自组网中基于簇的预密钥管理方案

许 力，章 静

(福建师范大学数学与计算机科学学院 福州 350007)

【摘要】自组网是由无线节点组成的不需要固定基站的临时性的计算机通信网络。以提供安全、可靠的保密通信为目标的密钥管理方案和协议的设计是自组网安全中一个重要的研究课题，自组网的多跳通信和资源受限等固有特性使得密钥管理面临许多挑战。该文在基于团的快速分簇算法的基础上，提出了一种基于簇的分层密钥预分配方案。分析表明，相比于传统随机密钥预分配方案，新方案不仅能够提高网络的连通性，而且可以减少节点所需存储空间。

关 键 词 自组网; 分簇; 预密钥分发; 安全性

中图分类号 TP389.1 文献标识码 A

Cluster-Based Key Pre-Distribution Scheme for Ad hoc Networks

XU Li，ZHANG Jing

(School of Math and Computer Science, Fujian Normal University Fuzhou 350007)

Abstract Ad hoc Network is a collection of wireless nodes forming a temporary computer communication network without the aid of any established infrastructure or centralized administration. The design of key management schemes and protocols, whose main objective is to provide secure and reliable communication, is one of the most important aspects and basic research filed of secure ad hoc networks. The key management in ad hoc network meets many new challenges due to its intrinsic properties such as multi-hip communication, limited resource and so on. In this paper, a method to improve the random key pre-distribution scheme based on cluster scheme is proposed. The comparison to random key pre-distribution scheme shows that the new approach can substantially improve the connectivity of network and reduce the amount of memory required at the same time.

Key words Ad hoc networks; cluster; key pre-distribution; security

自组网[1]由一些相互通信的移动节点组成，节点间的通信不需要通过已存的通信设施。在其无线通信范围内的节点是直接通信的，而一些相隔很远的节点间的通信要通过中间节点来传递消息。尽管自组网很容易快速部署和方便地移动，但是这种网络与生俱来的弱点(如受到窃听、伪造、拒绝服务等攻击)使得它很容易受到恶意的攻击。为保证自组网络安全运行，节点间的通信应加密，重要的网络数据需认证。要达到此目的，首先必须解决密钥分配问题，在相互通信的节点间建立会话密钥。

由于自组网络特性，不宜采用公钥密码[2]，应采用对称加密算法、低能耗的认证机制和Hash函数。在传统网络中使用的基于可信第三方的密钥分配协议[3]也不适用于自组网络。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)，把需要的密钥预先分发给节点。

1 相关工作

KPS有多种实现方法。文献[4]提出一种随机密钥预分配方案R-KPS(Random Key Pre-distribution Scheme)，自组节点在部署前，从生成的密钥池(Key Poo1)中随机选取一定数目的密钥子集，节点部署到指定簇后，通信双方在各自的密钥子集中寻找共同密钥，每对节点协商密钥时，只需在各自的密钥子集中找到一个共同密钥。在此方案基础上，文献[5]提出q重随机密钥预分配方案(q-Compositerandom Key Pre-Distribution Scheme)，如果一对节点之间要进行安全通信，则必须在各自的密钥子集中找到至少q个共同密钥。文献[8]利用正交向量表快速生成cover free family，并进行密钥预分配，同时在连通性和抗合谋两方面取得较好的性能。文献[9]基于LU Deco- mposition提出了计算复杂度较低的密钥预分

收稿时间：2007 – 09 – 14

基金项目：国家自然科学基金(60502047)；福建省自然科学基金(A0440001)

作者简介：许 力(1970 –)，男，博士，副教授，主要从事无线网络与移动计算、网络与信息安全方面的研究；章 静(1970 –)，女，硕士，主要从事自组网优化和安全方面的研究.

发策略。文献[6]在随机密钥分配方案基础上，提出一种适用于无线传感器网络的利用部署和位置信息的KPS方案。本文受文献[6]研究工作的启发，在分簇算法的基础上，针对自组网特性进行改进，消除了节点需定位的缺点，并考虑两两邻居簇间不同重叠因子，提出了基于簇的随机密钥预分配方案(Cluster-Based Random Key Pre-distribution Scheme，CB-KPS)。网络进行分簇算法后，覆盖范围划分为较小的簇，节点按照所属簇部署密钥，在一定程度上能提高相邻节点共享密钥的概率。

2 CB-KPS的设计

自组网络节点通常只与邻居节点直接通信。如果能把大的网络覆盖范围划分为较小的簇，密钥池同样划分为与簇相对应的子集，节点按簇的划分从相应的密钥子集中选取密钥，可以使同一簇内节点的共享密钥概率提高。相邻簇之间的节点通过密钥子集的重叠可以达到一定的共享密钥概率。

自组网划分为多个簇后，每个簇具有不同的簇标识，可以把节点获得的信息与所在簇地理位置相联系。本文采用基于团的分簇算法[7-10]，可将网络划分为若干个簇，每个簇头(Cluster Head，CH)负责一个簇。

基于团的分簇算法步骤有：

(1) 任意选取若干发起者；

(2) 以此点为中心求其一跳补图；

(3) 得到最小度数点 u，设 u 的颜色为1；

(4) 中心点的一跳邻居启动计时器T，T先消亡者为中心并赋上颜色2，并将其为中心的消息发给其邻居节点；

求新中心节点的一跳补图时有两种情况：一是补图中有与上次中心节点相连的点，若相连的点只有一个，则以此节点为中心，并赋上颜色1，若相连的节点大于一个，则再次启动倒计时T，T先消亡者胜出，赋上颜色1，回到步骤(2)；二是若与上次中心无连接的点，回到步骤(4)。赋上颜色2的节点为网关节点。

为了确定簇标识，发起者标记上自己的簇标识(a,b)；每个选定的CH上用四个定向天线，$\angle\alpha=\angle\beta=\angle\lambda=\angle\varphi=90°$，且$\angle\alpha$、$\angle\lambda$以正东方为角平分线，$\angle\beta$、$\angle\varphi$以正北方为角平分线，如图1所示；经过一次算法得到的CH，回复消息给上一CH(a, b)，CH(a, b)先收到若干CH的消息后判断其簇标识。若在$\angle\alpha$区域，节点标识为CH$(a, b+1)$；若在$\angle\beta$区域，节点标识为CH$(a-1, b)$；若在$\angle\lambda$区域，节点标识为CH$(a-1, b-1)$；若在$\angle\varphi$区域，节点标识为CH$(a+1, b)$；若在线L_1上，节点标识为CH$(a-1, b+1)$；若在线L_2上，节点标识为CH$(a-1, b-1)$；若在线L_3上，节点标识为CH$(a+1, b-1)$；若在线L_4上，节点标识为CH$(a+1, b+1)$。重复直至所有簇头拥有了簇标识。

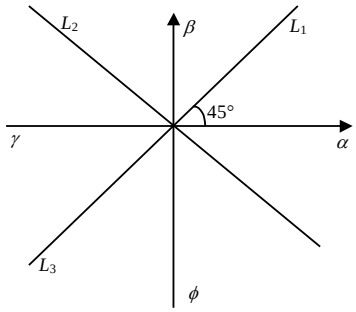

图1 簇标识判断

文献[4]提出的随机密钥预分配方案分为三个阶段：密钥预分配、共享密钥发现和路径密钥建立。本文提出的方案以此为基础。

2.1 密钥预分配阶段

首先根据任务需求把网络覆盖范围划分为多个簇，并通过簇标识算法拥有了各自的簇标识CH(i, j)，然后由网络管理者生成密钥池S，并把S分成不同的子密钥空间subset(i, j)，每一个子密钥空间与一个簇对应。相邻簇之间的子密钥空间有部分重叠，重叠因子C表示相邻区域子密钥空间重叠部分在子密钥空间中所占的比例。各邻居簇重叠部分是不一致的，故重叠因子也是各异的。C的判断方法为：由坐标为(i, j)的CH发送其所在邻居节点ID给$(i, j-1)$的CH，由$(i, j-1)$的CH计算(共同节点/CH$(i, j-1)$邻居)，定义为C_{ij}；同样由坐标为(i, j)的CH发送其所在邻居节点ID给$(i-1, j)$CH，由$(i-1, j)$的CH计算(共同节点/CH$(i-1, j)$邻居)，定义为C_{ij}'。本文只考虑四个方向上的重叠因子，其他方向暂不考虑。此外，所有节点需要发送(C_{ij}, C_{ij}'，自身簇标识)给所有(a, b)，其中$a>i, b>j$，若未收到以0计算，以便(a, b)计算其子密钥空间坐标。

设自组网在物理上分成$M\times N$个簇，密钥池S组织成一个$(M\times r)\times(N\times r)$的密钥矩阵($r$是密钥矩阵系数，由密钥池大小决定)。每个CH$(i, j)$对应密钥矩阵的一个子集subset$(i, j)$，因采用的是一跳的分簇算法，故各簇大小视为相同，对应的子密钥空间大小也相同，处于CH(i, j)中的节点从其对应的子密钥空间subset(i, j)中随机选取m个不同密钥作为节点的密钥链。簇与子密钥空间之间的映射关系如图2所示。

CH(i, j)所对应的子密钥空间subset(i, j)是密钥矩阵的子矩阵，设图2中的subset(i, j)左上角和右下角的元素为A，B，则下标(x, y)和(x', y')由式(1)计算得到。

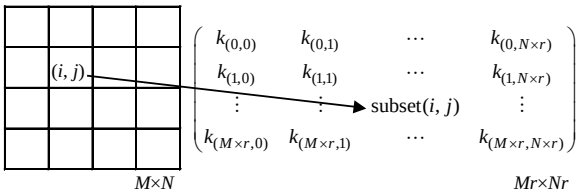

图2　簇与子密钥空间之间的映射关系

$$\begin{cases} x = \dfrac{Mr}{M - \sum_{k=1}^{M-1} C_{kj}} (i - \sum_{k=1}^{i} C_{kj}) \\ y = \dfrac{Nr}{N - \sum_{k=1}^{N-1} C_{ik}'} (j - \sum_{k=1}^{j} C_{ik}') \end{cases} \tag{1}$$

$$\begin{cases} x' = \dfrac{Mr}{M - \sum_{k=1}^{M-1} C_{kj}} (i+1 - \sum_{k=1}^{i+1} C_{kj}) - 1 \\ y' = \dfrac{Nr}{N - \sum_{k=1}^{N-1} C_{ik}'} (j+1 - \sum_{k=1}^{j+1} C_{ik}') - 1 \end{cases}$$

式中　C为重叠因子；r为密钥矩阵系数；M和N表示网络分为$M\times N$个簇。

2.2　共享密钥的发现和路径建立

经过初始化配置之后，每个节点都得到了一个密钥集。用这些密钥来进行相互间的通信的步骤如下：首先，每个节点需要知道它同周围的节点共享了哪些密钥，为此每个节点p要广播一条包含了它拥有的密钥的索引值的消息。邻居节点(如q)收到消息之后，就得知了它跟广播消息的节点p共享的密钥有哪些。同时节点p同样也会收到节点q广播的包含密钥索引值的消息。如果邻居节点q需要验证节点p是否知道某个密钥，它们就可以进行一次握手。这一步结束之后，一个共享密钥或者说安全连接的连通图就形成了。整个协议的流程如图3所示。

假设节点i和节点V_1共享密钥k_1，节点V_1和节点V_2共享密钥k_2，节点V_2和节点V_3共享密钥k_3，节点V_3和节点j共享密钥k_4。接下来，节点i首先产生一个随机的对称加密密钥SK，会将消息e(SK)k_1发送给节点V_1。节点V_1收到e(SK)k_1后，先找到在这条路径上的下一个节点V_2，选择一个它们之间共享的密钥k_2，将消息先用k_1解密，然后用k_2加密得到e(SK)k_2，发送给节点V_2。节点V_2和节点V_3会执行同节点V_1相同的操作步骤。节点j最终收到消息e(SK)k_3，它用密钥k_3解密这个消息，就可以得到节点i要传给它的会话密钥了。接下来它们之间的通信就会通过这个密钥来加密。当节点V_1、V_2、V_3收到数据包的时候就不需要再加密解密了，它们只要找出路径上的下一个节点，将消息发给它就可以了。此方法的安全性好，并且实现了更好的网络效率。

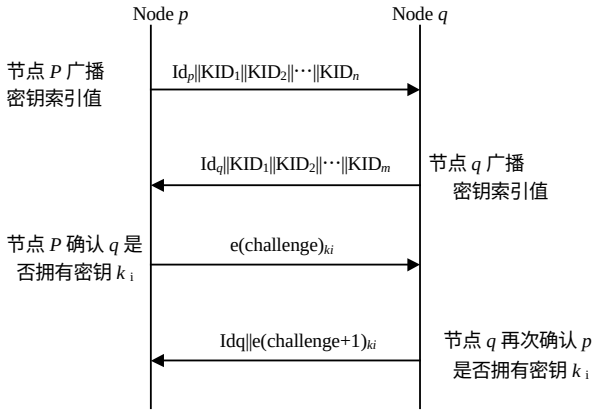

图3　协议的流程图

密钥更新：在一个节点的密钥集中的大部分密钥都被攻陷或者密钥池中的大部分密钥都被攻陷；或每隔一段时间(如一天或一周)会对节点的密钥集和簇头的密钥池进行更新的情况下，需要更新密钥池和Ad hoc网络中节点的密钥集。

3　性能分析

依据文献[6]的指标来分析本文提出的策略的性能，要使随机密钥预分配方案能达到要求的网络连通概率>0.99，则要满足$P_{\text{share}}>P_{\text{locol}}$，其中$P_{\text{share}}$为网络不分簇中任意两节点共享一个密钥的概率，由式(2)表示；P_{locol}为节点与邻居之间的本地连通概率。如果采用分簇，P_{ij}表示CH(i，j)内任意两节点共享一个密钥的概率，Q_{ij}为相邻节点共享一个密钥的概率，由式(3)表示。

图4是分簇与不分簇两种情况下，S=10 000时，P_{ij}和Q_{ij}的随机密钥链长度变化曲线，可以看出$P_{ij}>Q_{ij}>P_{\text{share}}$。

$$P_{\text{share}} = 1 - \frac{((s-m)!)^2}{s!(s-2m)!} \tag{2}$$

$$P_{ij} = 1 - \frac{((\omega - m)!)^2}{\omega!(\omega - 2m)!}, \quad P_{ij}' = 1 - \frac{((\omega c - mc)!)^2}{(\omega c)!(\omega c - 2mc)!} \tag{3}$$

式中　$\omega = \dfrac{s}{(N - \sum_{k=1}^{N-1} C_{ik}')(M - \sum_{k=1}^{M-1} C_{kj})}$。

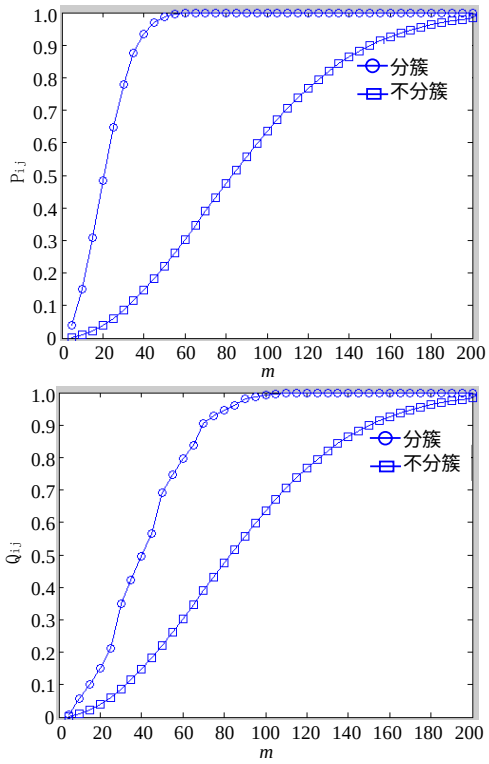

图4 P_{ij}和Q_{ij}的随机密钥链长度变化曲线

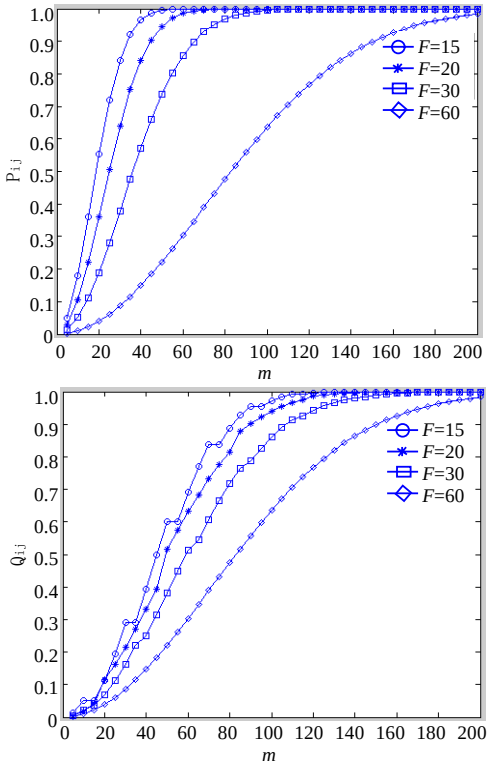

图5 不同传输半径时，P_{ij}和Q_{ij}随m变化的曲线

不同的传输半径，相应的重叠因子也不同，所分簇数量也有所变化，不同的传输半径对共享密钥概率有影响。图5为S=10 000时，P_{ij}、Q_{ij}随m变化的曲线。可以看出，随着半径的减小，P_{ij}、Q_{ij}增加，超过不分簇的概率值。共享密钥概率的提高意味着更多的邻居节点可以在共享密钥发现阶段得到。

采用分簇算法，密钥池S可以扩大，图6是m=150时，不同传输半径情况下共享密钥概率P_{ij}、Q_{ij}随S变化曲线。密钥池越大，共享密钥的概率越低；在密钥池大小确定时，半径越小，共享密钥的概率越大。

在保证相同共享密钥概率的前提下，如果能把网络进行分簇，节点的密钥链长度就可以减小。图7是在P_{ij}、Q_{ij} 都取0.5，S=10 000，采用不同半径时所要求的节点密钥链长度。从图7可以得出，当半径为15时，在同等共享密钥概率的情况下，其密钥链长度比半径为60时可以减小一半以上。

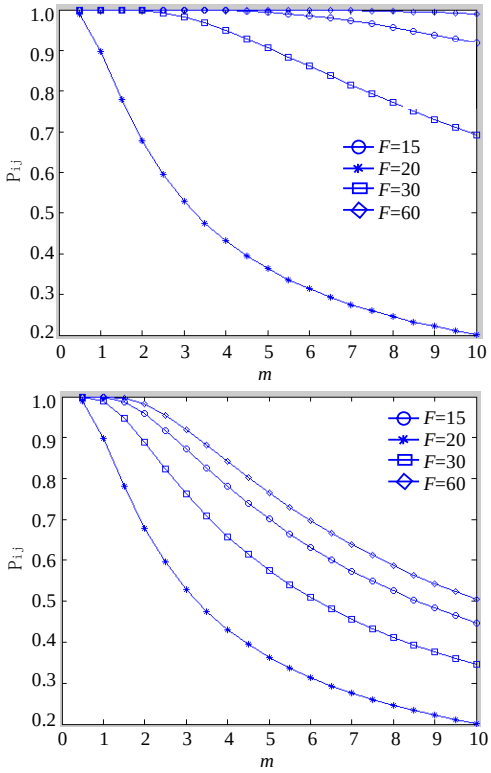

图6 不同传输半径时，P_{ij}和Q_{ij}随S变化的曲线

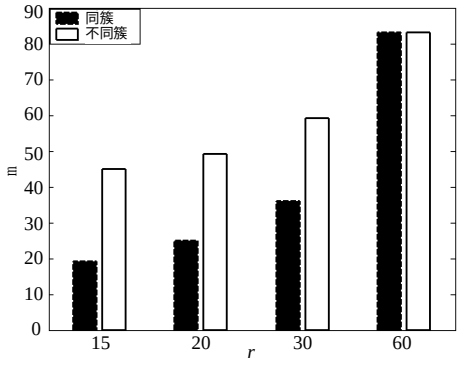

图7 不同半径时所要求的节点密钥链长度

5 总　结

自组网络的安全机制有自身的特点，其密钥分配和管理一直是研究的热点问题之一。本文在随机密钥预分配方案基础上，通过引入分簇方案，提出基于簇的自组网络密钥预分配方案，并进行了性能分析，其性能相比随机密钥预分配方案有一定提高。

参　考　文　献

[1] RAM R, JASON R. A brief overview of mobile Ad Hoc networks: challenges and directions [J]. IEEE Communications Magazine, 2002, 40(5): 20-22.

[2] CARMAN D W, KRUUS P S, MATT B J. Constraints and ap-proaches for distributed sensor security. [2007-07-08]. [J/OL]. http://www.cs.umbc.edu/courses/graduate.

[3] NEUMAN B C, TSO T K. An authentication service for computer networks IEEE Communications[J]. 1994, 32(9): 33-38.

[4] 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: [s.n.], 2002: 4l-47.

[5] CHAN H, PERRIG A, SONG D. Random key edist rjbuti0n schem es for sensor networks[C]//The Proceedings of the IEEE Symposium on Security and Privacy, Berkeley. California: IEEE, 2003: 197-213.

[6] 刘志宏, 马建峰, 黄启萍. 基于区域的无线传感器网络密钥管理[J]. 计算机学报, 2006, 29(9): 1608-1616.

[7] 章　静, 许　力, 林志伟. 自组网中基于簇的混合密钥管理策略[J]. 计算机应用, 2006, 26(6): 1328-1330.

[8] CHEN Jiang-wei, LI Xu, YI Mu. A new group rekeying scheme based on t-packing designs for Ad Hoc networks [M/CD]. The Proceeding of INFOSCALE2007. ACM Press. 2007.

[9] SUNG J C, HEE Y Y. An efficient key pre-distribution scheme for secure distributed sensor networks[C]//EUC 2005 workshops, Lecture Notes in Computer Science.[S. l.]: Springer-Verlag, 2005, 3823: 1088-1097.

[10] LIN Zhi-wei, LI Xu, WANG Da-jin, et al. A coloring based backbone construction algorithm in wireless Ad hoc network[C]//Advances in Grid and Pervasive Computing. The Proceedings of GPC 2006, Lecture Notes in Computer Science. [S. l.]: Springer Press, 2006.

编　辑　税　红

(上接第1154页)

[5] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE public key cryptosystem by relinearization[C]//CRYPTO 1999. Heidelberg: Springer, 1999, LNCS 1666: 19-30.

[6] PATARIN J. Hidden field equations and isomorphisms of polynomials: two new families of asymmetric algorithms[C]//EUROCRYPT 1996. Heidelberg: Springer, 2007, LNCS 1070: 33-48.

[7] GOUBIN L, COURTOIS N. Cryptanalysis of the TTM cryptosystem[C]//ASIACRYPT 2000. Heidelberg: Springer, 2000, LNCS 1976: 44-57.

[8] YANG B, CHEN J. Building secure tame-like multivariate public key cryptosystems the new TTS[C]//ACISP 2005. Heidelberg: Springer, 2005, LNCS 3574: 518-531.

[9] COURTOIS N, KLIMOV A, PATARIN J, et al. Efficient algorithms for solving overdefined systems of multivariate polynomial equations[C]//EUROCRYPT 2000. Heidelberg: Springer, 2000, LNCS 1807: 392-407.

[10] YANG B-Y, CHEN J, COURTOIS N. On asymptotic security estimates in XL and Gröbner bases-related algebraic cryptanalysis[C]//ICICS-2004. Heidelberg: Springer, 2004, LNCS 3269: 401-413.

编　辑　黄　莘