无线传感网固定簇结构的密钥管理机制*

刘 宁

(柳州职业技术学院,广西 柳州 545006)

摘 要：由于传感器节点的资源严格受限,现有的网络安全机制无法应用于无线传感网中。提出了固定簇区域的网络结构,以大型脱机密钥池方式随机分配密钥形成密钥环,并周密地设计了密钥更新方案。仿真实验证明,该机制在能量消耗和安全性方面具有优秀的性能。

关键词：无线传感网;簇;密钥管理;安全性

中图分类号：TP393 **文献标识码**：A **文章编号**：1674-7720(2011)01-0041-03

The key management mechanism of wireless sensor network based on fixed-cluster structure

Liu Ning

(Liuzhou Vocational & Technical College, Liuzhou 545006, China)

Abstract: As sensor nodes are strictly limited resources, existing network security mechanisms can not be applied to wireless sensor networks. This paper proposes a fixed cluster area network structure to form key ring by randomly assigned key in a large key pool offline mode, and careful designs the key update program. The simulation experiments show excellent performance of the mechanism in energy consumption and safety area.

Key words: WSN; cluster; key management; security

微传感器技术、微电子技术、无线通信技术以及计算机技术的进步,极大地推动了集信息采集、处理、无线传输等功能于一体的无线传感器网络 WSN(Wireless Sensor Networks)的发展。WSN 以其低成本、低功耗的特点,在军事、环境监测、医疗健康等领域有着广泛的应用,并逐渐深入到人类生活的各个领域。

当 WSN 部署在一个敌对的环境中,安全性就显得极为重要,因为它们容易产生不同类型的恶意攻击。例如,敌人可以冒充合法节点窃取网络中的通信数据,或者发送错误的信息给其他节点。为了确保从网络中收集到的数据正确可靠,节点间的数据通信必须采取安全机制。而 WSN 区别于其他传统的无线网络,具有非常有限的资源,如有限的能量、带宽以及处理和存储数据的能力,这就要求面向 WSN 的安全机制必须轻量简单,易于在微型传感器上实现。

近几年,WSN 的安全问题受到了许多研究者的关注。参考文献[1]提出一种低通信开销的点对点认证协议,该协议的安全性完全依赖于基站,如果基站被攻陷,网络将毫无安全性可言。参考文献[2]提出点到多点认证方案,解决了共享密钥问题,但是无法抵御 DoS 攻击。参考文献[3]提出一种随机密钥分配方案,但该方案无法保证网络的连通性。参考文献[4]提出一种使通信双方具有 q 个公共密钥的 q-composite 模型,增强了网络的连通性,但方案增加了通信开销。参考文献[5]认为任何一种单一的密钥机制都不可能实现 WSN 所需的安全通信,因此提出多密钥机制——LEAP 协议,其优点是任何节点的受损都不会影响其他节点的安全,缺点是节点部署后,在一个特定的时间内必须保留全网通用的组密钥,若组密钥一旦被暴露,则整个网络的安全都受到威胁。

本文在 LEAP 的多密钥机制基础上,对网络区域进行簇的划分,以减少数据传输产生的能量消耗,并设计密钥更新算法,进一步增强网络的安全性。

1 基于固定簇结构的密钥管理方案

1.1 固定簇结构

在本方案中,网络区域被基站划分为若干大小相

* 基金项目:广西教育厅科研基金项目(编号:200708LX260)

等、固定不变的的网格，每个网格形成一个簇，每个簇有一个轮换选出的簇头节点，如图 1 所示。节点在网络中的位置是已知的，节点形成簇是基于它们的位置。簇区域的划分是在簇头选举的第一轮进行，在整个网络生命周期内不再变动。从第二轮开始，不再需要基站的任何控制信息，极大地减少了在初始化阶段与基站的通信量。

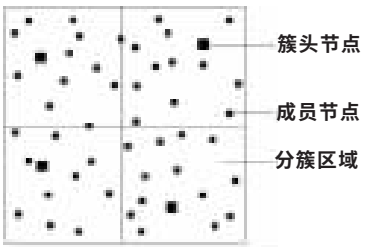

图 1 网络结构

采用网格的形式划分并固定簇区域的方法，可以使簇头节点均匀分布在网络中，以得到较优化的簇结构。同时，由于簇区域已经固定，在每一轮的初始化阶段(除了第一轮)要完成的工作只是簇头节点的选择，减少了形成簇所需要的一系列广播带来的能耗。

当簇形成以后，簇头节点确定 TDMA 时隙表并通告每个簇内成员。当簇头的电池能量降低到一个预定的值 E_{hmin} 时，或作为簇头节点服务了一段预定的时间后，它将在簇内广播一条新的选举信息，选出一个新的簇头节点。

1.2 网络密钥类型

本方案支持四种类型的密钥：个体密钥、对密钥、簇密钥和组密钥。下面将讨论每一种类型的密钥。

(1)个体密钥：每个成员节点都有一个唯一的与基站共享的密钥，用于成员节点与基站之间的安全通信。例如，一个成员节点如果发现邻居节点的异常行为，可以发送警报给基站；基站也可以使用该密钥加密信息发送给成员节点。

(2)对密钥：每个节点与其直接邻居节点共享一个对密钥。对密钥用于需要加密或进行数据源认证的安全通信。例如，一个节点可以使用它的对密钥保护其与邻居节点的簇密钥，或保证其读数能传输到一个聚合节点。但是对密钥不能在消极参与中使用。

(3) 簇密钥：簇头节点与其成员节点共享一个簇密钥，以确保本地广播信息(如路由控制信息、节点间传送的消息)的安全性。研究人员已经发现，在网络处理技术中，数据融合和消极参与对节省 WSN 的能量消耗是非常重要的。例如，当一个节点侦听到邻居节点转发的数据与当前自己读取的数据相同时，则可以选择不发送。在响应最大值聚合操作时，如果一个节点读取的数据小于侦听到的数据，即可废止自己的数据。为了使消息安全可行，邻居节点应该能够解密并验证信息的级别，如传感器读取的数据和邻居转发的数据。这意味着这些信息应该被加密或通过本地共享密钥验证身份。因此，在本方案中每个簇都拥有一个唯一的簇密钥，用于簇内信息的加密，其直接邻居节点使用相同密钥解密或验证该信息。

(4) 组密钥：用于对整个网络中的广播消息进行加密，如基站发布任务或查询。由于组密钥在网络所有节点中共享，如果一个节点被攻陷，应即时更新组密钥，因此需要一个有效的密钥更新机制。

1.3 随机密钥分配方案

随机密钥分配方案主要分为 4 个阶段：

(1)密钥重新分配阶段。由中央密钥服务器生成一个大型脱机密钥池，其密钥分配步骤如下：

①分配一个唯一的节点标识符或密钥环标识符给每个传感器节点。

②从密钥池中选择 m 个不同的密钥给传感器节点，形成一个钥匙环。

③将密钥环装入传感器节点的内存。

(2)传感器部署阶段。传感器是随机挑选并统一大面积分布的。通常，一个成员节点的邻居节点数目 n 远小于网络节点的总数 N。

(3)密钥发现阶段。在该阶段，每个传感器节点广播明文密钥标识符或使用私有共享密钥发现机制发现与邻居节点共享的密钥。通过比较拥有的密钥，一个传感器节点可以建立与之共享密钥的节点名单，然后广播此名单。通过从邻居收到的名单，一个传感器节点就可以构建一个基于邻居之间共享密钥关系的密钥图。

(4)对密钥建立阶段。如果一个传感器节点与给定的邻居共享密钥，此共享密钥被视为它们的对密钥。如果一个传感器节点不与给定的邻居共享密钥，即可在密钥发现阶段利用密钥图查找密钥路径，从而建立对密钥。该方案有两个特点，第一，预装在一个节点中的密钥也可以安装在其他节点中，即一个密钥可以由一对以上的节点共享。第二，在当前大部分方案中，预装密钥与节点 ID 之间没有任何关系。

1.4 密钥更新方案

如果一些节点使用同一密钥进行了 20 k/3 次加密运算(k 是密钥的位数)，则进行密钥更新。

(1)定期簇密钥更新：簇头节点使用簇密钥进行了 20 k/3 次加密运算后，由其产生新的随机簇密钥，新密钥用旧密钥加密，附加数字签名，并向簇中所有成员发送。

(2)定期组密钥更新：当基站使用相同的密钥进行了 20 k/3 次加密运算后，由基站产生新的随机组密钥，新密钥用旧密钥加密，附加数字签名并在网络中广播。

(3)成员加入簇密钥更新：新成员加入簇，簇头将产生新密钥，新密钥用旧密钥加密并发送给所有簇成员，新簇密钥用对密钥加密并发送给新成员，随后，簇头请求基站执行成员加入组密钥更新。

(4)成员加入组密钥更新：基站验证来自簇头的密钥

更新请求后，将执行组密钥更新。该过程与定期组密钥更新算法相同，但是新成员不知道当前的组密钥，所以新成员的簇头将向其专门发送新组密钥和基站的公钥，并保持向后保密特性。

(5)成员离开簇密钥更新：当一个簇成员的电池能量耗尽或不再满足簇的功能时将离开簇，簇头将进行密钥的更新。新的簇密钥用旧密钥加密，由簇头发送给所有成员并在成员中共享，然后，簇头请求基站发起成员离开组密钥更新。

(6)成员离开组密钥更新：该过程与定期组密钥更新算法相同。

2 性能分析

2.1 能耗分析

使用 NS2 仿真工具将本方案与其他协议（如 LEAP）进行比较。建立仿真模型如下：网络由 150 个节点组成，每个节点的初始能量为 0.25 J，随机分布在 80 m×80 m 的范围内，基站距离最近的节点约 100 m，模拟时间 4 000 s。从图 2 的仿真结果中可以看出，由于本方案采用固定簇结构，有效地节省了节点的能耗。

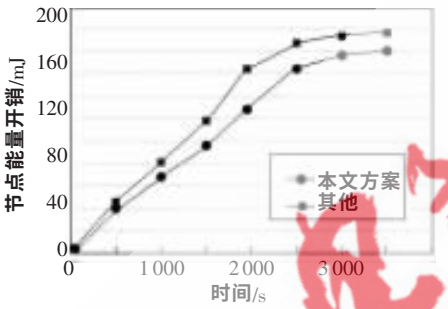

图 2 网络能耗比较

2.2 安全性分析

为了确保网络的安全性，方案采取定期更新密钥的方法。然而，如果密钥的更新不能发生在攻击者利用密钥之前，那么一个被攻陷的成员节点可能在下一轮选举中担当簇头，产生新密钥，用现有的簇密钥加密新密钥进行分发。本方案靠数字签名验证更新的密钥来抵御这种攻击，同时也抵御了所有的欺骗攻击和数据完整性攻击。

在与能耗仿真一样的仿真模型下，并在网络正常运行期间随机选择一些被捕获的节点，分别在不同的被捕获节点数目下，运行仿真程序（执行 50 次），将本方案与其他协议（如 LEAP）进行对比，结果如图 3 所示。结果显示，由于本方案采取全面的密钥更新机制，具有更好的安全性能。

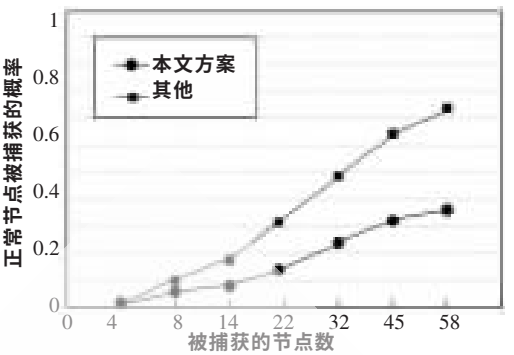

图 3 网络安全性比较

本文介绍了一个固定簇结构的密钥管理机制，仿真实验证明，该方案对于无线传感网减少能量消耗和保护簇的安全性方面效果显著。今后，将通过全面的仿真进一步测试该方案的各方面性能，特别是在阻止节点合谋攻击方面的性能。

参考文献

[1] PERRIG A, SZEWCZYK R, WEN V, et al. SPINS: security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534.

[2] PERRIG A, CANETTI R, SONG D, et al. Efficient and secure source authentication for multicast streams over lossy channels[C]. Proceedings of IEEE on SP00, 2000: 56.

[3] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks [C]. Proceedings of ACM on CCS'02, NOV, 2002: 41-47.

[4] CHAN H, PERRIG A, SONG D. Random key pre-distribution schemes for sensor networks [C]. Proceedings of IEEE on SP03, May 2003: 197-213.

[5] ZHU S, SETIA S, JAJODIA S. LEAP: efficient security mechanisms for large-scale distributed sensor networks [C]. Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003: 62-72.

（收稿日期：2010-08-02）

作者简介：

刘宁，男，1971 年生，在读硕士，讲师，主要研究方向：无线传感器网络技术与信息安全。