Scientific Research

Study on the Key Management Technology for Wireless Sensor Networks

GONG Wenchao, LI Xiaomin

Naval University of Engineering, Electronic Engineering Institute, Wuhan, China

Abstract: The Wireless Sensor Network is widely applied in many realms. The security problem of the WSN has become to be one of the most important research directions. The characteristics as well as potential security problems of the WSN are briefly introduced in this paper. Based on the classification of the key management models, eight kinds of important key management schemes are carefully discussed. These schemes represent the trends of the key management technology and they have a vital application prospect.

Keywords: wireless sensor network; key management; key distribution

WSN 密钥管理技术研究

龚文超，李小珉

海军工程大学 电子工程学院，武汉，中国，430033

摘　要：随着 WSN 应用在许多行业的纵深发展，WSN 的安全问题已经成为一个重要研究方向。简要介绍了 WSN 特点以及存在的安全隐患。在对 WSN 密钥管理模型分类的基础上，详细阐述了几种重要的密钥管理方案，它们代表了 WSN 密钥管理技术的发展方向，具有重要的应用前景。

关键词：无线传感器网络；密钥管理；密钥分配

1 引言

无线传感器网络（Wireless Sensor Network，WSN）是由大量密集分布在检测区域内的微型自主传感器节点，通过无线自组织的通信方式构成的专用无线网络。随着 WSN 应用在许多行业的纵深发展，人们对 WSN 特性的要求也越来越高。安全问题表现得尤为突出，比如在军事、金融、医疗等方面的应用，敏感信息的泄露将会给个人、集体、国家带来无法挽回的损失。因此，近年来，WSN 安全问题的研究已经成为 WSN 研究的一个重点问题。

2 WSN 网络特点与安全隐患

与其它无线网络相比，甚至是与传统无线自组织网络相比，它有很多自身独有的特性，具体体现在以下几个方面[1]：

- 传感器节点在资源上比其它网络节点更受限制，体积小、成本低。
- 传感器节点数量巨大，是传统网络的很多倍，节点分布密度非常大，并且故障率高。
- 网络带宽更窄，数据传输数率很低。
- 传感器节点一般依赖电池供电，并处于无人值守的区域，大多数情况下缺乏维护，能量得不到持续供应。
- 传感器节点无线通信消耗的能量远远高于执行指令消耗的能量。
- 由于节点故障、休眠、被破坏或者无线信道的不稳定等原因，WSN 的网络拓扑经常处于动态的变化之中。

WSN 节点的资源限制以及网络本身的特点，给 WSN 带来了更加严重的安全隐患，主要有下述几点：

（1）与传统网络相比，攻击者更容易捕获传感器节点，破获密钥信息，进而插入恶意节点破坏网络正常获取信息的能力。

（2）传感器节点资源非常受限，这使得传统的性能优良的安全机制难以照搬到传感器网络中。

（3）由于通信距离有限，节点数目巨大，传感器网络采用无线多跳的通信方式，这有利于节约能量，但是却为窃听、干扰等攻击行为提供了温床。、WSN 严重的安全隐患使得 WSN 安全问题的研究涉及很多方面[2]，比如加密算法、攻击与防御策略、密钥管理、

978-1-935068-04-4

安全架构、安全路由、安全定位、安全数据融合、入侵检测等，但是以提供安全、有效的保密通信为目标的密钥管理技术是目前 WSN 安全研究最重要、最基本的问题，同时它也是其它安全机制的基础。

3 WSN 密钥管理模型分类

近年来，WSN 密钥管理方案的研究取得了长足的进步。密钥管理方案的种类繁多，分类方式各异。这里主要从网络结构和节点之间通讯模型两个方面对密钥管理模型进行分类。

3.1 根据网络结构分类

WSN 结构可以分为分布式网络结构和分层次网络结构两类。针对不同的网络结构，密钥管理的方案也有所不同[3]。

3.1.1 基于分布式的密钥管理模型

分布式网络中没有固定的基础设施，网络节点的能量和功能相同，部署网络时将节点随机投掷在目标区域自组织形成网络。针对这种网络结构，目前提出了三类密钥管理模型。

- 预置全局密钥管理模型
- 预置所有对密钥管理模型
- 随机预分配密钥管理模型

3.1.2 基于分簇的密钥管理模型

在分簇式 WSN 中根据各个节点的功能和能量不同可以将节点分成三类：基站、簇头和普通的传感器节点。针对分簇式网络结构，目前提出了如下三类密钥管理模型。

- 基于 KDC（密钥分发中心）的对密钥管理模型
- 低能耗密钥管理模型
- 轻量级密钥管理模型

3.2 根据节点通讯模型

在 WSN 中，还可以根据通讯节点的多少，将密钥管理模型分为以下两种[4]：

- 对密钥管理机制：对密钥管理机制是用于节点与节点之间安全通信。
- 组密钥管理机制：组密钥管理机制是用于网络内一组节点协同工作。

4 重要密钥管理方案

在上述密钥模型的基础上，已经研究出了很多种密钥管理方法，其中代表了未来研究趋势的有如下几种重要管理方案。

4.1 随机密钥预分配方案

Eschenauer 和 Gligort 提出了随机密钥预分配方案[5]，基本思想是：节点部署之前，每个节点从一个大型密钥池随机选择若干密钥作为自己的密钥环，密钥发现阶段，节点广播自己的密钥环发现与自己有共同密钥的邻居节点，然后建立安全通信。

这个方案灵活、应用简单，它是很多密钥管理方案的基础，在密钥管理领域有着不可替代的作用。但是在网络安全性和连通性之间很难找到契合点。虽然初始密钥池越大，网络安全性越好，但是两个节点之间找到共享密钥的概率会越小，连通性会越小，甚至出现安全孤岛。反之，网络安全性将会受到很大威胁。在网络规模较大时，该方案的缺点更加明显。

4.2 部署信息改进的密钥管理方案

Du，Deng，Han 以及 Varshney 等人第一次尝试利用部署信息来改进密钥管理方案[6]，其基本思想是：将部署节点和部署区域进行等量的分组，然后按照一定的顺序，将节点以组的形式分布在相应的部署区域，并利用非一致性概率密度函数模仿每个区域中节点的分布情况。通过调节相邻区域的距离。使得在每个特定区域中找到某个节点的概率相等。在这些假设的前提下，可以在节点部署之前获得节点之间的部署信息。然后利用这些部署信息，以不同的概率分配节点之间的共享密钥，相邻组之间有更多的共享密钥，距离较远的组之间有很少的共享密钥或没有共享密钥。

通过利用部署信息，可以减少密钥数量，提高了网络抗毁性，降低了网络的通信量。全面提高了网络图形的连通性。但是，就目前技术水平来讲，节点部署知识的获得方法还需进一步研究。

4.3 EBS 动态密钥管理方案 SHELL

Younis，Ghumman 以及 Eltoweissy 在分簇式 WSN 中提出了位置识别的 EBS 动态密钥管理方案 SHELL[7]。在 SHELL 中，普通节点按照其地理位置被划分为若干簇，由簇头或网关节点来控制。网关节点有可能被命令节点指定为其它簇的密钥生成网关节点。根据簇数和节点的存储容量。簇 C_i 的网关节点矩阵 $G_{CH}[i]$ 使用正则矩阵法生产所在簇的（n,k,m）——EBS 矩阵，并把矩阵的相关部分内容分别发送给该簇的密钥生产网关节点 $G_{K1}[i]$ 和 $G_{K2}[i]$ 等。密钥生成网关节点根据 EBS 矩阵的内容生成相应的管理密钥，并通过 $G_{CH}[i]$ 广播给簇内给节点。为了避免串谋攻击，相邻节点管理密钥的汉明距设计为最小。

SHELL 支持密钥更新，支持受损节点撤除。不过如果有新节点加入时，系统执行初始化程序。

这个方案利用 EBS 较好的实现了密钥的产生、分配及密钥的更新，有效的保护了当前、前向与后向秘密；网络的可扩展性较好，可以支持大规模的网络及其动态变化，单个节点捕获对网络的安全通信影响不大。缺点是当节点频繁的被捕获时，频繁的密钥更新大大增加了网络的通信负载，消耗了网络能量。同时它也没有很好的解决删除簇头后簇内节点的分配问题。

4.4 路由驱动的密钥管理方案

X. Du, M. Guizani, Y. Xiao 等人针对 HSN（HSN），提出了一种路由驱动的密钥管理方案[8]。HSN 模型由少量的高端节点和大量的低端节点组成，高端节点在能量、存储能力、通信能力等方面都远远优于低端节点。节点部署之后，HSN 形成分簇式的拓扑结构。将网络划分为许多个不同的簇，高端节点充当簇头的角色，低端节点选择最近的高端节点作为它的簇头。高端节点可以与邻居高端节点直接通信，所有的高端节点形成网络的通信骨干网络。簇内低端节点通过建立树状路由，将数据包顺着树传递给簇头节点。低端节点采用多跳通信的方式将数据传递给高端节点，高端节点通过多跳通信的方式将数据传递给汇聚节点。网络利用这种多对一的通信模式，提出了一种新的密钥管理设想，每个低端节点不需要与所有的邻居节点建立共享密钥，而只需要与它们的父亲节点和孩子节点建立共享密钥。这大大的降低了密钥建立的通信开销和计算开销，从而降低了网络的能量消耗。

由于方案所需的共享密钥很少，计算复杂度不高，因此这个方案采用了轻量级的公约加密算法——椭圆曲线加密算法（ECC）。使得加密过程更加灵活、简单，不需要提前预分配密钥对，不需要建立复杂的单向密钥链。与传统的密钥预分配方案相比，这种方案大大节约了网络的存储开销和通信开销。方案中，每个低端传感器节点加载了独有的私钥，密钥建立阶段之后，每一对低端通信节点具备不同的共享密钥。某个节点的捕获不会影响网络中其它节点之间的安全通信。这个方案适用于安全级别要求高的场合，但是公钥加密算法的复杂性依然有待检验，由于部署时间较长，它一般不适用于要求快速部署的场合。

4.5 概率性不均衡密钥管理方案

Traynor P., Kumar R., Choi H 等针对异构网络，提出概率性不均衡密钥管理方案[9]。网络由两种不同传感器节点组成。普通感知节点（L1）能力非常有限，执行数据采集的任务。高端节点（L2）具有更多的内存、更强的处理能力以及额外的无线发射装置。这类节点配备了附加密钥，它们在网络中起着路由和网关节点的作用。

在随机密钥管理的基础上，不是给每个节点分配相同的密钥个数，而是根据节点资源的多少分配不同数目的密钥，其中 L2 节点分得的密钥远远多于 L1 节点。节点部署之后，通过密钥查找发现邻居节点之间的共享密钥，建立安全通信。如果邻居节点没有共享密钥，就通过一个多跳的安全链路为双方建立会话密钥。

通过在异构网络中建立不均衡的密钥分配机制，大大减轻了 L1 节点的负担，提高了网络的生存时间。同时，为了适应传感器网络大规模发展的趋势，它自行设计了一套叫做 LIGER 的互补式密钥分配协议，支持网络在不同工作模式之间进行转换。通过利用预先分布的密钥，工作在独立模式的节点可以相互安全有效的建立密钥。由于支持基于 KDC 的工作模式，方案支持节点认证。这使得网络的安全水平有了很大的提高。

4.6 可扩展性协议

在随机密钥预分配方案的基础上，Kausar F., Hussain S., Yang L.T., Masood A 针对 HSN 密钥管理，提出了一种可扩展性协议[10]。这个协议对传感器节点的存储、计算、和通信等资源限制特别敏感。同其它的异构网络一样，在网络中定义了两种不同类型的传感器节点：高端节点和低端节点。网络形成分簇的拓扑形式，高端节点是簇头节点，低端节点是簇内成员节点，采集周围环境的数据并传送给高端节点。高端节点各方面资源都优于低端节点，它们配备了防篡改硬件，可以直接与基站进行通信。为了方便网络扩展与维修，高端节点和低端节点可以随时加入网络。方案通过少量生产密钥来代替大型密钥池。主要是利用特定的生产密钥和一个公开的种值，以及密钥 hash 函数生成密钥链；密钥链的集合就构成了密钥池。因为每个低端节点只存储了少量的生产密钥，这大大降低了方案的存储要求。方案还加入了一个密钥更新机制，用于定期的更新所有的密钥，这使得方案的安全性能比较好，与基本的密钥预分配方案相比，大大提高了抗节点捕获能力。

4.7 基于地理位置的密钥管理方案

F. Anjum 提出了一种基于地理位置的密钥管理方案[11]。这种方案不依赖网络的部署信息，只需要在网络中引进少量的特殊节点——锚节点，同时假设在节点刚部署的很短时间中，敌人不能捕获传感器节点。

978-1-935068-04-4 © 2009 SciRes.

锚节点能够以不同的功率水平给周围的传感器节点发送 beacon 数据包。方案的执行过程分为预分配过程、初始化过程、通信过程三个阶段。

在预分配阶段，每个传感器节点从一个基数为 P 的大型密钥池中随机选择 R 个密钥作为自己的原始密钥环（R《P）。每个传感器节点还内嵌了相同的 HASH 算法。然后为所有的传感器节点和锚节点加载一个相同的密钥 K。初始化阶段，锚节点以不同的功率水平发送不同的 beacon。beacon 中包含经过加密认证的随机数字和公同密钥 K。传感器节点收到数据包后，利用密钥 K 解密数据包，获得 beacon 中的随机数字，这样传感器利用自己的原始密钥环、随机数序列，通过 HASH 函数，获得自己的衍生密钥环，并清除原始密钥环。其中，衍生密钥环与传感器节点周围锚节点的多少，以及传感器节点与锚节点的距离密切相关。最后共享密钥查找，建立邻居节点之间的安全通路，进行通信。

由于敌人不能获得原始密钥环，在敌人访问了所有的 beacon 数据包的情况下，敌人不能计算出不同区域节点的衍生密钥，说明该方案的抗毁性强，节点毁坏具有局部特征。利用地理位置信息，在具有少量密钥的条件下，方案同样具有很好的连通性，降低了网络的内存需求。不足之处就是扩展性不好。新节点的加入会导致系统不停的进行初始化过程，使得网络能耗大，降低了网络的生存时间。

4.8 基于部署信息的密钥管理方案

Zhen Yu 和 Yong Guan 提出了基于部署信息的密钥管理方案[12]。该方案将目标区域平均划分为六边形网格。按照网格的多少，将传感器节点平均的分组。然后以分组部署模型，将传感器节点以组的形式对应的部署在相应的网格之中。这意味着每一个传感器节点的大部分邻居节点来自组内或邻居组。因此，为了获得很高的连通概率，关键就是要使得组内节点和邻居组的节点之间的共享密钥概率最大化。这个方案分为两个阶段：密钥预分配阶段和共享密钥查找阶段。

密钥预分配阶段，系统会产生一个全局公共矩阵 G，还有一些私有矩阵 A 和 B。所有的分组共享矩阵 G，意味着每个组内的每个传感器节点可以从 G 中获得一个相应的列。每个组独享一个矩阵 A，这说明组内的每个节点可在 A 中获得一个相应的行。这样保证了来自同一个组的两个节点一定可以找到一对共享密钥。然后我们还有给每组分配一些 B 矩阵，并且保证每一对邻居组至少共享一个相同的矩阵 B。这样组内的每个节点可以从相应的 B 中获得行信息。密钥查找阶段，邻居节点会互换自己的组标号、B 矩阵标号和 G 矩阵的列。如果节点来自同一组，它们利用矩阵 A 和 G 获得共享密钥。如果来自不同的组，他们利用某个共同的 B 矩阵和矩阵 G 获得共享密钥。然后，具有共享密钥的节点之间会建立安全通信链路，然后进行通信。

这个方案可以获得很高的抗毁性能，很低的存储要求。同时，可以利用较短距离的通信获得理想的连通性，降低了网络能耗。在网络规模大型化的发展中，有很强的实际意义。

5 结论

随着 WSN 安全要求的日益提高，密钥管理方案的研究在未来依然会是一个热门。WSN 应用的广泛性必将导致 WSN 结构的异构性，因此，将来应将更多的精力放在异构网络密钥管理上。同时，相关信息的利用，如部署信息、位置信息等，会大大的改善网络性能。所以，应该根据实际情况，挖掘一些可利用的条件，为 WSN 的实际应用提供更优越的平台。

References (参考资料)

[1] 李敏，殷建平，伍勇安等。无线传感器网络密钥管理方案综述。计算机工程与科学，2008，30（12）.
[2] 马建庆。无线传感器网络安全的关键技术研究[D].复旦大学，2007.
[3] 孙利民，李建中。无线传感器网络[M]。北京：清华大学出版社，2005：1，5-6，203.
[4] 李晖。无线传感器网络安全技术研究[D].上海交通大学，2007.
[5] Eschenauer L , Gligor V D, “A key management scheme for distributed sensor networks”, in Proceedings of the 9th ACM Conference on Computer and Communication Security, p.p.41-47, 2002.
[6] Du W, Deng J, Han Y S, et al, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,” in the Proceedings of IEEE INFOCOM 2004.
[7] 苏忠，林闯，封富军等。无线传感器网络密钥管理的方案和协议。软件学报，2007，18（5）：1218-1231.
[8] Du X, Guizani M, Xiao Y, et al, “A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor networks,” in the Proceedings of IEEE International Conference.
[9] On Communication 2007(ICC'07): pp.3407-3412 : June 2007.
[10] Traynor P, Kumar R, Choi H, et al, “Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks”, in IEEE Tansactions on mobile computing 6(6), pp. 663-77, June 2007.
[11] Kausar F, Hussain S, Yang L T, et al, "Scalable and efficient key management for heterogeneous sensor networks" , in Journal of Supercomputing (2008) 45: pp.44-65.
[12] Anjum F, “Location Dependent Key Management Using Random Key-predistribution In Sensor Networks,” In proceedings of WiSe'06.
[13] Yu Z, Guan Y, “A Key Management Scheme Using Deployment Knowledge for Wireless Sensor Networks”,IEEE Transactions On Parallel And Distributed Systems, 19(10): Oct.2008.