计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
45(1):165~171, 2008

基于通信半径动态调整的无线传感器网络密钥管理协议

陈海坤　石胜飞　李建中
(哈尔滨工业大学计算机科学与技术学院　哈尔滨　150001)
(haikun.chen@yahoo.com.cn)

A Key Management Scheme Based on Variable Transmission Range in Wireless Sensor Networks

Chen Haikun, Shi Shengfei, and Li Jianzhong
(*College of Computer Science & Technology, Harbin Institute of Technology, Harbin* 150001)

Abstract　Establishing a pair-wise key between nodes is important to secure communications in wireless sensor networks. Because traditional solutions for key management are difficult to implement in a resource-constrained environment, several methods, such as key pre-distribution, have been proposed to achieve the goals of data secrecy and integrity. In this paper, a new key management scheme KMVTR based on variable transmission range of sensor nodes is proposed. This scheme uses group-based deployment method and pre-distributes keys in groups and between groups. In each group, there are certain special nodes which can assist nodes from adjacent groups in establishing a pair-wise key. The KMVTR scheme can use the powerful senior nodes act as such special nodes, and can also use normal nodes act as such special nodes. The theory analysis and simulation result shows that the connect probability of two adjacent groups will be high enough when using normal nodes act as special nodes. The analysis also shows the communication energy cost of the KMVTT scheme is acceptable for wireless sensor networks. Compared with other methods, the KMVTR scheme has several advantages such as providing perfect resilience against node capture, supporting larger network size, and doesn't have to know the expected locations of sensor nodes in key pre-distributed phase.

Key words　wireless sensor networks; security; key management; key pre-distribution; variable transmission range

摘　要　为了实现传感器网络的安全,对节点间传送的数据进行加密解密是非常重要的,这需要在节点间建立共享密钥对.由于传感器节点的资源有限,传统分发密钥的方法不能应用在无线传感器网络中.目前已经有研究者提出若干种密钥预分布方法来保证传感器网络的安全.利用传感器节点通信范围可调节的特点,提出了一种新的基于通信半径动态调整的密钥预分布方案KMVTR.该方案不仅适用于具有大通信距离的高级节点的网络,而且同样适用于只有普通节点组成的网络.和其他方案相比,KMVTR具有若干优点,如提供最佳的抗节点俘获的能力,并且可以支撑较大的网络规模,而且在预分布阶段不需知道节点的期望部署位置.

关键词　无线传感器网络;安全;密钥管理;密钥预分配;通信半径可调

中图法分类号　TP393.08

收稿日期:2007-05-31;**修回日期**:2007-06-27

基金项目:国家自然科学基金重点项目(60533110);国家"九七三"重点基础研究发展规划基金项目(2006CB303000);国家自然科学基金项目(60473075,60703012,60773068,60773063);黑龙江省自然科学基金重点项目(ZJG03-05);国家教育部新世纪优秀人才支持计划基金项目(NCET-05-0333);黑龙江省青年科技专项基金项目(QC06C033)

无线传感器网络作为一种特殊的自组织无线网,由集成了无线通信模块、微处理器、微型传感器及资源有限的节点组成,节点间通过无线通信协助完成各种任务[1-2]. 安全问题是无线传感器网络中的一个研究热点. 其中,密钥管理是无线传感器网络中消息认证、加密解密等各种安全技术的基础. 目前研究者已经设计了多种密钥管理方案. 在基本的随机密钥预分布模型[3]中,先产生一个比较大的密钥池,每个节点拥有密钥池中的一部分密钥,任意两个节点将以一定概率共享至少一个公共密钥. 文献[4]对基本随机预分布模型进行扩展,提出 q-composite 模型以及随机密钥对模型[4]. 另外研究者提出了几种基于阈值的方案[5-6],这些方案在被俘获节点的数量低于阈值前不会泄露其他的链路. 而使用对等节点作为信任中间节点的 PIKE 方案[7]增强了对节点俘获攻击的抵抗能力. 还有一些基于分簇、利用簇头节点进行安全通信的方案[8-9],这些方案共同的缺点是簇头节点被俘给网络带来的致命威胁.

另外,若干种利用传感器网络部署位置信息来改进性能的方案[10-14]被提出. 这些方案根据部署信息可以获知哪些节点被部署在相同区域,从而减少节点需要存储的密钥数量. 其中文献[10-13]中的方案假定预先知道传感器节点部署后的期望位置,文献[14]中的方案不需要知道节点预期部署位置.

最近,文献[15]提出了一种基于层次网络的密钥预分布方案 PKH. PKH 方案将传感器网络划分为若干个区域,每个区域内有若干个高级节点以及大量普通节点. 普通节点存放少量的密钥,高级节点存放大量密钥,而密钥发现过程和随机密钥预分布模型[3]相同,只要两个节点的密钥环存在相同密钥即可建立共享密钥.PKH 中高级节点还充当网关节点,即使两个属于不同区域的节点互为邻居也需要通过高级节点才能通信,这会增大网络的延迟. 由于高级节点存储了大量的密钥,因此即使极少量的高级节点被俘获也会泄漏网络中大量的链路信息.

PKH 中的问题是由于高级节点存放大量密钥,并且作为网关节点运行在网络中引起的. 为了解决这些问题,本文提出一种新的通信半径可调的无线传感器网络密钥管理方案 KMVTR. 基本思想是弱化高级节点在密钥管理中的作用,仅利用高级节点通信距离远的特点达到安全连通,或者不使用高级节点,直接使用通信半径可调的普通节点达到网络的安全连通,以减少高级节点被俘给网络带来的威胁. 主要贡献如下:

1) KMVTR 利用节点通信半径可动态调整的特点来改进安全性能,被俘获的任何节点都不会泄漏除与其直接相连的链路外的任何链路的信息,不存在高级节点被俘带来的严重威胁;

2) 理论及实验分析表明,KMVTR 在没有高级节点的情况下,使用通信半径可调的普通节点替代高级节点,仍然可以保证高安全连通概率;

3) KMVTR 支持灵活的部署方式,不需知道每个分组的预期部署位置.

1 使用高级节点的 KMVTR

1.1 基于分组的部署模型

本节介绍本文中使用的部署模型,在部署网络之前,先将所有的传感器节点分成 k 个分组,每一个分组由 n 个节点组成. 分组完成后将所有的传感器节点按照分组进行部署,通常属于一个分组的所有节点会在同一时间同一地点被部署. 例如,使用直升飞机在到达预定地点上空后投放同一分组的所有节点.

通常可以预期,属于同一个分组的节点,由于同属于一个分组的节点通常在同一时间同一地点被部署,它们在地理位置上会相互更靠近. 因此下面假设一个分组的传感器节点组成的网络在物理上连通是合理的. 本文同时假定同一分组内的节点最后的实际位置满足相同的概率分布函数,并且在部署之后节点位置不会发生变化. 实际上,传感器节点最后位置受到很多因素的影响,通常认为传感器节点最后的位置满足均匀分布或者二维高斯分布.

1.2 KMVTR 密钥预分布

本文的基于分组的密钥预分布方案分为 3 个阶段:密钥预分布阶段、共享密钥发现阶段、路径密钥建立阶段. 由于路径密钥建立阶段和其他方案的相同,下面仅介绍前两个阶段的过程. 以下称具有更远通信半径、更多能量的高级节点为 A 类节点,普通节点为 B 类节点. 在共享密钥发现阶段中,A 类节点会扩大自己的通信范围,可以和相邻分组的 A 类节点直接进行通信.

1.2.1 密钥预分布阶段

根据上述的传感器网络部署模型,整个传感器网络的通信可以分为两类:分组内通信和分组间通信. 同一分组内的节点通过分组内密钥预分布即可建立共享密钥;属于不同分组的节点间则需要通过 A 类节点来协助建立共享密钥对,A 类节点在分组

间密钥预分布阶段已经存储了一些分组间通信需要的密钥信息.

分组内密钥预分布为同一分组内的节点通信建立共享密钥对. 首先,为每一个分组随机产生至少 n 个惟一的节点 ID,并为每对节点 ID 分配一个密钥. 可以多产生一些节点 ID,将来再加入新节点时使用. 然后,分组内的每个节点在产生的节点 ID 中选择其中一个作为自己的 ID,并把该节点 ID 关联的所有密钥一起存储到节点中. 这样,分组内的任意一对节点都有一个共享的密钥. 最后,如果存储在节点内的节点 ID 为 A 类节点的 ID,则标记该节点 ID 为 A 类节点 ID,否则为 B 类节点 ID.

在分组内建立共享的密钥对之后还需要进行分组间密钥预分布. 传感器网络中有 k 个分组,每个分组内有 g 个 A 类节点,整个网络中有 kg 个 A 类节点. 把这 kg 个 A 类节点视做一个新的分组,然后用分组内密钥预分布相同的方法为这个新的 A 类节点分组进行密钥预分布. 最后,每个 A 类节点都存储剩余 $(k-1)g$ 个 A 类节点的 ID 以及共享密钥.

1.2.2 共享密钥发现阶段

在密钥预分布阶段结束后,传感器网络的各个分组将会被部署到实际监测区域,每个分组内都有若干个 A 类节点和 B 类节点,B 类节点比 A 类节点要多很多. 在密钥发现阶段 A 类节点将使用大通信半径,使得分属于两个相邻分组的 A 类节点可以直接通信,如图 1 中的两个 A 类节点 g_1, n_1,使所属的两个相邻分组连通.

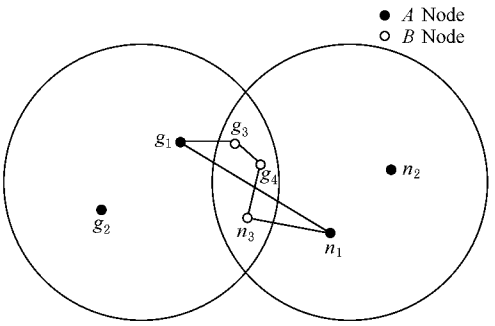


Fig. 1 Nodes $g_1, g_2, g_3, g_4, n_1, n_2, n_3$ in two groups.

图 1 节点 $g_1, g_2, g_3, g_4, n_1, n_2, n_3$ 分别属于两个分组

对于同一个分组的任意一对节点,在密钥预分布阶段已经为它们建立共享密钥. 本文假定在分组内密钥建立完毕后,分组内路由[16]也随后建立完毕.

下面将对分组间建立共享密钥的过程进行说明.对每个节点用分组标记来标示所属的分组,具体分组间密钥建立过程描述如下:

1) 每个节点明文广播所属的分组标记 i、节点 ID、节点类型给自己所有的一跳邻居. 如 A 类节点 g_1 进行广播,分组内节点就知道可以通过 g_1 协助建立分组间密钥.

2) 如果在第 1 步中两个节点发现它们属于不同分组且互为邻居节点,则节点 ID 大的节点将选择分组内的一个 A 类节点,将邻居节点 ID 以及其所属的分组标记发送给该 A 类节点. 如图 1 中,节点 g_4 和 n_3 互为邻居节点,且属于不同分组,其中 g_4 节点 ID 比较大,因此会将 n_3 节点 ID 以及分组标记通过分组内路由加密发送给 A 类节点 g_1.

3) A 类节点收到步骤 2 中节点的请求之后,与对应相邻分组中的一个 A 类节点进行协商得到临时密钥,并发送给这两个相邻节点,然后两个 A 类节点删除该临时密钥. 如图 1 中,A 类节点 g_1 和 n_1 将临时密钥发送给 B 类节点 g_4 和 n_3,由此两个 B 类节点建立共享密钥.

4) 如果 A 类节点已经为一个相邻分组协助建立共享密钥 s 次,则广播已经和这个相邻分组中节点建立共享密钥的 s 个 B 类节点 ID 以及相邻分组标记. 分组中 A 类节点随后删除和这个相邻分组中 A 类节点的所有共享密钥.

5) 收到步骤 4 中 A 类节点广播的 B 类节点,如果需要和对应相邻分组的 B 类节点建立共享密钥,则通过已经建立的 s 条到相邻分组的安全路径可以建立和邻居节点的共享密钥.

6) 如果 A 类节点部署后经过时间 T,没有发现相邻分组的 A 类邻居节点,或者距离上次协助请求过去时间 T 后,则可以删除所有预分布的分组间 A 类节点密钥,并把通信半径调到和 B 类节点相同. 如图 1 中的 A 类节点 $n2$ 将删除预分布的 A 类节点间的密钥,将自己变成一个普通的 B 类节点.

在第 4 步中的广播信息,可以使用已有的任意一种广播加密方法进行安全广播,如 μTESLA 等协议. 另外,把 A 类节点与一个相邻分组建立共享密钥的次数限制在 s 内,是为了 A 类节点在足够短的时间内删除不同分组 A 类节点间的共享密钥,以防止攻击者记录从部署网络开始的网内所有通信并通过俘获 A 类节点来攻击分组间通信.

只有在上述过程中 A 类节点使用扩大的通信半径进行通信,之后所有行为和 B 类节点都相同. 在共享密钥发现阶段结束后整个网络的各个分组已经相互连通,若有新的节点加入或者节点的位置

发生变化,则可以进入路径密钥建立阶段来建立共享密钥.

2 性能分析

在无线传感器网络中,密钥管理方案的性能主要从安全连通性、抗节点俘获、支持的网络规模以及通信存储负载方面进行分析.

2.1 安全连通性分析

如果一条路径上各跳间都有密钥进行保护则称这条路径是安全的.如果网络中的任意一个节点可以通过多跳方式和网络中的任意其他节点建立一条安全路径,则称这个网络是安全连通的.同一个分组内的任意一对节点都已被预分布一个共享密钥,因此,在假设分组内网络是物理连通的情况下,分组内的网络安全连通概率为 1.对于任何相邻的分组,由于可以通过具有大通信半径的 A 类节点建立共享密钥,因此也是相互安全连通的.所以,本文使用高级节点的 KMVTR 方案在部署的网络物理连通的情况下网络安全连通的概率为 1.

2.2 抗节点俘获分析

节点俘获对安全构成极大的威胁.通常以在攻击者俘获若干节点后,除和被俘获节点直接相连的链路外,网络中泄漏的其他链路数量来衡量抗节点俘获能力.对于 B 类节点,因为每个密钥对都是惟一的,任何 B 类节点的被俘都不向攻击者透露除了其本身参与的直接通信以外的任何信息.而对于 A 类节点,由于在协助 B 类节点建立密钥后会立即删除该临时密钥,因此 A 类节点的被俘同样不会透露出其本身参与的直接通信以外的任何信息.

在上面介绍的各种密钥预分布方案中,只有文献[11-12]中的方案以及随机密钥对模型[4]能提供和 KMVTR 相同的抗节点俘获的能力.但文献[11-12]中的方法假设在密钥预分布阶段就知道节点期望的具体部署位置.这个假设严重限制了这两种方法的应用范围,因为通常很难,甚至不可能保证获得节点的期望的部署位置.而本文的方法在密钥预分布阶段不需要知道每个节点期望的部署位置.

随机密钥对模型[4]中由于每个节点存储了大量用不到的密钥,受限于节点的存储容量,所能支持的网络规模十分有限.Eschenauer 和 Gligor 给出规模为 N 的网络为达到 c 以上的安全连通概率,任意两个相邻节点能建立安全链路的概率 p 存在以下关系[3]:

$$p = \frac{N-1}{N} \times (\ln N - \ln(-\ln(c))) \times \frac{1}{n'}, \tag{1}$$

其中,n'为一个节点的平均邻居节点数量,N 为网络中节点总数.N 比较大时$\frac{N-1}{N}$近似为 1,要求网络安全连通概率 $c = 0.9999$ 时,式(1)可以简化如下:

$$p = \frac{\ln N + 9.21}{n'}. \tag{2}$$

所以每个节点需要存储的密钥数量 m 和网络规模 N 存在以下关系:

$$m = N \times p = \frac{N \times (\ln N + 9.21)}{n'}. \tag{3}$$

在 KMVTR 中,对于一个由 N 个节点组成的网络,若将网络分为$\sqrt{N}$ 个分组,每个分组有$\sqrt{N}$ 个节点,其中有 g 个 A 类节点,则节点最多需要存储密钥数量 m 和网络规模 N 存在以下关系:

$$m = \sqrt{N} - 1 + (\sqrt{N} - 1) \times g. \tag{4}$$

比较式(3)和式(4),N 足够大时,随机密钥对模型每个节点需要的存储空间比 KMVTR 方案要多.当平均邻居节点数量 $n' = 30$,$N \geqslant 2$ 时,$p \leqslant 0.33$,每个节点至少需要存储 $0.33N$ 个密钥.如图 2 所示,这时随机密钥对模型和 KMVTR 相比,能支撑的最大网络规模要小.和文献[15]中 PKH 相比,本文在抗节点俘获性能上更加优秀.由于 PKH 无论是采用平衡或者不平衡的密钥分布模型,每个密钥都有多个拷贝存储在多个节点中,因此部分节点的被俘将泄漏除和被俘获节点直接相连的部分链路.在图 3 中,PKH 设置一个区域内部署 35 个普通节点、5 个高级节点,在普通节点中分别存放 83,30,10 个密钥,高级节点存储足够的密钥使得网络连通性达到 0.99999.如果区域内有 10 个普通节点被俘获,攻击者利用被俘获普通节点中存储的密钥,获

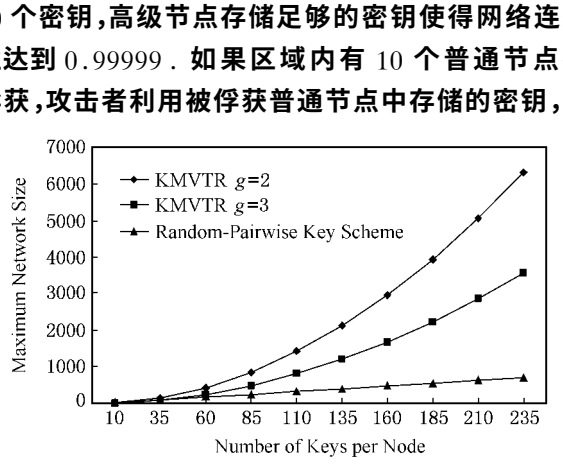


Fig. 2 Maximum network size.

图 2 KMVTR 和随机密钥对方案支撑的网络规模比较

取区域内除被俘普通节点直接参与的链路信息的概率分别有 0.999,0.6,0.096. PKH 方案中高级节点被俘会导致严重后果. 当普通节点存放 30 个密钥、高级节点存放 750 个密钥时,如果一个高级节点被俘,则除被俘高级节点直接参与的链路之外的链路被泄露的概率达到 0.902. 而本文 KMVTR 中,任何节点的被俘都不向攻击者透露除了其本身参与的直接通信以外的任何信息.

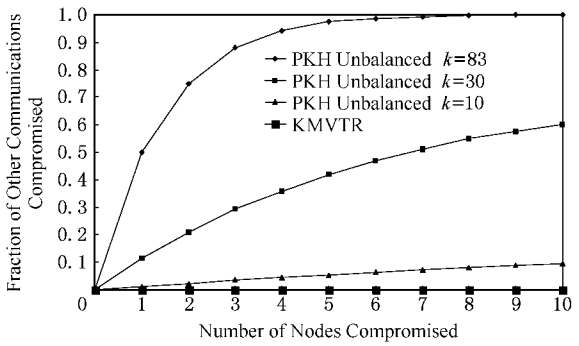


Fig. 3 Resistance against node capture.

图 3 本文方案 KMVTR 和 PKH 方案抗节点俘获能力的比较

2.3 通信负载分析

由于每次节点发送消息所消耗的能量和发送的距离的四次方成正比,因此,密钥建立阶段通信负载主要考虑 A 类节点大范围通信次数. 在分组间密钥建立步骤 1,A 类节点需要广播自己的 ID 以及分组标记,步骤 3 中的协商建立以及分配密钥需要两个分组的 A 类节点各发送两次数据,步骤 4 需要分组内协助建立密钥的 A 类节点广播一次数据,步骤 2,5,6 均不需要发送数据. 假设一个分组最多有 8 个邻居分组,则最多发生 $16s$ 次步骤 3,因此一个分组中 A 类节点大范围通信次数最多为 $16s+2g$,g 为分组内 A 类节点的个数.

文献[15]的 PKH 方案中引入了高级节点作为探测区域中的网关节点,除了密钥建立阶段需要高级节点进行通信,不同区域间的节点进行通信都需要通过高级节点转发. 因此,高级节点进行大范围通信的次数要远远高于本文 KMVTR 中的 A 类节点.

3 不使用高级节点的 KMVTR

从上面分析中可以看出,A 类节点进行大范围发送的次数很少,实际上密钥建立阶段消耗的能量并不多. 传感器网络中的普通节点的通信半径通常为 10m~100m[17-18],并且其通信半径可以进行调节. 因此考虑使用普通节点充当 A 类节点.

由于普通节点通信半径即使在最大情况下,也不能和高级节点一样保证两个分组的 A 类节点能相互直接通信,而这直接影响两个分组的安全连通概率. 为此,通过增加一个分组内的 A 类节点数量来保证两个相邻分组有较高的概率安全连通.

如图 4 所示,考察两个相邻分组,每个分组有 200 个节点,其中有 g 个 A 类节点. 同一分组的节点部署在半径为 R 的圆形区域内,相邻分组部署位置距离为 $\sqrt{3}R$. 则两个分组安全连通的概率 P 等于至少存在一对分属于两个分组的 A 类节点物理上可以通信的概率. 图 4 中阴影区域 S 是一个直径为 R 的圆,当 A 类节点最大通信半径等于部署区域半径 R 时,至少存在一对分属于两个分组的 A 类节点落在圆 S 内的概率 P' 是 P 的下界. 经计算得到 $P'=(1-0.845^g)^2$,所以 $P\geqslant(1-0.845^g)^2$. 当 $g=20$ 时,$P\geqslant 0.93$,即两个相邻分组在 A 类节点占节点总数 10% 且 A 类节点的最大通信半径为 R 时,安全连通的概率至少在 0.93 以上.

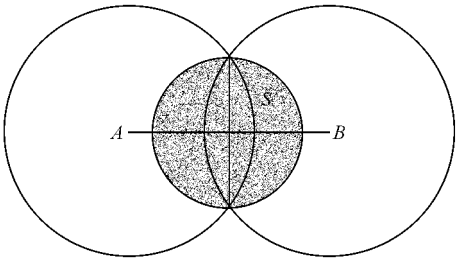


Fig. 4 Two adjacent groups.

图 4 两个相邻分组

下面通过模拟实验进一步研究 A 类节点数量和通信半径对相邻分组连通概率的影响. 在实验中,每个分组有 200 个节点随机分布在半径为 R 的区域内,两个相邻分组部署位置距离为 $\sqrt{3}R$. 分别考察当 A 类节点占节点总数的 5%,10%,15% 时,两个相邻分组连通概率随 A 类节点扩大后的通信半径变化的规律. 对 3 种情况进行 100 万次的随机分布,统计两个相邻分组的安全连通次数,即有一对属于不同分组的 A 类节点可以直接通信的次数. 实验结果如图 5 所示.

实验结果验证了上面的理论分析,即分组中包含适量的 A 类节点即可保证相邻分组较高的安全连通概率. 为了使相邻分组连通概率达到 0.99,当 A 类节点比例为 5% 时,A 类节点最大通信半径需要达到 $1.3R$;比例为 10% 时,最大通信半径达到 $0.9R$;比例为 15% 时最大通信半径达到 $0.7R$.

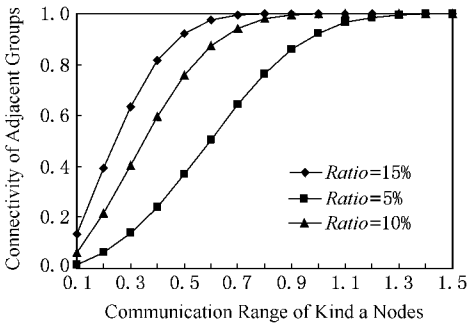


Fig. 5 Connectivity of adjacent groups.

图 5 分组间连通概率分析

如果分组部署区域半径为 100m,普通节点通信半径为 35m,在 A 类节点占分组内节点 10% 的情况下,按实验结果,A 类节点需要在密钥建立阶段使用至少 90m 的通信半径才能使得两个相邻分组连通概率达到 0.99. 对剩下 0.01 有可能存在的不连通的情况,可以通过 A 类节点两跳扩展即可达到 0.99996 的安全连通概率.

由于每次节点发送消息所消耗的能量和发送的距离的四次方成正比,因此一次大半径通信相当于 81 次小范围通信. 在 $s=5$, $g=20$ 情况下,平均每个 A 类节点进行 5 次大范围通信,消耗的能量相当于进行 405 次 B 类节点间的通信. 这样 A 类节点进行大范围通信消耗的能量,对可以进行上万次短距离通信的节点来说是完全可以接受的.

因此,普通节点在分组部署区域半径小于 100m 时完全可以充当 A 类节点,降低网络成本. 而付出的代价是需要部署更多的 A 类节点,以使网络能达到可以接受的安全连通概率. 总之,本文 KMVTR 方案即使是在没有高级节点的情况下也能使用.

4 结 论

本文给出了一种新的基于分组的密钥预分布方案 KMVTR,该方案利用了传感器节点通信范围动态调整的特点来改进网络的安全性能,提供最佳的抗节点俘获的能力,具有良好的网络扩展性,并且不需要预先知道节点部署后的期望位置. 理论分析及实验结果均表明本文的方法具有很高的安全性能.

在节点具有比较强移动性的网络中,本文的方法将不再适用,因为节点的移动将会破坏已经建立的安全连通,而重新建立共享密钥将会带来比较大的延迟. 因此,接下来的工作需要研究如何改进方案使得在移动性强的网络中依然适用.

致谢 感谢几位匿名审稿专家对本文提出的修改意见!

参 考 文 献

[1] Li Jianzhong, Li Jinbao, Shi Shengfei. Concepts, issues and advance of sensor networks and data management of sensor networks [J]. Journal of Software, 2003, 14(10): 1717-1727 (in Chinese)
(李建中, 李金宝, 石胜飞. 传感器网络及其数据管理的概念、问题与进展[J]. 软件学报, 2003, 14(10): 1717-1727)

[2] Cui Li, Ju Hailing, Miao Yong, *et al*. Overview of wireless sensor networks [J]. Journal of Computer Research and Development, 2005, 42(1): 163-174 (in Chinese)
(崔莉, 鞠海玲, 苗勇, 等. 无线传感器网络研究进展[J]. 计算机研究与发展, 2005, 42(1): 163-174)

[3] L Eschenauer, V Gligor. A key management scheme for distributed sensor networks [C]. ACM Conf on Computer and Communications Security (CCS). New York: ACM Press, 2002

[4] H Chan, A Perrig, D Song. Random key pre-distribution schemes for sensor networks [C]. The IEEE Symp on Security and Privacy (S&P). Piscataway: IEEE Communication Societ, 2003

[5] W Du, J Deng, Y S Han, *et al*. A pair-wise key pre-distribution scheme for wireless sensor networks [C]. The 10th ACM Conf on Computer and Communications Security (CCS '03). New York: ACM Press, 2003

[6] D Liu, P Ning. Establishing pair-wise keys in distributed sensor networks [C]. The 10th ACM Conf on Computer and Communications Security (CCS '03). New York: ACM Press, 2003

[7] H Chan, A Perrig. PIKE: Peer intermediaries for key establishment in sensor networks [C]. In: Proc of IEEE INFOCOM 2005. Piscataway: IEEE Communication Society, 2005

[8] Chanjun Yang, Jianming Zhou, Wensheng Zhang, *et al*. Pairwise key establishment for large-scale sensor networks: From identifier-based to location-based (invited paper) [C]. The 5st Int'l Conf on Scalable Information Systems. New York: ACM Press, 2006

[9] T A Zia, A Y Zomaya. A secure triple-key management scheme for wireless sensor networks [C]. IEEE INFOCOM 2006 Students Workshop. Piscataway: IEEE Communication Societ, 2006

[10] W Du, J Deng, Y S Han, *et al*. A key management scheme for wireless sensor networks using deployment knowledge [C]. IEEE INFOCOM 2004. Piscataway: IEEE Communication Society, 2004

[11] D Huang, M Mehta, D Medhi, *et al*. Location-aware key management scheme for wireless sensor networks [C]. The 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04). New York: ACM Press, 2004

[12] D Liu, P Ning. Location-based pair-wise key establishments for static sensor networks [C]. 2003 ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN '03). New York: ACM Press 2003

[13] Z Yu, Y Guan. A key pre-distribution scheme using deployment knowledge for wireless sensor networks [C]. ACM/IEEE Int'l Conf on Information Processing in Sensor Networks (IPSN). New York: ACM Press, 2005

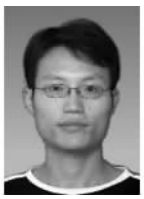
[14] Donggang Liu, Peng Ning, Wenliang Du. Group-based key pre-distribution in wireless sensor networks [C]. The 4th ACM Workshop on Wireless Security, Cologne, Germany, 2005

[15] P Traynor, H Choi, G Cao, *et al*. Establishing pair-wise keys in heterogeneous sensor networks [C]. In: Proc of IEEE INFOCOM 2006. Piscataway; IEEE Communication Society, 2006

[16] Yang Wenguo, Guo Tiande, Zhao Tong. Routing algorithms of the wireless sensor network based on dynamic programming [J]. Journal of Computer Research and Development, 2007, 44(5): 890-897 (in Chinese)
(杨文国,郭田德,赵彤. 基于动态规划的无线传感器网络的路由算法[J]. 计算机研究与发展, 2007, 44(5): 890-897)

[17] I F Akyildiz, W Su, Y Sankarasubramaniam, *et al*. A survey on sensor networks [J]. IEEE Communications Magazine, 2002, 40(8): 102-114

[18] V Raghunathan, *et al*. Energy-aware wireless microsensor networks [J]. IEEE Signal Procsessing Magazine, 2002, 19(2): 40-50



Chen Haikun, born in 1983. Master. His main research interests include security in sensor networks.
陈海坤,1983 年生,硕士,主要研究方向为无线传感器网络中的安全问题.

Shi Shengfei, born in 1972. Ph. D. and associate professor. His current research interests include data management in wireless sensor networks.
石胜飞,1972 年生,博士,副教授,主要研究方向为无线网络中的数据管理.

Li Jianzhong, born in 1950. Professor and Ph. D. supervisor. Senior member of China Computer Federation. His main research interests include wireless sensor network, parallel database technology, *etc*.
李建中,1950 年生,教授,博士生导师,中国计算机学会高级会员,主要研究方向为传感器网络、并行数据库技术等(lijzh@hit.edu.cn).

Research Background

Security is one of the essential problems in wireless sensor networks, and key management is a basic technology to assure the security in wireless sensor networks. In this paper we propose a new key management scheme KMVTR based on variable transmission range of sensor nodes. This scheme can be used in wireless sensor networks with some powerful sensor nodes, and can also be applied in sensor networks without powerful nodes which have wide transmission range. KMVTR has several advantages such as providing perfect resilience against node capture, and supporting larger network size. If the sensor nodes have high mobility, KMVTR will be useless. So the future work of this paper includes making KMVTR available in wireless sensor networks which have high mobility. The work of this paper is supported by several foundations such as the National Natural Science Foundation of China, and the National Grand Fundamental Research 973 Program of China.