方案简介

EK-KDS 方案建立在 Liu 等人基于地理信息的对称二元多项式随机密钥预分配方案(LBKP)基础上,分为三个阶段,即密钥预分配阶段、共享密钥发现阶段和路径密钥发现阶段。其中,再预分配阶段采用不同的密钥材料生成及分配方式,以减少网络中拥有某个多项式对应秘密分量的节点数目,达到提高安全性的目的;共享密钥发现阶段及路径密钥发现阶段与 LBKP 方案相同,都是利用节点间的共享多项式计算配对密钥或通过多跳路径建立密钥。

2.2.1　密钥预分配阶段

密钥预分配阶段,部署服务器生成与区域边数相等的有限域 F_q 上的对称 t 阶二元双变量对称多项式 f,为每个多项式建立相应索引,q 为素数,且 F_q 要足够大以容纳所有多项式系数。网络中全部节点按照区域数量进行分组,一个分组中所有节点的期望位置为同一区域,部署服务器为每个节点计算其所在区域的四条边对应的对称多项式秘密分量并装入节点中。其中每个边多项式仅被某区域及其某一个邻居区域共享。t 阶多项式有 t 安全门限,即不超过 t 个拥有与某多项式对应的秘密多项式分量的节点被俘,多项式仍然安全。

2.2.2　共享密钥发现

1)每个节点在其通信范围内广播节点 ID 与多项式索引。考虑到安全性因素,可对多项式索引进行加密。例如,节点 A 可以先广播其 ID,然后利用存储的秘密多项式和邻居节点 ID 对索引进行加密[5],形成一个加密索引链表并发送给邻居节点。那些知道节点 A 的 ID 且与 A 有共享多项式的邻居节点可以正确解密加密索引链表中的一个或多个消息,进而得到节点 A 的多项式索引。

2)节点间通过多项式索引,发现共享多项式。

3)邻居节点间通过共享多项式建立密钥。

设两个有共享双变量二元对称多项式 $f(x,y)$ 的邻居节点 u、v 的 ID 分为 k、j,被服务器事先计算并预装入的秘密分量为 $f(k,y)$、$f(j,y)$。两个节点以对方 ID 为输入分别计算 $f(k,j)$ 与 $f(j,k)$。由于多项式的对称性,有

$$f(k,j)=f(j,k)=k_{u,v} \tag{1}$$

节点 u、v 以 $k_{u,v}$ 作为它们之间的通信密钥。

2.2.3　路径密钥发现

与 LBKP 方案相同,当两个无共享多项式的邻居节点通信时,可通过多跳路径进行间接密钥协商。例如节点 u、v 是邻居节点,分别属于 $C_{2,2}$ 与 $C_{3,1}$,无共享多项式,则可通过一定的路由算法寻找一个中间节点 i,i 与 u、v 分别有共享多项式,即 i 属于 $C_{3,2}$ 或 $C_{2,1}$,与节点 u 和 v 可进行直接密钥协商得到会话密钥 $K_{ui}(k)$、$K_{iv}(k)$,则 u 可选择一随机密钥 k 作为 u、v 间的会话密钥,将 $K_{ui}(k)$ 发送给节点 i,i 再生成 $K_{iv}(k)$ 发送给 v。

2.2.4　节点加入及去除

在传感器网络生存期内,可能需要加入新的节点以取代损坏或被俘的节点。为了加入一个新节点,部署服务器需为该节点预装入上文中的五个秘密多项式。

出于安全性考虑,有时也需要从传感器网络中去除部分节点,如被俘节点等。假设有某些异常节点的检测方法,可以判定节点是否被俘。为了去除被俘节点,那些与被俘节点有共享多项式的节点需要将被俘节点的 ID 存入本地黑名单,并删除对应的密钥。当黑名单中与某个共享多项式对应节点 ID 数目超过多项式次数 t 时,则去除对应的秘密多项式分量及黑名单中拥有该秘密多项式的被俘节点 ID。

3　性能分析

本文主要从连通率、安全性、方案开销(包括存储开销、通

信开销、计算开销)等方面对 EK-DKS 进行性能分析。设网络规模 N 为 10^4 个传感器节点,目标区域面积为 $10^3 \times 10^3\ m^2$,节点通信半径为 40 m,区域边长为 L,节点存储容量 m 为 200 个密钥,节点服从正态分布,标准方差为 σ,部署半径为 3σ。

3.1　连通率分析

本文使用与 LBKP 方案相同的方法对连通率进行分析(限于篇幅,文中不再进行连通率的推导,具体过程可参见文献[6])。设节点服从正态分布,邻居部署点间的距离 $d = a \times \sigma$,$\sigma = 50$ 为标准方差,即区域边长 $L = d$。图 3 为给定部署半径时,不同区域边长下连通率分析(以 σ 为单位长度)。从图中可看出,给定部署半径为 3σ 时,当 L 较小时,某节点与少部分邻居节点进行直接密钥协商。由于密钥分配方式不同,在 EK-DKS 中,某区域与其对角邻居区域无共享多项式,在 L 较小时密钥连通率劣于 LBKP 方案;随着 L 的增加,某节点的邻居节点中来自本区域及邻居区域的节点所占比例随之增加,网络连通率也在不断提高,EK-DKS 方案仍然到达了很高的网络连通率。

3.2　安全性分析

本文采用与 LBKP 方案相同的标准衡量节点被俘对非被俘节点间通信链路的影响,即用某个秘密多项式暴露的概率衡量非被俘节点间通信链路受损比例。

某秘密多项式被俘的概率 p_c 为

$$p_c = 1 - \sum_{i=1}^{t} C_n^i p^i (1-p)^{n-i} \qquad (2)$$

其中:P_c 为某秘密多项式被俘的概率;n 为网络中拥有该 t 次多项式秘密分量的节点数;p 为任一被俘节点含有该多项式对应秘密分量的概率,对应 LBKP 方案,$p = 5/N$,对应 EK-DKS 方案,$p = 2/N$,N 为网络中划分的区域总数。

两种方案的安全性比较如图 4 所示。其中区域边长 L = 100,节点存储容量 m 为 200 个密钥,每个区域对应的节点分组中的节点数目为 100 个。对于 LBKP 方案中的任一多项式(多项式次数为 39),网络中有 500 个节点拥有其对应的秘密分量;对于 EK-DKS 方案中的任一多项式(多项式次数为 39),网络中最多有 200 个节点拥有其对应的秘密分量(其中预分配的对应与区域的秘密多项式仅为本区域对应节点分组中 100 个节点共享,对于预分配的与边邻接邻居区域的共享秘密多项式,为 2 个区域中共 200 个节点共享),是相同多项式次数下的安全性比较。

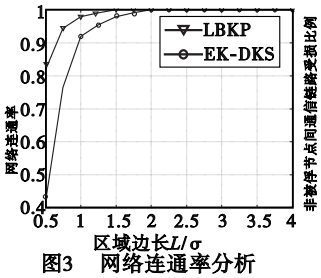

图3　网络连通率分析

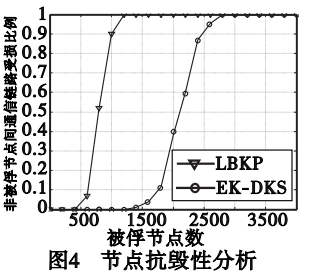

图4　节点抗毁性分析

如前所述,在给定密钥存储空间及多项式安全门限,即多项式次数下,多项式的暴露概率取决于网络中拥有该多项式对应秘密分量的节点数目占总节点数的比例。该比例越大,意味着敌手任意捕获的节点中含有该多项式对应秘密分量的概率越大,即为暴露该多项式,敌手需付出的代价较小。显然,在上设网络环境下,当被俘节点超过 1 200 时,LBKP 中的秘密多项式将暴露;在 EK-DKS 方案中,被俘节点超过 2 800 时,秘密多项式将暴露。在相同的多项式次数下及网络规模下,本文方案中的安全性远高于 LBKP 方案。

3.3　方案开销分析

1)存储开销　节点的存储开销最主要的是存储各秘密多项式系数所需的存储空间。对于 LBKP 方案,每个节点要存储预分配的 5 个 t 次秘密多项式分量,需占用 $5(t+1)\log F_q$ 的存储空间;对于 EK-DKS 方案,每个节点要存储预分配的 4 个 t 次秘密多项式分量,需占用 $4(t+1)\log F_q$ 的存储空间。显然,本文方案的存储开销较优。

2)通信开销　对于两种方案,建立配对密钥的通信开销主要来自于共享密钥发现。邻居节点间为发现共享密钥,需广播自己的 ID 及多项式索引(可加密形成多项式索引链表以提高安全性),以及对邻居节点广播消息的确认,通信开销为 $O(2)$。

3)计算开销　为了建立配对密钥,两种方案中节点均需对 t 次多项式进行计算,计算开销为 t 次模乘及 t 次模加。计算开销取决于多项式次数。

两种方案都采用多项式作为建立密钥的工具,在相同的多项式次数下,使用不同的密钥分配方式不会影响节点间建立配对密钥所用计算开销及通信开销。

4　结束语

传感器网络的密钥分配一直是研究的热点问题之一。本文在基于 LBKP 密钥预分配方案及部署知识的基础上,提出一种新的基于边密钥的传感器网络密钥动态密钥协商方案——EK-DKS 方案。通过改变密钥的生成及分配形式,在保证高的网络连通率的基础上,在预部署阶段就有效地减少了网络中拥有某秘密多项式秘密分量的节点数目占总节点的比例,在减小节点存储开销的基础上,有效地提高了安全性。

参考文献:

[1] ESCHENAUER L, GLIGOR V. A key management scheme for distributed sensor networks[C]//Proc of the 9th ACM Conference on Computer and Communications Security. New York: ACM Press, 2002:41-47.

[2] CHAN Hao-wen, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]//Proc of IEEE Symp on Security and Privacy. Washington DC: IEEE Computer Society, 2003:197-213.

[3] YOUNIS M, GHUMMAN K, LTOWEISSY M. Location-aware combinatorial key management scheme for clustered sensor networks[J]. IEEE Trans on Parallel and Distribution System, 2006, 17(8): 865-882.

[4] LIU Dong-gang, NING Peng. Location-based pairwise key establishments for static sensor networks[C]//Proc of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks. New York: ACM Press, 2003:72-82.

[5] DU Wen-liang, DENG Jing, HAN Y S, *et al*. A pairwise key predistribution scheme for wireless sensor networks[C]//Proc of the 10th ACM Conference on Computer and Communications Security. Washington DC: ACM Press, 2003:42-51.

[6] 苏忠,林闯,封富君,等. 无线传感器网络密钥管理的方案和协议[J]. 软件学报,2007,18(5):1218-1231.

[7] 陈克非,陈菲,宋志高. 无线传感器网络中对密钥管理评估指标研究[J]. 计算机仿真,2005, 22 (5):137-140.

[8] 刘志宏,马建峰,黄启萍. 基于区域的传感器网络密钥预分配方案[J]. 计算机学报, 2006, 29(9):1608-1616.

[9] 王佳昊,王胜坤,秦志光,等. 随机预分配密钥在 WSN 跟踪算法中的应用[J]. 四川大学学报,2005,27(11):113-119.