ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.5, May 2007, pp.1218−1231
DOI: 10.1360/jos181218
© 2007 by *Journal of Software*. All rights reserved.

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无线传感器网络密钥管理的方案和协议*

苏 忠+, 林 闯, 封富君, 任丰原

(清华大学 计算机科学与技术系,北京 100084)

Key Management Schemes and Protocols for Wireless Sensor Networks

SU Zhong+, LIN Chuang, FENG Fu-Jun, REN Feng-Yuan

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

+ Corresponding author: Phn: +86-10-62772487, E-mail: zsu@csnet1.cs.tsinghua.edu.cn, http://www.tsingha.edu.cn

Su Z, Lin C, Feng FJ, Ren FY. Key management schemes and protocols for wireless sensor networks. *Journal of Software*, 2007,18(5):1218−1231. http://www.jos.org.cn/1000-9825/18/1218.htm

Abstract: 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 field of secure wireless sensor networks. The key management in wireless sensor networks meets many new challenges due to its intrinsic properties. In this paper, the secure and performance evaluation criterion of key management is introduced, the taxonomy for the key management schemes and protocols is proposed, the classic key management schemes and protocols are discussed and compared in detailed, and finally the open research problems and the possible solution are also pointed out. Recent related work indicates that future work will focus on some key issues such as fully distributed, self-organized, fault-tolerance and intrusion-tolerance, and location-aware etc.
Key words: wireless sensor network; security; key management; key pre-distribution; pair-wise key

摘 要: 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无线传感器网络安全最为重要、最为基本的研究领域.无线传感器网络固有的特性使得密钥管理研究面临许多新挑战.介绍了密钥管理的安全评价和性能评价指标体系;还介绍了密钥管理的方案和协议的分类方法;着重综述和比较了典型的密钥管理方案和协议;最后指出了存在的开放问题及解决思路.目前的研究进展表明,全分布式、自组织性、容错容侵性、与地理信息相结合等研究问题将是下一步的重点研究方向.
关键词: 无线传感器网络;安全;密钥管理;密钥预分配;配对密钥
中图法分类号: TP393 文献标识码: A

无线传感器网络(wireless sensor networks,简称 WSN)集微机电技术、传感器技术、通信技术于一体,可广泛应用于教育、军事、医疗、交通等诸多领域,拥有巨大的应用潜力和商业价值[1,2],引起了国内外广泛的关注和研究[3−6].安全是 WSN 最基本的一项服务,特别是 WSN 被部署在无人触及或容易受损或被俘获的环境时,保

* Supported by the National Natural Science Foundation of China under Grant Nos.90412012, 60673187, 60429202, 60573122, 60672118 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2006AA01Z218, 2006AA01Z225 (国家高技术研究发展计划(863))

Received 2006-11-09; Accepted 2006-12-15

© 中国科学院软件研究所 http://www.jos.org.cn

证 WSN 的安全性更是应该优先考虑的问题[7,8].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,有效的密钥管理机制也是其他安全机制,如安全路由[9]、安全定位[10]、安全数据融合[11]及针对特定攻击的解决方案[12]等的基础.

在传统网络中,密钥管理的研究与应用中已取得许多成果[13−18].但因为 WSN 所固有的特点,使得这些研究成果一般不能直接应用于 WSN.具体表现在:(1) WSN 节点资源(包括存储容量、计算能力、通信带宽和距离等)受到更加严格的限制.例如,UCB(University of California Berkeley)研制的 MICA2 mote[19],使用 8 位 7.3828MHz ATmega 128L 处理器,SRAM 为 4KB,ROM 为 128KB,通信频率为 916MHz,带宽为 10Kbps.资源的严格受限使得传统的对节点计算、存储和通信开销较大的密钥管理方案或协议[13−15]无法应用于 WSN.(2) 一般而言,WSN 没有固定的基础设施支持.因此,基于在线的密钥分配中心(key distribution center,简称 KDC)的密钥管理方案或协议[16]无法应用于 WSN.(3) 节点容易受损.WSN 节点一般被设计为无特殊物理保护的,容易受到物理损坏或被俘获,网络中的部分节点处于非正常运行状态是一个普遍现象,一些状态敏感的密钥管理方案或协议[17,18]就无法应用于 WSN.

目前,WSN 的研究缺乏普适性的统一体系结构指导,密钥管理研究处于起步和发展阶段,存在着一些开放的问题.本文阐述了 WSN 密钥管理研究的性能评价标准,在详细综述和比较典型的 WSN 密钥管理方案和协议的基础上,指出了需要解决的研究问题以及未来的研究方向.

1 无线传感器网络密钥管理的安全和性能评价

与典型网络一样,WSN 密钥管理必须满足可用性(availability)、完整性(integrity)、机密性(confidentiality)、认证(authentication)和认可(non-reputation)等传统的安全需求[20,21].此外,根据 WSN 自身的特点,WSN 密钥管理还应满足如下一些性能评价指标:

(1) 可扩展性(scalability).WSN 的节点规模少则十几个或几十个,多则成千上万.随着规模的扩大,密钥协商所需的计算、存储和通信开销都会随之增大,密钥管理方案和协议必须能够适应不同规模的 WSN.

(2) 有效性(efficiency).网络节点的存储、处理和通信能力非常受限的情况必须充分考虑.具体而言,应考虑以下几个方面:存储复杂度(storage complexity),用于保存通信密钥的存储空间使用情况;计算复杂度(computation complexity),为生成通信密钥而必须进行的计算量情况;通信复杂度(communication complexity),在通信密钥生成过程中需要传送的信息量情况.

(3) 密钥连接性(key connectivity).节点之间直接建立通信密钥的概率.保持足够高的密钥连接概率是 WSN 发挥其应有功能的必要条件.需要强调的是,WSN 节点几乎不可能与距离较远的其他节点直接通信,因此并不需要保证某一节点与其他所有的节点保持安全连接,仅需确保相邻节点之间保持较高的密钥连接.

(4) 抗毁性(resilience).抵御节点受损的能力.也就是说,存储在节点的或在链路交换的信息未给其他链路暴露任何安全方面的信息.抗毁性可表示为当部分节点受损后,未受损节点的密钥被暴露的概率.抗毁性越好,意味着链路受损就越低.

2 无线传感器网络密钥管理方案和协议的分类

近年来,WSN 密钥管理的研究已经取得许多进展[22].不同的方案和协议,其侧重点也有所不同.下面我们依据这些方案和协议的特点进行适当的分类.

2.1 对称密钥管理与非对称密钥管理

根据所使用的密码体制,WSN 密钥管理可分为对称密钥管理和非对称密钥管理两类.在对称密钥管理方面,通信双方使用相同的密钥和加密算法对数据进行加密、解密,对称密钥管理具有密钥长度不长,计算、通信和存储开销相对较小等特点,比较适用于 WSN,目前是 WSN 密钥管理的主流研究方向.在非对称密钥管理方面,节点拥有不同的加密和解密密钥,一般都使用在计算意义上安全的加密算法.非对称密钥管理由于对节点的计

© 中国科学院软件研究所 http://www.jos.org.cn

算、存储、通信等能力要求比较高,曾一度被认为不适用于 WSN,但一些研究[23,24]表明,非对称加密算法经过优化后能适用于 WSN.从安全的角度来看,非对称密码体制的安全强度在计算意义上要远远高于对称密码体制.

2.2 分布式密钥管理和层次式密钥管理

根据网络的结构,WSN 密钥管理可分为分布式密钥管理和层次式密钥管理两类.在分布式密钥管理[25−33]中,节点具有相同的通信能力和计算能力.节点密钥的协商、更新通过使用节点预分配的密钥和相互协作来完成.而在层次 WSN 密钥管理[34−37]里,节点被划分为若干簇,每一簇有一个能力较强的簇头(cluster head).普通节点的密钥分配、协商、更新等都是通过簇头来完成的.

分布式密钥管理的特点是密钥协商通过相邻节点的相互协作来实现,具有较好的分布特性.层次式密钥管理的特点是对普通节点的计算、存储能力要求低,但簇头的受损将导致严重的安全威胁.

2.3 静态密钥管理与动态密钥管理

根据节点在部署之后密钥是否更新,WSN 密钥管理可分为静态密钥管理和动态密钥管理两类[38].在静态密钥管理[25−33]中,节点在部署前预分配一定数量的密钥,部署后通过协商生成通信密钥,通信密钥在整个网络运行期内不考虑密钥更新和撤回;而在动态密钥管理[36,37]中,密钥的分配、协商、撤回操作周期性进行.

静态密钥管理的特点是通信密钥无须频繁更新,不会导致更多的计算和通信开销,但不排除受损节点继续参与网络操作.若存在受损节点,则对网络具有安全威胁.动态密钥管理的特点是可以使节点通信密钥处于动态更新状态,攻击者很难通过俘获节点来获取实时的密钥信息,但密钥的动态分配、协商、更新和撤回操作将导致较大的通信和计算开销.

2.4 随机密钥管理与确定密钥管理

根据节点的密钥分配方法区分,WSN 密钥管理可分为随机密钥管理与确定密钥管理.在随机密钥管理中,节点的密钥环通过随机方式获取,比如从一个大密钥池里随机选取一部分密钥[25],或从多个密钥空间里随机选取若干个[27].而在确定性密钥管理中,密钥环是以确定的方式获取的,比如,使用地理信息[28],或使用对称 BIBD (balanced incomplete block design)[33]、对称多项式[39]等.从连通概率的角度来看,随机密钥管理的密钥连通概率介于 0,1 之间,而确定密钥管理的连通概率总为 1.

随机性密钥管理的优点是密钥分配简便,节点的部署方式不受限制;其缺点是,密钥的分配具有盲目性,节点可能存储一些无用的密钥而浪费存储空间.确定性密钥管理的优点是密钥的分配具有较强的针对性,节点的存储空间利用得较好,任意两个节点可以直接建立通信密钥;其缺点是,特殊的部署方式会降低灵活性[28],或密钥协商的计算和通信开销较大[33,39].

3 典型的无线传感器网络密钥管理的方案和协议

3.1 Eschenauer随机密钥预分配方案[25]

Eschenauer 和 Gligor 在 WSN 中最先提出随机密钥预分配方案(简称 E-G 方案).该方案由 3 个阶段组成.第 1 阶段为密钥预分配阶段.部署前,部署服务器首先生成一个密钥总数为 P 的大密钥池及密钥标识,每一节点从密钥池里随机选取 $k(k<<P)$个不同密钥,这种随机预分配方式使得任意两个节点能够以一定的概率存在着共享密钥.第 2 阶段为共享密钥发现阶段.随机部署后,两个相邻节点若存在共享密钥,就随机选取其中的一个作为双方的配对密钥(pair-wise key);否则,进入到第 3 阶段.第 3 阶段为密钥路径建立阶段,节点通过与其他存在共享密钥的邻居节点经过若干跳后建立双方的一条密钥路径.

根据经典的随机图理论[40],节点的度 d 与网络节点总数 n 存在以下关系: $d=\frac{n-1}{n}(\ln n-\ln(-\ln P_c))$,其中,P_c 为全网连通概率.若节点的期望邻居节点数为 $n'(n'<<n)$,则两个相邻节点共享一个密钥的概率 $p'=\frac{d}{n'-1}$.在给

© 中国科学院软件研究所 http://www.jos.org.cn

定 p'的情况下,P 和 k 之间的关系可以表示如下: $p'=1-\frac{((P-k)!)^2}{(P-2k)!P!}$.

E-G 方案在以下 3 个方面满足和符合 WSN 的特点:一是节点仅存储少量密钥就可以使网络获得较高的安全连通概率,例如,要保证节点数为 10 000 的 WSN 几乎保持全连通,每个节点仅需从密钥总数为 100 000 的密钥池随机选取 250 个密钥即可满足要求;二是密钥预分配时不需要节点的任何先验信息(如节点的位置信息、连通关系等);三是部署后节点间的密钥协商无须 Sink 的参与,使得密钥管理具有良好的分布特性.

3.2 对E-G方案的几种改进

E-G 方案的密钥随机预分配思想为 WSN 密钥预分配策略提供了一种可行的思路,后续许多方案和协议都在此框架基础上发展.它们分别从共享密钥阈值、密钥池结构、密钥预分配策略、密钥路径建立方法等方面提高随机密钥预分配方案的性能.

3.2.1 q-Composite 随机密钥预分配方案[26]

在 Chan 提出的 q-composite 随机密钥预分配方案(简称 q-composite 方案)中,节点从密钥总数为$|S|$的密钥池里预随机选取 m 个不同的密钥,部署后两个相邻节点至少需要共享 q 个密钥才能直接建立配对密钥.若共享的密钥数为 $t(t\geq q)$,则可使用单向散列函数建立配对密钥 $K=hash(k_1||k_2||\ldots||k_t)$(密钥序列号事先约定).

随着共享密钥阈值的增大,攻击者能够破坏安全链路的难度呈指数增大,但同时对节点的存储空间需求也增大.因此,阈值 q 的选取是该方案需要着重考虑的一个因素.实验表明[26],当网络中的受损节点数量较少时,该方案的抗毁性比 E-G 方案要好,但随着受损节点数量的增多,该方案变得比较差.

3.2.2 多密钥空间随机密钥预分配方案[27]

Blom 单密钥空间方案[41]使得网络中的任意两个节点都能够直接建立配对密钥,并且确保在受损节点数不超过阈值时,网络不会泄露任何机密信息.Du 将其扩展为多密钥空间随机密钥预分配方案[27].网络节点总数为 N,部署前,部署服务器在有限域 $GF(q)$(q 为足够大的素数)上生成一个$(\lambda+1)\times N$的公开矩阵 G(G 满足任意 $\lambda+1$ 列线性不相关)和ω个$(\lambda+1)\times(\lambda+1)$的对称机密矩阵 $D_1,D_2,\ldots,D_\omega$,每一对$(D_i,G)_{i=1,2,\ldots,\omega}$称为一个密钥空间.部署服务器分别计算 $A_i=(D_i\times G)^T$.每一节点随机选取τ个$(2\leq\tau<\omega)$密钥空间,对于被节点 j 选中的矩阵 D_i,j 保存矩阵 A_i 的第 j 行元素,这些行元素信息是机密的,不公开,节点同时也保存矩阵 G 第 j 列相应的种子值(仅保留种子值是出于节约存储空间的考虑).部署后,若任意两个相邻节点共享一个密钥空间,就可以利用矩阵 A_i 的对称性直接建立配对密钥.配对密钥的生成如图 1 所示.

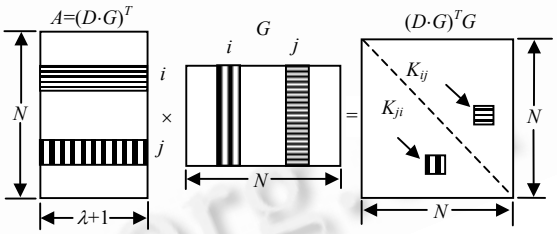


Fig.1 Generating pairwise key[27]

图 1 生成配对密钥[27]

只要选择合适的ω和τ就能够提高密钥空间不被暴露的概率.实验表明[27],要使 10%的安全链路受损,E-G 方案和 q-composite 方案就必须俘获比该方案 5 倍多数量的节点.方案的缺点是计算开销较大.与 Blom 方案相比,该方案虽然降低了密钥连通概率,但却提高了网络密钥连通的抗毁性.

3.2.3 对称多项式随机密钥预分配方案[28]

Blundo 方案[39]使用对称二元多项式的性质($f(x,y)=\sum_{i,j=0}^{t}a_{ij}x^iy^j$ 且$f(x,y)=f(y,x)$)为网络中的任意两个节点建立配对密钥.Liu 在此基础上提出了基于多个对称二元多项式的随机密钥预分配方案[28].部署前,部署服务器在有限域 F_q 上随机生成 s 个 t 阶对称二元多项式$\{f_i(x,y)\}_{i=1,2,\ldots,s}$;然后,每一节点随机选取 s'个多项式共享.部署后,相邻节点若有相同的多项式共享,则直接建立配对密钥.

实验表明[28],当受损节点数较少时,该方案的抗毁性比 E-G 方案和 q-composite 方案要好,但当受损节点超过一定的阈值时(如 60%节点受损),该方案的安全链路受损数量则超过上述两个方案.

© 中国科学院软件研究所 http://www.jos.org.cn

3.2.4 基于地理信息或部署信息的随机密钥预分配方案[29−31]

在一些特殊的应用中,节点的位置信息或部署信息可以预先大概估计并用于密钥管理.Liu 在静态 WSN 里建立了基于地理信息的最靠近配对密钥方案(简称 CPKS(closest pairwise keys scheme)方案)[29].部署前,每个节点随机与最靠近自己期望位置的 c 个节点建立配对密钥.例如,对于节点 u 的邻居节点 v,部署服务器随机生成配对密钥 $k_{u,v}$,然后把$(v,k_{u,v})$和$(u,k_{u,v})$分别分配给 u 和 v.部署后,相邻节点通过交换节点标识符确定双方是否存在配对密钥.

CPKS 方案的优点是,每个节点仅与有限个相邻节点建立配对密钥,网络规模不受限制;配对密钥与位置信息绑定,任何节点的受损不会影响其他节点的安全.缺点是密钥连通概率的提高仅能通过分配更多的配对密钥来实现,受到一定的限制.

针对上述问题,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[29](简称 LBKP (location-based key predistribution)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,并为每一区域指定唯一的二元多项式.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 4 个区域以及节点所在的区域共 5 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 1 个二元多项式共享就可以直接建立配对密钥.该方案通过调整区域的大小来解决 CPKS 方案存在的连通概率受限的问题.与 E-G 方案和 q-composite 方案甚至 Blundo 方案相比,LBKP 方案的抗毁性明显提高,但缺点是计算和通信开销过大.

在基于部署知识的随机密钥预分配方案[30]中,假定网络的部署目标区域是一个二维矩形区域且节点部署服从 Gaussian 分布.节点被划分为 $t\times n$ 个部署组,每个组 $G_{i,j}(i=1,\ldots,t,j=1,\ldots,n)$的部署位置组成一个栅格.密钥池(密钥数为$|S|$)被划分成若干个子密钥池(密钥数为$|S_c|$),每个子密钥池对应于一个部署组.若两个子密钥池是水平或垂直相邻,则至少共享 $a|S_c|$个密钥;若两个子密钥池是对角相邻,则至少共享 $b|S_c|$密钥(a,b 满足以下关系:$0<a,b<0.25$ 且 $4a+4b=1$).若两个子密钥池不相邻,则没有共享密钥.如图 2 所示.

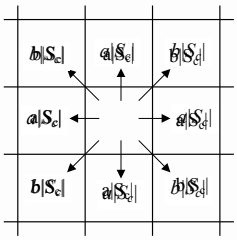


Fig.2 Shared keys between neighboring key pools

图 2 相邻密钥池之间的共享密钥数

对于组内每一节点,从对应的子密钥池随机取 m 个不同的密钥.部署后,若相邻节点存在共享密钥,则可以直接建立配对密钥.

实验表明[30],在同等条件下,该方案提高了节点的连通概率.例如,当节点预分配的密钥数为 100 时,E-G 方案的节点连通概率仅为 0.095,而该方案能够达到 0.687.使用部署知识使得节点减少了预分配无用密钥的数量,提高了网络抗毁性.但该方案的子密钥池的划分需要慎重考虑.

尽管 Liu[29]和 Du[30]都在密钥预分配时使用节点的位置信息以提高抗毁性,但存在着攻击者容易对节点进行定位后俘获以及节点因缺乏认证机制而被伪造等问题.针对上述问题,Huang 的栅格组部署方案[31]使用限制组的节点数量、设定密钥空间被选中的阈值等方法提出了解决方案.

3.2.5 多路径密钥增强方案[26]

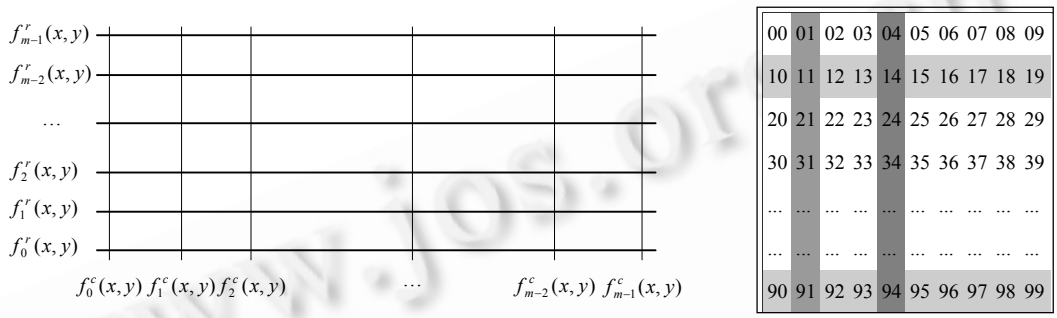
在 E-G 方案里,两个相邻节点 A 和 B 所被分配的密钥有可能被分配给其他节点,若这些节点受损,则 A 和 B 之间的链路会受到安全威胁.Liu 提出了多路径密钥增强方案[26].假设 A 和 B 经过密钥协商后存在着 j 条不相交的路径,A 产生 j 个随机值 $v_1,v_2,\ldots,v_j$,然后通过 j 条不相交的路径发送给 B,B 接收到这 j 个随机值后,生成新的配对密钥 $K=k\oplus v_1\oplus v_2\oplus\ldots\oplus v_j$.攻击者若不能获取全部的 j 个随机值,则不能破译配对密钥 K.该方案若与 E-G 方案或其他随机密钥管理方案结合使用,则能够显著提高相应方案的安全性能.但该方案的缺点是,如何建立和能否建立足够数量的不相交路径在目前尚属于 NP 问题.

3.3 基于栅格的密钥预分配方案[28,32]

在随机密钥预分配方案中,相邻节点只能以一定的概率建立密钥连接,有些密钥管理方案和协议则致力于为任意两个节点建立配对密钥.Liu 和 Chan 基于栅格分别建立了密钥预分配方案.

© 中国科学院软件研究所 http://www.jos.org.cn

建立栅格方法如下:根据网络中的节点总数 N 构造 $m\times m$ 个栅格,其中,$m=\left\lfloor\sqrt{N}\right\rfloor$.在 Liu 提出的方案(简称 GBKP(grid-based key predistribution)方案)[28]里,部署前,部署服务器生成 $2m$ 个多项式,栅格的每一行对应于唯一的一个多项式,每一列对应另一个唯一的多项式.部署服务器把节点逐一对应于各栅格的汇合点,并把对应的多项式共享和标识符配置给该节点,如图 3(a)所示;部署后,同一行或列的节点可以直接建立配对密钥,不同行列的节点通过中间节点建立密钥路径.而在 Chan 提出的 PIKE(peer intermediaries for key establishment)方案[32]里,节点按照栅格的行列号编号,部署前,每一节点都与同一行列共 $2(\sqrt{N}-1)$ 个其他节点建立配对密钥,然后节点按照序列号顺序进行部署,如图 3(b)所示;部署后,同一行或列的节点直接拥有配对密钥,不同行列的节点则通过公共行列的节点建立密钥路径.



(a) GBKP scheme
(a) GBKP 方案

(b) PIKE scheme
(b) PIKE 方案

Fig.3 Grid-Based key predistribution
图 3 基于栅格的密钥预分配

GBKP 方案和 PIKE 方案都保证任意两个节点能够建立配对密钥,与节点密度无关,且能够显著降低节点的通信和存储开销.但其缺点是部署方式固定,不够灵活,中间节点的受损会影响整个网络的安全.

3.4 基于组合论的密钥预分配方案[33]

Camtepe 把组合设计理论(combinatorial design theory)用于设计 WSN 确定密钥预分配方案[33].假设网络的节点总数为 N,用 n 阶有限射影空间(finite projective plane)(n 为满足 $n^2+n+1\geq N$ 的素数)生成一个参数为 $(n^2+n+1,n+1,1)$的对称 BIBD,支持的网络节点数为 n^2+n+1,密钥池的大小为 n^2+n+1,能够生成 n^2+n+1 个大小为 $n+1$ 的密钥环,任意两个密钥环至少存在 1 个公共密钥,并且每一密钥出现在 $n+1$ 个密钥环里.可见,任意两个节点的密钥连通概率为 1.但素数 n 不能支持任意的网络规模.例如,当 $N>n^2+n+1$ 时,n 必须是下一个新的素数,而过大的素数则会导致密钥环急剧增大,突破节点的存储空间而不适用于 WSN.使用广义四边形(generalized quadrangles,简称 GQ)可以更好地支持网络规模,如 $GQ(n,n)$,$GQ(n,n^2)$和 $GQ(n^2,n^3)$分别支持的网络规模达 $O(n^3)$,$O(n^5)$和 $O(n^8)$,但也存在着素数 n 不容易生成的问题.

为此,Camtepe 提出了对称 BIBD 与 GQ 相结合的混合密钥预分配方案:使用对称 BIBD 或 GQ 生成 b 个(b 值大小由 BIBD 或 GQ 决定,$b<N$)密钥环,然后使用对称 BIBD 或 GQ 的补集设计(complementary design)随机生成 $N-b$ 个密钥环,与前面生成的 b 个密钥环一起组成 N 个密钥环.这种混合的密钥预分配方案提高了网络可扩展性和抗毁性,但不保证节点的密钥连通概率为 1.无论是对称 BIBD,GQ 还是混合方案,都有比 E-G 方案更高的密钥连通概率,平均密钥路径长度也更短.

3.5 SPINS(security protocols for sensor networks)协议[34]和LEAP(localized encryption and authentication protocol)协议[35]

Perrig 利用 Sink 作为网络的可信密钥分发中心为网络节点建立配对密钥及实现对广播数据包的认证.SPINS 协议由两部分组成:SNEP(secure network encryption protocol)和 μ TESLA(timed efficient stream

© 中国科学院软件研究所 http://www.jos.org.cn

loss-tolerant authentication).SNEP 主要通过使用计数器(counter)、消息认证码(message authentication code,简称 MAC)等机制来实现数据的机密性及数据认证.通信双方的配对密钥及 MAC 密钥都通过使用从 Sink 获取的主密钥及伪随机函数生成.SNEP 使得协议达到语义级安全(相同的明文在不同的时段加密,其密文不相同),保证了数据的鲜活性;MAC 密钥长度固定,仅为 8 字节,不增加过多的通信负载.

μ TESLA 实现对广播数据的认证.Sink 首先使用单向散列函数 H 生成一个单向密钥链$\{K_0,K_1,...,K_n\}$,其中,$K_i=H(K_{i+1})$,由 K_{i+1} 很容易计算得到 K_i,而由 K_i 则无法计算得到 K_{i+1}.网络运行时间分为若干个时间槽(slot),在每一时间槽使用密钥链里对应的一个密钥.在第 i 个时间槽里,Sink 发送认证数据包,然后延迟一个时间δ后公布密钥 K_i.节点接收到该数据包后首先保存在缓冲区里,并等待接收到最新公布的密钥 K_i,然后使用其目前保存的密钥 K_v,并使用 $K_i=H^{i-v}(K_v)$来验证密钥 K_i 是否合法,若合法,则使用 K_i 认证缓冲区里的数据包.

μTESLA 工作示意图如图 4 所示.

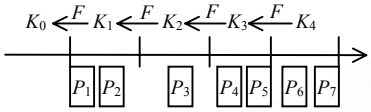


Fig.4 μTESLA one-way key chain[34]

图 4 μTESLA 单向密钥链[34]

在μ TESLA 里,攻击者很难获取或伪造最新的认证密钥.因此,μ TESLA 提供了良好的广播认证机制.但密钥延迟暴露和非实时认证的问题,使其很容易受到 DoS 攻击.针对这些问题,Liu 分别提出了使用多级μTESLA[42]和 Merkle 散列树[43]的解决方法.

在 SPINS 协议里,任何节点的配对密钥生成、数据包认证都必须通过 Sink 来完成.一旦 Sink 受损,则整个网络的安全都受到威胁.而且 Sink 开销过大,SPINS 协议仅适用于规模较小的网络.

Zhu 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 LEAP 协议[35],建立了 4 种类型的密钥:个体密钥、配对密钥、组密钥和簇密钥.个体密钥为节点与 Sink 共享的密钥,由节点在部署前通过预分配的主密钥和伪随机函数来生成.若两个相邻节点要生成配对密钥,则通过交换其标识符及使用预分配的主密钥和单向散列函数计算得到.若节点作为簇头要建立与其邻居节点共享的簇密钥,则产生一个随机密钥作为簇密钥,然后使用与邻居节点的配对密钥逐一地对簇密钥加密后发送给对应节点,邻居节点把簇密钥解密后保存下来.组密钥为 Sink 与所有节点共享的通信密钥.Sink 首先把组密钥使用与其子节点共享的簇密钥加密后广播给子节点,子节点获取最新的组密钥后,用与其下一级子节点共享的簇密钥加密组密钥后广播给其子节点.依此类推,直到所有节点都获取最新的组密钥为止.

LEAP 协议的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主密钥.若主密钥一旦被暴露,则整个网络的安全都受到威胁.

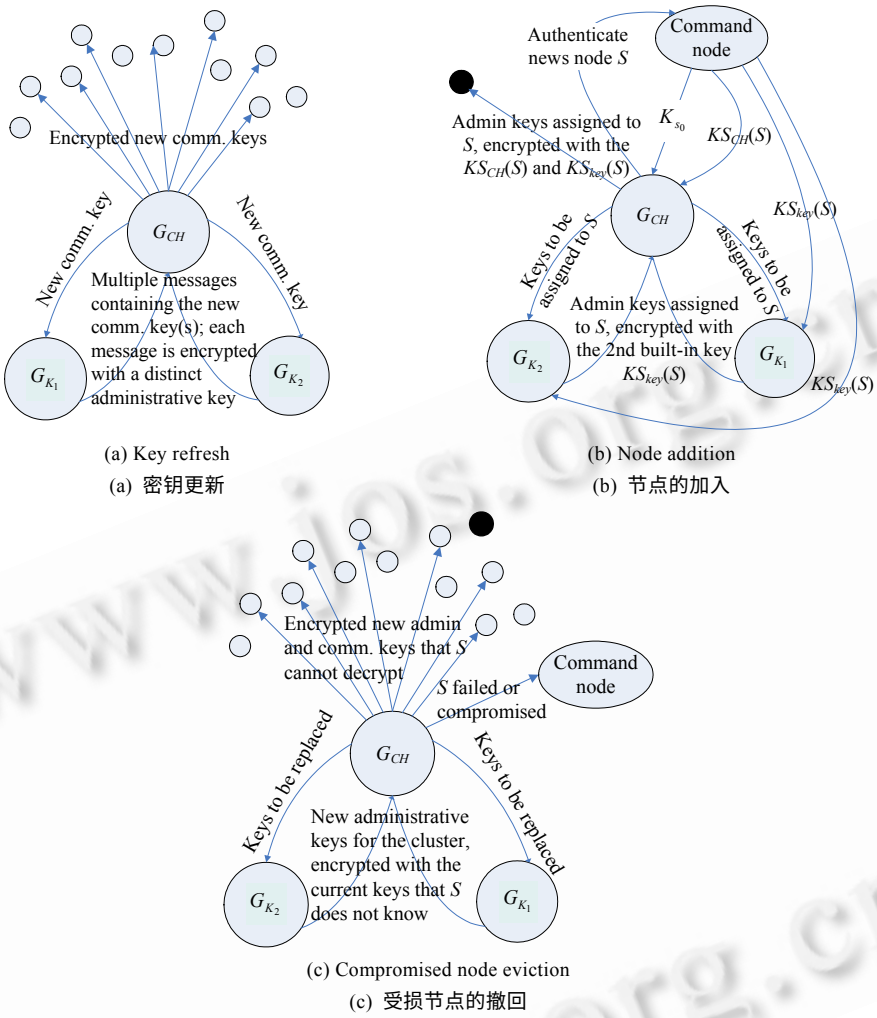
3.6 基于EBS(exclusion basis systems)的动态密钥管理方案[36]

EBS 由 Eltoweissy 提出,主要用于密钥动态管理[44].EBS 为一个三元组(n,k,m)表示的集合Γ,其中,n 为组的用户数,k 为节点存储的密钥数,m 为密钥更新的信息数.对于任一整数(用户)$t\in[1,n]$,具有以下属性:(1) t 最多出现在Γ的 k 个子集(密钥)里,表示任一用户最多拥有 k 个密钥;(2) 有 m 个子集(密钥),$A_1,A_2,\ldots,A_m$,满足 $\bigcup_{i=1}^{m}A_i=[1,n]-\{t\}$,表示使用 m 个与 t 无关的密钥更新信息可撤回用户 t.

Younis 在层次式 WSN 里提出基于位置信息的 EBS 动态密钥管理方案 SHELL(scalable, hierarchical, efficient, location-aware, and light-weight)[36].在 SHELL 方案里,普通节点按照其地理位置被划分为若干簇,由簇头,或称为网关节点(gateway)来控制.网关节点有可能被命令节点指定为其他簇的密钥生成网关节点(key generating gateway).它并不存储和生成自己簇里各节点的管理密钥.根据簇数和节点的存储容量,簇 C_i 的网关节点 $G_{CH}[i]$使用正则矩阵法生成所在簇的(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成网关节点 $G_{K1}[i]$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,并通过网关节点 $G_{CH}[i]$广播给簇内各节点.为了避免串谋攻击,相邻节点管理密钥的汉明距(Hamming distance)设计为最小.

SHELL 定期更新密钥.当需要更新密钥时,由簇头首先把最新的通信密钥发送给密钥网关生成节点,然后由密钥网关生成节点生成新的管理密钥,再通过簇头发送给簇内各节点,如图 5(a)所示.

© 中国科学院软件研究所 http://www.jos.org.cn



(a) Key refresh
(a) 密钥更新

(b) Node addition
(b) 节点的加入

(c) Compromised node eviction
(c) 受损节点的撤回

Fig.5 Key refresh, node addition and compromised node eviction
图 5 密钥更新、节点的加入与受损节点的撤回

当新的节点加入时,首先根据其地理位置确认加入所在簇,并通过命令节点认证其身份,然后由簇头与密钥生成网关节点协调启动管理密钥生成进程,如图 5(b)所示.当要撤回受损的节点时,若是簇头受损,则可以采取指定新的簇头或把簇内节点重新分配到其他正常的簇内等方法;若是普通节点受损,簇头把受损节点信息通知密钥生成网关节点,然后由密钥网关生成节点利用 EBS 的性质生成新的管理密钥,并通过簇头广播发送给簇内节点,受损节点由于无法解密广播数据包而无法获取新的管理密钥,如图 5(c)所示.

与随机密钥分配方案相比,SHELL 明显增强了抗串谋攻击的能力.例如,当 k=4,n=200 时,若要发起串谋攻击,则在 SHELL 里需要使 11 个节点受损,而在随机密钥分配方案时仅需 3 个节点受损.但在 SHELL 里由密钥网关生成节点存储相应簇的节点密钥,这意味着,密钥网关生成节点受损数量越多,网络机密信息暴露的可能性就越大.针对 SHELL 的缺点,Eltoweissy 提出了 LOCK(localized combinatorial keying)方案[37].该方案使用两层 EBS 管理密钥对基站、簇头和普通节点的密钥分配、更新、撤回进行管理,使得簇头的受损不会暴露更多的机密信息.

3.7 对称与非对称混合密钥管理协议

在基于证书密码体制(certificate-based cryptography,简称 CBC)的 PKC(public key cryptography)涉及的一个

© 中国科学院软件研究所 http://www.jos.org.cn

基本问题是公钥的认证,即在使用对方节点的公钥加密时,必须先对公钥进行认证.Huang 提出使用椭圆曲线密码体制(elliptic curve cryptography,简称 ECC)与对称密钥的混合密钥管理协议[45]来解决异构节点之间的公钥认证问题.

在异构 WSN 里,FFD(full-functional devices)被认为具有较强的计算和通信能力,而 RFD(reduced-functional devices)的能力则比较受限.部署前,首先通过有限域 $GF(q)$上的一条椭圆曲线及相关信息生成隐式证书(implicit certificate)和 FFD 节点、RFD 节点各自的公/私密钥.部署后,FFD 节点和 RFD 节点通过对方的隐式证书获取相应的公钥,然后各自随机生成链路密钥的基值,并使用对方公钥加密后发送给对方.若双方的链路密钥基值都得到验证,则与标识符 ID 一起共同协商生成链路密钥,FFD 节点与 RFD 节点就使用生成的链路密钥进行安全通信.在该方案中,FFD 节点和 RFD 节点都提供链路密钥的基值,但最终链路密钥是通过密钥派生函数生成的,因此,FFD 节点和 RFD 节点都不能完全控制对链路密钥的选择,攻击者为了获取私钥所付出的代价比解决椭圆曲线的离散对数问题(discrete logarithm problem,简称 DLP)所付出的代价还要大.该协议提供了隐式和显式的密钥验证,这样就能确保只要在运行期间不出错,双方接收到的信息都是正确的.

该协议把 ECC 所产生的计算开销大都集中在 FFD 节点,未过多增加 RFD 节点的计算和通信开销.Kotzanikolaou 对该协议进行了功能扩展[46],允许任意两个同构节点之间建立链路密钥.

3.8 基于IBC(identity-based cryptography)的密钥预分配方案[47]

与 CBC 相比,基于身份密码体制(IBC)[48]的主要优点是节点的公钥由公开信息直接推导获得,无须对公钥进行认证,从而有效地降低了计算复杂度和通信负载,被认为比较适用于 WSN.Zhang 提出了将 Bilinear Pairing 技术与地理信息相结合的 IBC 密钥管理方案.

部署前,节点 A 预加载系统参数($p,q,E/F_q,G_1,G_2,\hat{e},H,h,W,W_{pub}$)以及私钥 IK_A.其中,p 和 q 为有限域 F_q 的两个素数,E 为 F_q 上的椭圆曲线,G_1 和 G_2 分别是 F_q 上的加法群和乘法群,$\hat{e}$ 为双线性映射,W 是在 G_1 上随机选取的生成元,H 和 h 为两个散列函数,$W_{pub}=\kappa W$(κ 是主密钥),$IK_A=\kappa H(ID_A)$.部署后,节点 A 通过定位算法获取其位置信息 l_A 后计算其私钥 $LK_A=\kappa H(ID_A||l_A)$.节点 A 与邻居节点 B 可以通过获取公开的 ID 和对方的地理信息来建立配对密钥 $K_{A,B}$:A 生成配对密钥 $K_{A,B}=\hat{e}(LK_A,H(ID_B||l_B))$,$B$ 生成配对密钥 $K_{B,A}=\hat{e}(LK_B,H(ID_A||l_A))$,根据映射 $\hat{e}$ 的性质可知,$K_{A,B}=\hat{e}(\kappa H(ID_A||l_A),H(ID_B||l_B))=\hat{e}(H(ID_A\parallel l_A),\kappa H(ID_B||l_B))=K_{B,A}$,从而建立双方的配对密钥,在此基础上,使用 h 和配对密钥就可生成通信所需的各种类型的会话密钥.

该方案具有很强的容侵能力,任何节点的受损都不会暴露其他节点的机密信息.由于采用可靠的节点间认证机制,从而有效防止了 Wormhole,Sinkhole,Sybil 和 Bogus Data Injection 等攻击.但该方案也存在一些缺陷:一是在节点预分配的主密钥 κ 必须等待私钥生成后才能删除,若主密钥被暴露,则整个网络的机密信息都会暴露;二是因其位置是固定的,因而仅适用于静态 WSN;三是对节点资源的使用需求高,制约了其应用范围.

4 方案和协议的综合分析与所需解决的研究问题

从研究现状看,随机密钥预分配方案或协议被认为是最适用于 WSN[25,26]的,目前是 WSN 密钥管理的一个主流研究方向.表 1 在密钥池结构、密钥连接概率、抗毁性等方面对部分典型的随机密钥管理方案进行了比较.较高的密钥连通概率意味着相邻节点甚至全网络都可以达到较高的安全连通性;而密钥被暴露的概率越小,则意味着抗毁性就越好.在表 1 中,“↓”表示下降,“↑”表示上升,而“—”表示不变.

将密钥池设计为结构化、提高共享密钥阈值、利用地理信息或部署知识,可以有效地提高随机密钥预分配方案或协议的抗毁性.密钥连通概率与节点部署密度相关,其理论基础为经典的随机图模型.但文献[49]指出,经典随机图模型并不完全适用于 WSN,同时也指出如何选取适当的密钥池及密钥环大小,以确保获取较高的密钥连接概率.文献[50]也针对随机图模型以及若干个随机密钥预分配方案进行了深入分析.

表 2 通过处理复杂度、通信复杂度、存储复杂度以及网络可扩展性等性能指标比较了一些典型的密钥管理方案和协议.

© 中国科学院软件研究所 http://www.jos.org.cn

Table 1 Comparison of random key management schemes and protocols

表 1 随机密钥管理方案和协议的比较

Schemes and protocols	Structure of key pool	Key connectivity	Resilience	Comparison with E-G scheme	
				Key connectivity	Resilience
E-G scheme[25]	Non-Structure	$1-\frac{((P-k)!)^2}{(P-2k)!P!}$	$1-\left(1-\frac{k}{P}\right)^x$	–	–
q-Composite scheme[26]	Non-Structure	$1-\sum_{i=0}^{q-1}\frac{\binom{\lvert S\rvert}{i}\binom{\lvert S\rvert-i}{2(m-i)}\binom{2(m-i)}{m-i}}{\binom{\lvert S\rvert}{m}^2}$	$\sum_{i=q}^{m}\left(1-\left(1-\frac{m}{\lvert S\rvert}\right)^x\right)^i\frac{p(i)}{p}$	↓	↑
Multiple-Space key pre-distribution scheme[27]	Structured	$1-\frac{((\omega-\tau)!)^2}{(\omega-2\tau)!\omega!}$	$\le\omega\sum_{j=\lambda+1}^{x}\binom{x}{j}\left(\frac{\tau}{\omega}\right)^j\left(1-\frac{\tau}{\omega}\right)^{x-j}$	↓	↑
Polynomial-Based key predistribution scheme[28]	Structured	$1-\prod_{i=0}^{s'-1}\frac{s-s'-i}{s-i}$	$1-\sum_{i=0}^{t}\binom{N_c}{i}\left(\frac{s'}{s}\right)^i\left(1-\frac{s'}{s}\right)^{N_c-i}$	↑	↑
CPKS[29]	Structured	$\frac{c}{m}\iint_{(x-i_x)^2+(y-i_y)^2\le d'^2}\frac{p(v_{j_x,j_y},u_{i_x,i_y})}{\pi d'^2}\mathrm{d}x\mathrm{d}y$	0	↑	↑
LBKP[29]	Structured	$\frac{\sum_{C_{j_c,j_r}\in S_{i_c,i_r}}p(C_{j_c,j_r},C_{i_c,i_r})}{\sum_{\forall j_c,j_r}p(C_{j_c,j_r},C_{i_c,i_r})}$	$1-\sum_{i=1}^{t}\binom{N_s}{i}p_c^{\,i}(1-p_c)^{N_s-i}$	↑	↑
Key pre-distribution scheme using deployment knowledge[30]	Structured	$1-\frac{\sum_{i=0}^{\min(m,\lambda\lvert S_c\rvert)}\binom{\lambda\lvert S_c\rvert}{i}\binom{(1-\lambda)\lvert S_c\rvert}{m-i}\binom{\lvert S_c\rvert-i}{m}}{\binom{\lvert S_c\rvert}{m}^2}$	$1-\left(1-\frac{m}{\lvert S\rvert}\right)^x$	↑	–
Grid-Group deployment scheme[31]	Structured	$1-\frac{((\omega-\tau)!)^2}{(\omega-2\tau)!\omega!}$	λ-secure	↓	↑

Table 2 Performance comparison of key management schemes and protocols

表 2 密钥管理方案和协议的性能比较

Schemes and protocols	Computation complexity	Communication complexity	Storage complexity	Scalability
E-G scheme[25]	$o(k)$	$o(2)$	$o(k)$	Good
q-Composite scheme[26]	$o(m)$	$o(2)$	$o(m)$	Moderate
Multiple-Space key pre-distribution scheme[27]	$o(\lambda)$	$o(2)$	$o(\lambda\tau)$	Weak
Polynomial-Based key predistribution scheme[28]	t modular multiplication and t modular addition	$o(2)$	$o(t\log q)$	Weak
CPKS[29]	0	0	$o(c)$	Strong
LBKP[29]	t modular multiplication and t modular addition	$o(2)$	$o(t\log q)$	Moderate
Key pre-distribution scheme using deployment knowledge[30]	$o(m)$	$o(2)$	$o(m)$	Moderate
Grid-Group deployment scheme[31]	$o(\lambda)$	$o(\tau)$	$o(\lambda\tau)$	Moderate
Grid-Based key predistribution[28]	t modular multiplication and t modular addition	$o(2)$	$o(t\log q)$	Weak
PIKE	$o(2)$	$o(\sqrt{n})$	$o(\sqrt{n})$	Weak
Hybrid designs for scalable key distributions[33]	$o(n)$	$o(d)$	$o(n)$	Moderate
SNEP[34]	1 encryption and 1 MAC computation	$o(2)$	8bytes	Weak
μ TESLA[34]	1 hash computation	0	High	Weak
LEAP[35]	$o\left(\frac{d^2}{N}\right)$	$o(\log N)$	$o(d+L)$	Weak
SHELL	High	High	$o(k)$	Moderate
LOCK	High	High	$o(k)$	Moderate
Fast authenticated key establishment protocols[45]	760ms	1 437bytes	5.2kbytes	Moderate
Location-Based key management scheme[47]	62.04ms	84bytes	High	Strong

© 中国科学院软件研究所 http://www.jos.org.cn

随机密钥预分配方案或协议虽然不能提供最佳的密钥连通概率,但其计算、存储和通信开销较为理想,且具有良好的分布特性.而确定密钥预分配或非对称密钥管理方案和协议虽然可以保证任何两个节点都能建立密钥连接,但计算、存储和通信开销大的问题仍需进一步优化.

总之,虽然密钥管理的研究取得了许多成果,但密钥管理的方案和协议仍然不能满足各种应用需求,还存在一些需要解决的问题.具体如下:

(1) 建立多种类型的通信密钥.目前的 WSN 密钥管理方案和协议大多仅考虑建立邻居节点间的配对密钥,但配对密钥只能实现节点一对一通信,不支持组播或全网广播[21].方案或协议应建立多种类型通信密钥,满足单播通信、组播通信或广播通信等需求.

(2) 支持密钥的分布式动态管理.节点的受损是不可避免的,若要把受损节点排除于网络之外,首先要动态更新或撤回已受损的密钥,但目前的大多数方案或协议较少考虑密钥动态管理.已有的密钥动态管理方案多以集中式为主,产生了过多的计算和通信开销.密钥更新和撤回应以节点之间的协作实现为主,才能使方案或协议具有良好的分布特性[51].

(3) 提供有效的认证机制.密钥的协商需要对数据包和节点身份进行有效认证,否则不能保证所建立的通信密钥的正确性.单纯的 MAC 机制在对称密钥管理中存在被伪造的问题,基于非对称密钥的数字签名机制目前还不适用于 WSN.提供符合 WSN 特点的认证机制是密钥管理研究的重要内容.

(4) 支持容侵和容错.节点易受损及计算通信能力受限的特点,使得节点很容易受到 DoS 攻击[52],全面防御 DoS 攻击是比较困难的.此外,即使未受到安全威胁,节点出于对节能的考虑或因资源被耗尽导致不能保证永远处于正常运行状态,数据包丢失不可避免.因此,方案和协议应具有良好的容侵和容错性.

从体系结构的观点来看,密钥管理要为其他安全机制提供基础服务,并与这些安全机制共同组成 WSN 的整体安全解决方案.我们认为,实现跨层设计的密钥管理将有利于明确设计目标及性能优化.例如,目前绝大多数的密钥管理方案和协议都仅仅致力于建立相邻节点之间的通信密钥,而在一些有效的安全解决方案[12,53]里,多跳节点之间的通信密钥也是必要的.加强密钥管理与安全路由、安全定位、安全数据融合等安全机制的耦合,就能够从系统整体的角度对方案和协议的处理复杂度、存储复杂度和通信复杂度进行优化,从而使得所设计的密钥管理方案和协议更加符合 WSN 特点,具有良好的适应性.

运用符合 WSN 特点的理论分析方法进行密钥管理的研究是十分必要的,这样能够避免所设计的机制和算法过多地依赖直觉经验而缺乏严谨的、科学的、可信的理论依据,从而避免研究成果的片面性、局部化,甚至不可用.为了提供更加有效的解决方案,我们将依靠成熟且可行的理论方法,如随机图理论、信息论等理论方法,采用 WatchDog[54]、单向散列函数/链、self-healing 技术[55]等安全算法和技术,结合 WSN 的资源受限、拓扑易变、部署随机、自组织、规模大、无固定设施支持等特点,设计可行、可靠的密钥管理方案或协议,实现密钥管理机制和算法的可模型化、可度量化和可计算.

5 总结和展望

随着微机电技术、传感器技术、通信技术等技术的不断发展,无线传感器网络的应用必将不断深入和广泛.作为一项最基本的安全服务,密钥管理的研究将会引起更大的关注和重视.密钥管理的方案和协议必须符合和满足 WSN 特点,如可扩展性、计算复杂度小、存储空间需求低、通信负载低、拓扑结构易变等,也必须与应用密切相关.密钥管理方案和协议的全分布式、自组织性、容错容侵性、与地理信息相结合等研究问题,将是下一步的研究工作所需要重点关注和解决的.此外,当 WSN 节点资源不再受到严格限制时,非对称密钥管理方案和协议也必将成为具有潜力的研究方向.

致谢 在此,我们向对本文提出宝贵建议的审稿专家及参与本文内容讨论的所有老师和同学表示衷心的感谢.

© 中国科学院软件研究所 http://www.jos.org.cn

References:

[1] Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor network: A survey. Computer Networks, 2002,38(4): 393−422.

[2] Romer K. Mattern F. The design space of wireless sensor networks. IEEE Wireless Communications, 2004,11(6):54−61.

[3] Estrin D, Govindan R, Heidemann J, Kumar S. Next century challenges: Scalable coordination in sensor networks. In: Proc. of the ACM/IEEE Int'l Conf. on Mobile Computing and Networking. New York: ACM Press, 1999. 263−270.

[4] GENI. Global environment for network innovations. 2006. http://www.geni.net

[5] Ren FY, Huang HN, Lin C. Wireless sensor networks. Journal of Software, 2003,14(7):1282−1290 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1282.htm

[6] Li JZ, Li JB, Shi SF. Concepts, issues and advance of sensor networks and data management of sensor networks. Journal of Software, 2003,14(10):1717−1727 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1717.htm

[7] Carman DW, Kruus PS, Matt BJ. Constraints and approaches for distributed sensor security. Technical Report, #00-010, NAI Laboratories, 2000.

[8] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks. Communications of the ACM (Special Issue on Wireless Sensor Networks), 2004,47(6):53−57.

[9] Deng J, Han R, Mishra S. INSENS: Intrusion-Tolerant routing in wireless sensor networks. Technical Report, CU-CS-939-02, Colorado University, 2002.

[10] Lazos L, Poovendran R. SeRLoc: Secure range-independent localization for wireless sensor networks. In: Proc. of the 2004 ACM Workshop on Wireless Security. New York: ACM Press, 2004. 21−30.

[11] Przydatek B, Song D, Perrig A. SIA: Secure information aggregation in sensor networks. In: Proc. of the 1st Int'l Conf. on Embedded Networked Sensor Systems. New York: ACM Press, 2003. 255−265.

[12] Ye F, Luo HY, Lu S, Zhang LX. Statistical en-route detection and filtering of injected false data in sensor networks. IEEE Journal on Selected Areas in Communications, 2005,23(4):839−850.

[13] Diffie W, Hellman ME. New directions in cryptography. IEEE Trans. on Information Theory, 1976,22(6):644−654.

[14] Koc KC. High-Speed RSA implementation. Technical Report, TR201, RSA Laboratories, 1994.

[15] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612−613.

[16] Neuman BC, Tso T. Kerberos: An authentication service for computer networks. IEEE Communications, 1994,32(9):33−38.

[17] Mcgrew DA, Sherman AT. Key establishment in large dynamic groups using one-way function trees. IEEE Trans. on Software Engineering, 2003,29(5):444−458.

[18] Basagni S, Herrin K, Bruschi D, Rosti E. Secure pebblenets. In: Proc. of the 2nd ACM Int'l Symp. on Mobile Ad Hoc Networking & Computing. New York: ACM Press, 2001. 156−163.

[19] Crossbow Technology. MICA2: Wireless measurement system. http://www.xbow.com/Products/Product_pdf_files/Wirelesspdf/6020-0042-04_A_MICA2.pdf

[20] Shi E, Perrig A. Designing secure sensor networks. Wireless Communication Magazine, 2004,11(6):38−43.

[21] Karlof C, Sastry N, Wagner D. TinySec: A link layer security architecture for wireless sensor networks. In: Proc. of the 2nd ACM Conf. on Embedded Networked Sensor Systems. New York: ACM Press, 2004. 162−175

[22] Jiang YX, Lin C, Shi MH, Shen XM. Security in Sensor Networks. Oxfordshire: Taylor and Francis Group, 2006. 113−143.

[23] Gaubatz G, Kaps J, Sunar B. Public keys cryptography in sensor networks—Revisited. In: Proc. of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS). New York: ACM Press, 2004. 2−18.

[24] Malan DJ, Welsh M, Smith MD. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In: Proc. of the 1st IEEE Int'l Conf. on Sensor and Ad Hoc Communications and Networks. IEEE Press, 2004. 71−80.

[25] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks. In: Proc. of the 9th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2002. 41−47.

[26] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proc. of the 2003 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2003. 197−213.

© 中国科学院软件研究所 http://www.jos.org.cn

[27] Du W, Deng J, Han YS, Varshney PK. A pairwise key pre-distribution scheme for wireless sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2003. 42−51.

[28] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2003. 52−61.

[29] Liu D, Ning P. Location-Based pairwise key establishments for static sensor networks. In: Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2003. 72−82.

[30] Du W, Deng J, Han YS, Chen S, Varshney PK. A key management scheme for wireless sensor networks using deployment knowledge. In: Proc. of the IEEE INFOCOM. Piscataway: IEEE Press, 2004. 586−597.

[31] Huang D, Mehta M, Medhi D, Harn L. Location-Aware key management scheme for wireless sensor networks. In: Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2004. 29−42.

[32] Chan H, Perrig A. PIKE: Peer intermediaries for key establishment in sensor networks. In: Proc. of the IEEE INFOCOM 2005. Piscataway: IEEE Communication Society, 2005. 524−535.

[33] Camtepe SA, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. In: Proc. of the Computer Security—ESORICS. Berlin: Springer-Verlag, 2004. 293−308.

[34] Perrig A, Szewczyk R, Tygar J, Wen V, Culler D. SPINS: Security protocols for sensor networks. ACM Wireless Network, 2002, 8(5):521−534.

[35] Zhu S, Setia S, Jajodia S. LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2003. 62−72.

[36] Younis M, Ghumman K, Eltoweissy M. Location-Aware combinatorial key management scheme for clustered sensor networks. IEEE Trans. on Parallel and Distribution System, 2006,17(8):865−882.

[37] Eltoweissy M, Moharrum M, Mukkamala R. Dynamic key management in sensor networks. IEEE Communications Magazine, 2006,44(4):122−130.

[38] Moharrum MA, Eltoweissy M. A study of static versus dynamic keying schemes in sensor networks. In: Proc. of the 2nd ACM Int'l Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks. New York: ACM Press, 2005. 122−129.

[39] Blundo C, Santis AD, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly secure key distribution for dynamic conferences. Information and Computation, 1998,146(1):1−23.

[40] Bollobás B, Fulton W, Katok A, Kirwan F, Sarnak P. Rand Graphs. 2nd ed., Cambridge: Cambridge University Press, 2001. 160−200.

[41] Blom R. An optimal class of symmetric key generation systems. In: Beth T, Cot N, Ingemarsson I, eds. Proc. of the EUROCRYPT'84. New York: Springer-Verlag, 1984. 335−338.

[42] Liu D, Ning P. Multilevel μ TESLA: Broadcast authentication for distributed sensor networks. ACM Trans. on Embedded Computing Systems, 2004,3(4):800−836.

[43] Liu D, Ning P, Zhu S, Jajodia S. Practical broadcast authentication in sensor networks. In: Proc. of the 2nd Annual Int'l Conf. on Mobile and Ubiquitous Systems: Networking and Services. Washington: IEEE Computer Society, 2005. 118−129.

[44] Eltoweissy M, Heydari H, Morales L, Sudborough H. Combinatorial optimization of key management in group communications. Journal of Network and Systems Management, 2004,12(1):33−50.

[45] Huang Q, Cukier J, Kobayashi H. Liu B, Zhang J. Fast authenticated key establishment protocols for self-organizing sensor networks. In: Proc. of the 2nd ACM Int'l Conf. on Wireless Sensor Networks and Applications. New York: ACM Press, 2003. 141−150.

[46] Kotzanikolaou P, Magkos E, Douligeris C, Chrissikopoulos V. Hybrid key establishment for multiphase self-organized sensor networks. In: Proc. of the 6th IEEE Int'l Symp. on a World of Wireless Mobile and Multimedia Networks. Washington: IEEE Computer Society, 2005. 581−587.

[47] Zhang YC, Liu W, Lou WJ, Fang YG. Location-Based compromise-tolerant security mechanisms for wireless sensor networks. IEEE Journal on Selected Areas in Communications, 2006,24(2):247−260.

© 中国科学院软件研究所 http://www.jos.org.cn

[48] Shamir A. Identity based cryptosystems and signatures schemes. In: Proc. of the Advances in Cryptology. New York: Springer-Verlag, 1984. 47−53.

[49] Pietro RD, Mancini LV, Mei A, Panconesi A, Radhakrishnan J. Connectivity properties of secure wireless sensor networks. In: Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2004. 53−58.

[50] Hwang J, Kim Y. Revisiting random key pre-distribution schemes for wireless sensor networks. In: Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2004. 43−52.

[51] Chan H, Gligor VD, Perrig A, Muralidharan G. On the distribution and revocation of cryptographic keys in sensor networks. IEEE Trans. on Dependable and Secure Computing, 2005,2(3):233−247.

[52] Wood AD, Stankovic JA. Denial of service in sensor networks. Computer, 2002,35(10):54−62.

[53] Zhu S, Setia S, Jajodia S, Ning P. An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 2004. 259−271.

[54] Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In: Proc. of the 6th Annual Int'l Conf. on Mobile Computing and Networking. New York: ACM Press, 2000. 255−265.

[55] Staddon J, Miner S, Franklin M, Balfanz D, Malkin M, Dean D. Self-Healing key distribution with revocation. In: Proc. of the 2002 IEEE Symp. on Security and Privacy. New York: IEEE Computer Society, 2002. 241−257.

附中文参考文献:

[5] 任丰原,黄海宁,林闯.无线传感器网络.软件学报,2003,14(7):1282−1290. http://www.jos.org.cn/1000-9825/14/1282.htm

[6] 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.软件学报,2003,14(10):1717−1727. http://www.jos.org.cn/1000-9825/14/1717.htm

苏忠(1969－),男,广西玉林人,博士生,主要研究领域为网络信息安全,无线传感器网络.

封富君(1978－),女,博士生,主要研究领域为网络信息技术与网络安全,Petri 网,访问控制.

林闯(1948－),男,教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络,系统性能评价,可信网络与可信计算,随机 Petri 网.

任丰原(1970－),男,博士,副教授,博士生导师,CCF 高级会员,主要研究领域为网络流量管理与控制,无线传感器网络,系统性能评价.

© 中国科学院软件研究所 http://www.jos.org.cn