无线传感器网络密钥管理研究综述*

黄鑫阳，杨 明
(解放军理工大学 指挥自动化学院 计算机系，江苏 南京 210007)

摘 要：通过分析无线传感器网络安全现状和密钥管理所面临的问题，对现存的密钥管理方案进行了分析和评估，并讨论了该方向上尚未解决的问题和发展趋势。

关键词：无线传感器网络；密钥管理；抗毁性；预分配；连通性
中图分类号：TP309 文献标志码：A 文章编号：1001-3695(2007)03-0010-06

Survey on Key Management for Wireless Sensor Networks

HUANG Xin-yang, YANG Ming
(Dept. of Computer, Institute of Command Automation, PLA University of Science & Technology, Nanjing Jiangsu 210007, China)

Abstract: This paper first analyzed the status quo of WSN(Wireless Sensor Network) and its security requirements, evaluated the existing protocol such as key pre-distribution, key dynamic generation, etc. At last, it discussed the unresolved topics and development trends in this field.

Key words: wireless sensor network; key management; resilience; pre-distribution; connectivity

无线传感器网络(Wireless Sensor Network, WSN)通常由大量的微小自治设备——传感器节点组成，其上集成了传感器、微处理器、无线通信子系统以及能量供应子系统。通常，传感器节点是随机地部署在一定区域，负责监视和数据收集工作。WSN 势必将越来越广泛地应用于军事、战场环境监测和跟踪、生态环境监测、病体定位和跟踪以及恶劣环境的监测等[1]。其通信是通过集成在其上的射频设备来实现的，由于使用了全向天线，只要在接收范围内，任何人都可以接收到该网络的信息和数据。当无线传感器部署在具有敌意的区域，则面临着各种类型的窃听、攻击和物理俘获，安全问题变得极端重要起来。如果没有对敏感数据加密，任何一个攻击者可以轻易地窃听到传输的数据、伪装成网络中的节点或者恶意提供错误的数据、伪造网关，以阻止或误导信息传递。因此，必须对这类 WSN 提供安全保密性，即必须对通信进行加密或验证。于是 WSN 的密钥生成和管理问题便突显出来。

1 密钥管理背景

1.1 网络拓扑

(1) 等级拓扑。如图 1 所示，在等级拓扑中，按等级划分为基站、簇首和普通节点。整个网络分为几个簇，普通节点报告事件到簇首，簇首根据既定的策略将基站的报告转发到基站。在这样的拓扑中，不是所有的传感器节点都是等同的，其中具备了较强计算能力和较强生存能力的担任网络中的簇首；基站一般担负网关的角色，并且在很多密钥管理协议中，被当做可信第三方或 KDC。这类网络一般应用于可以准确部署网络的环境下，拓扑事先可以明确，因此也可以理解为可以照料的网络；对于其上的各种应用，也是确定性的。

(2) 分布式拓扑。目前研究的热点和难点主要集中于分布式的拓扑形式，如图 2 所示，尤其是对于预先无法明确部署状况的 WSN。对于此类网络，每个节点的硬件状况是完全等同的，在网络中的地位也是同等的。节点通过随机的方式散落在被监测环境中，自主地建立路由并实现网络连通性，最终以多跳的形式建立到基站的连接。在网络形成后，目前最通常的方式是动态地建立簇以收集本地的监测信息，并由当时的临时簇首来负责处理和转发数据。

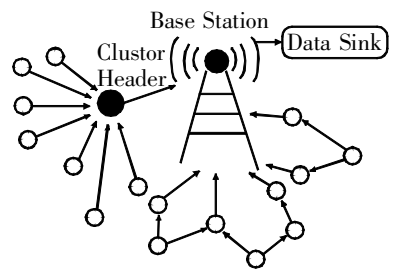

图 1 等级式拓扑

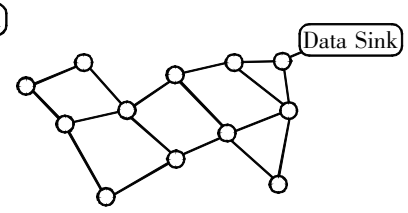

图 2 分布式拓扑

1.2 网络特性和主要相关技术

(1) 网络特性。①无线特性。全向性有限通信范围、不可靠。对于 WSN，报文的大小直接影响到丢包率问题，实验表明，基于典型的 Mica 平台和 TinyOS[2]，报文大小为 36 Bytes 时，丢包率达到最低[3]。②不安全性。由无线信道决定了网络通信是完全暴露的。③无人照料网络，网络实现自动管理，节点间协作性较高。网络在部署后，难以实施有效的外来管理。④网络部署的节点密集、规模大；节点无法预知全局拓扑，即使在部署形成网络之后，节点依然无法感知全局拓扑。⑤物理硬件受限。有限的能量、内存、计算能力和通信范围等，尤其是能耗问题。

(2) 主要相关技术。在这里讨论几个常用的，并且与密钥

收稿日期：2006-02-19；修返日期：2006-04-23 基金项目：国家自然科学基金重大资助项目(90304015)

作者简介：黄鑫阳(1979-)，男，福建泉州人，博士研究生，主要研究方向为密钥管理、无线网络安全协议；杨明(1968-)，男，副教授，博士，主要研究方向为信息安全、群组通信.

管理协议紧密相关的 WSN 应用层技术——内网数据处理。典型的有: ①数据融合[5] 技术。WSN 中, 以簇为单位实施监测任务, 当网络中出现监测对象时, 簇内成员向簇中的簇首报告信息, 由簇首来完成数据的融合, 并发送事件摘要到基站, 避免不必要的通信量和能量消耗。②数据聚集技术[6]。与数据融合的内网处理技术相类似。簇内的成员向簇首报告监测到的信息, 簇首不立即进行转发, 而是根据事先设定的定时器和聚集度(门限值); 当在定时器期满之前、达到聚集度要求时, 发送报告到基站。该技术避免了对同样事件的多次报告, 同时也避免了因为噪声或者波形畸变带来的误报[6]。聚集度和定时器值的设置成为关键。③被动参与技术[7] (Passive Participate)。传感器节点在监测到事件发生后, 同时也检测到有邻居节点发送了相同的事件, 则该节点抑制了本地的重复消息发送, 阻止多余的信息在网络的传输引起能量消耗。该技术对于节点部署密集的 WSN, 节能效果明显。

1.3　安全需求

WSN 不同于传统的计算机网络, 它具有传统计算机网络所不具备的特性。因此, 除了要具备传统网络密钥管理的一些基本需求外, 如保密性、完整性、真实性/可验证等, 也提出了一些特别的要求:

(1) 协议和算法的轻型化。由于硬件存储能力和能量消耗的限制, 要求应用于 WSN 的密钥管理协议所必需的通信量、计算量和存储需求比较小。

(2) 保证网络可用性/可达性。为了节约资源和延长寿命, 传感器节点要避免不必要的密钥管理信息和操作, 即密钥管理系统不能使网络中节点因为能耗问题而引起单点失效; 此外, 密钥管理协议不能阻碍传感器网络有效执行监测任务, 如因为实施安全措施妨碍内网处理技术的运行; 最后, 密钥管理协议要减小因节点被物理俘获造成的对于网络其余部分的影响。

(3) 可扩展性。随着 WSN 规模的增大, 保证密钥管理带来的通信、计算和存储负担增加不明显, 理想的状态应该是与网络规模无关的。

(4) 自组织性。WSN 部署前, 关于网络的部署知识无法预先得知, 因此密钥管理协议必须能够选择适当的机制来满足这样的特性; 同时, 对于应用在传感网络的密钥管理协议, 还必须与其他协议结合使用来增强功能, 如簇首的选举和轮转协议等。

2　现有主要方案分析

现有 WSN 的密钥管理协议大多数是基于对称加密算法的。因为公钥加密算法(如 RSA) 是计算密集型的算法, 每执行一个安全操作都需要 CPU 执行几百万甚至更多的乘法指令操作。而对于对称密钥加密算法的加密、解密和用于签名认证的散列函数来说, 所需 CPU 操作指令数却少得多。因此选择不同的密钥体制将会直接影响到 WSN 的寿命。例如, 在 Dragon Ball 微处理器上用 RSA 公钥加密算法对 1 024 位数据进行加密计算大约需要 42 mJ 的能量; 而采用 128 位 AES 计算大约只需 0.104 mJ 的能量[8]。以下讨论的密钥管理方案是基于对称密钥实现的。

在 WSN 中, 由于网络的拓扑情况不能事先预知, 节点只能在部署后, 通过协商、计算的方式得出节点之间的密钥、簇密钥或者是组密钥。目前针对 WSN 的密钥管理解决方案大致可以分为以下三类:

(1) 基于密钥分配中心(KDC) 和主密钥方式。该类协议基于单个密钥或密钥服务器来提供整个网络的安全性, 因此存在网络瓶颈和单点失效问题。它侧重于考虑 WSN 的能耗要求和存储要求, 实现比较简单, 但主密钥更新问题难以解决。其前提假设是初始化阶段, 主密钥不会发生泄漏。

(2) 基于预分配方式。WSN 网络部署不可预知的特性是该类协议产生的最大动力。网络部署前, 预先在节点上存储一定数量的密钥或计算密钥的素材, 用来在节点部署阶段生成所需的密钥。它侧重于提高网络安全性能, 消除了对于可信第三方是单个密钥的依赖, 也消除了网络瓶颈。其最初的预分配原形 E&G 协议在存储和通信开销方面比方式(1) 有所增加, 在后续的方案中, 从不同的角度分别对该协议进行了改进, 分为基于密钥池的预分配协议、基于动态计算的预分配方式和基于网络部署知识的预分配方式。

(3) 基于分组、分簇实现方式。该类协议将网络的节点动态或静态地分成若干个组或簇, 这类方案更加贴近于 WSN 的实际应用, 尤其是基于分簇实现的密钥管理协议。另外, 分组或者分簇实现能够有效减少节点上的密钥存储量; 但是当节点使用组密钥或簇密钥加密时, 单点失效影响的网络部分将扩大到一个组或者一个簇。因此, 如何有效地减小单点失效对于网络剩余部分的影响, 是这类协议尚待解决的一个主要问题。

2.1　基于 KDC 和主密钥方案

(1) SPINS 方式[10] 的基本思想是假设在网络中存在可信第三方 S 来执行密钥的协商和交换; 每个节点与服务器共享一个密钥, 类似于 Kerberos 协议。基本协商过程如图 3 所示。

该协议的主要优点是节点抗毁性好且实现简单; 存储开销是一个常数; 节点可以通过第三方来协商出节点对之间的密钥, 但是若没有协商出节点对密钥, 则无法支持内网处理技术。其存在的问题是服务器上的通信、存储开销会随着网络规模的增加成为瓶颈, 因为其密钥存储数量等于网络中的节点数目; 同时, 也要求网络中必须有具备健壮抗毁性能的可信第三方, 或者每个节点必须能够在部署后就具备与基站或者第三方通信的能力, 具有较大的局限性。

(2) 基于主密钥方式。全网节点共享一个密钥, 通过该密钥来实现验证并协商节点对密钥。文献[12, 13] 提出的协议本质上属于 C&R(询问—回答) 方式, 全网节点共享一个主密钥, 是一种简单的验证和密钥协商协议, 网络中的节点使用主密钥进行互相验证。这些方式不需要传感器网络中存在可信的第三方来实施密钥协商协议, 基本方式如图 4 所示, 图 4 也可以当作密钥对建立的基本模型。

这类方式对于基本的安全应用能够达到要求; 由于全网节点全部依赖于主密钥, 单点失效会引起网络崩溃; 另外, 通信开销比较大, 内网处理技术支持能力差。

(3) BROSK[13] 的基本思想是对 SPIN 方式进行改进, 使之达到节能的目的。该改进来源于如下观察结果: 加密的能量开销约为发送信息能量消耗的 3%。BROSK 协议将节点多次广

播降低为节点的一次广播完成。全网节点共享一个主密钥,由主密钥加密并验证广播信息,方式如下:

SN_i: { ID_i | N_i | $MAC_K(ID_i | N_i)$ } $K_{ij} = MAC_K(N_i | N_j)$

该协议最显著的优点是 BROSK 协议大大节约了能量消耗;但是基于简单主密钥来实现,一旦主密钥泄露,整个网络的安全性将遭到破坏,因此该协议的抗毁性能差。对于这类方案,如果要提高网络抗毁性,面临的主要问题在于密钥更新。对于 WSN 而言,全网密钥更新通信开销大、时延长、实现复杂。

2.2 基于预分配方案

为了提供 WSN 中邻居节点之间通信的安全,最原始的想法是在节点上预先存储所有节点之间的会话密钥用来加密通信。对于网络规模为 n,全网中需要的密钥总数为 C_n^2,每个节点存储 $(n-1)$ 个密钥。

该方案的优点是完美安全,无单点失效威胁,支持节点的动态离开。但节点存储负担大、网络可扩展性差,新增节点加入难以实现,对于网络连通性而言,存储了多余密钥。

这类方法一般分为如下几步:初始化阶段、节点部署阶段和密钥建立阶段。密钥建立阶段包括直接密钥建立和间接密钥建立。各种方案的差异在于初始化以及密钥建立阶段采取的不同机制分别有其自身特点。为了解决在网络部署后,节点仅与邻居之间建立会话密钥,提出了以下几种预分配方案。

(1) 基于密钥池预分配方案。该方案包括 E&G Scheme、Q-composite Scheme、OKS,完全消除了对于 TTP 的依赖。

E&G [14] 提出了一种全新的方式,目的是实现在节点部署之后,能够自主地与邻居节点建立密钥对,克服了 WSN 部署前无法预知的障碍。其基本思想是在节点部署前,所有的节点随机地从一个很大的对称密钥池中选取一部分密钥子集作为该节点的密钥环,并预先存储到节点上;在节点部署后,通过某种方式与直接邻居互相发现各自预先存储的子集间共同拥有的部分,称为共享密钥,并将这些作为邻居之间的会话密钥。若是直接邻居间没有共享密钥,则需要建立密钥对。通过已建立的安全链路迂回建立会话密钥,称之为间接密钥。根据随机图论知识[15] 可以推导出在随机图 $G(n, p_i)$ 中,为了达到期望的连通概率 P_C 时,节点的度 d、网络规模 n 以及节点存储密钥环大小 k 之间的关系。

该方案的特点是使得节点能够与邻居建立安全链路,存储量需求下降。但因为是基于概率的,不能提供确定的安全性,且节点密钥对中,可能存在同样的共享密钥,单点失效会引起网络中其余部分的不安全;另外一个不足之处在于部署阶段缺乏验证,内网处理技术支持能力较差,通信量比基本方案有所增加。

文献[13] 提出了一种对 E&G 方式的改进,简称为 OKS。它是使用一个长的比特字符串 KP 作为密钥集合;每个节点从中随机选取一段作为该节点的密钥子集;会话密钥用节点间的共享比特字符串来代替;其他阶段与 E&G 方式相类似,如图 5 所示。该方式相比较于 E&G 方式具有以下优点:内存的占用减少,而且提高网络安全性时,内存的需求不显著;对于不同应用程序的不同安全需求时,调节灵活。存在的问题在于:共享的字符串长度可能不等,即节点间使用的密钥长度不相等,导致硬件实现困难且全网中的安全性能不均匀。

Chan、Perrig 和 Song[16] 基于 E&G 协议提出了改进,基本思想类似 E&G 协议。改进在于 Q-composite 方案把原来的共享密钥要求提高为 q 个,由这 q 个密钥来生成通过异或计算节点之间的会话密钥,使得网络中使用同样会话密钥的概率大大地降低。这对于防止小范围的节点俘获失效能力有所提高。但是随着被俘获节点的增多,网络中剩余的部分受影响的范围将迅速增加。其付出的代价是存储量增加,对于网络规模的要求也增大,即网络规模的增加带来的节点存储需求增加速率大于 E&G 方式。

该想法来源于图 6 所示的仿真现象的观察。对于共享密钥个数增多(在一定的范围内,),攻击者想要攻破某一链路的难度呈指数上升。然而为了保证节点之间较高的密钥共享概率来建立安全信道,则必须减小密钥池 $|S|$ 的大小,这样却导致了攻击者俘获少量节点后能够获得密钥池中占比例较大的密钥。这是一对矛盾的因素,因此寻找最佳点成为该方式的动力。

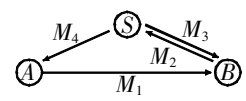

图 3 基本协商过程

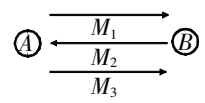

图 4 C&R 基本方式

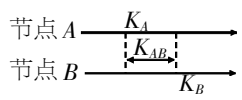

图 5 OKS

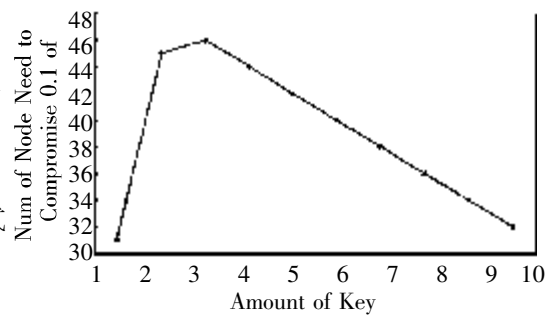

图 6 仿真现象的观察

Chan Aldar 等人[17] 主要面向于解决网络中的移动节点,根据预分配思想,节点预先存储 CFF(Cover Free Family) 子集,根据 CFF 子集的性质,本地节点能够独立计算与即时邻居的通信密钥。该协议的特点是消除了对可信第三方的依赖,通信量低,节点可独立地计算密钥对和组密钥;但其计算及存储开销较大,比较适合应用于 Ad hoc 网络密钥管理。

(2) 基于动态计算的预分配方案。其主要的典型协议有 Blom's Scheme[18]、Blom's Scheme 扩展到多空间[19]、Blom's Scheme 与 E&G Scheme 结合[20]、基于多项式方案[21]、多项式方案扩展到多维空间[22]。

Blom 利用对称矩阵的特性构造了一类新的会话密钥分发方式应用到传感器网络中,使得节点能够与邻居中的任何一个节点独立计算会话密钥,即 $k_{ij} = A(i) \times G(j) = k_{ji} = A(j) \times G(i)$。基于上述思想,使用 k_{ij} 和 k_{ji} 作为节点 i 和 j 之间的会话密钥。

Blom 方式具有 λ-secure[18],即网络中只有多于 λ 个节点被攻破后,整个网络才被攻破。存储负载为 $(\lambda+1)$ 个密钥长度,即 λ 个长度的矩阵行和一个矩阵生成元 g;λ 作为一个调节参数调节安全性和存储负载,当 $\lambda = n$ 时,网络是完美安全的;网络中任何一个会话密钥都是唯一的,能防止单点失效对其余部分的影响;但它同样在部署阶段缺乏验证,若要获得高安全性,则需要较高的存储,另外计算开销较大,内网应用支持能力较差。

Du 等人[19] 将此种方式扩展到了多维空间上,目的是为了提高网络抗毁性,是某种意义上与 E&G 方式的结合。将一维的密钥空间扩展定义为多维空间,即 (D, G), $D = \{D_1, \cdots, D_\omega\}$,

则 $A_i = (D_i, G)$; 每个节点从 (D, G) 中随机选取 τ个密钥空间作为本节点的密钥子集。在密钥协商阶段,每个节点首先要发现邻居节点是否与本地有共同的密钥空间;如果有共享的密钥空间则广播信息,在该信息中包含了密钥空间的索引和 G_i。余下的协商步骤与 Blom 方式是一致的;基于概率的分析与 E&G 方式相类似。随机选取了 τ个密钥空间预先存储在节点上,存储开销为 $(\lambda+1)\ \tau$ 与 Blom 协议相比,其安全性增强,但付出的代价是存储和计算开销增大。

Alan 和 Kosaka 等人[20] 将 Blom 协议和 E&G 协议糅合在一起,即密钥的前一半使用 E&G 协议,后一半利用 Blom 计算得出,两个半密钥连接形成一个完整的会话密钥。它消除了网络中可能存在的重复密钥,提供了唯一密钥,并且继承了 λ-secure,提高了网络的抗毁性;理论上降低了存储需求,相比 Blom 协议,降低了计算量。

Blundo[21] 提出了一种基于多项式计算的密钥管理协议,目的在于建立网络中所有节点之间的密钥对。其基于以下的基本思想: 对于一个 $2t$ 次方的二元多项式 $f(x,y) = \sum_{i,j=0}^{t} a_{ij} x^i j^j$,具有 $f(x,y) = f(y,x)$ 性质。类似于 Blom 方式对称密钥的思想,用该性质来计算网络中节点密钥对,即节点上预先存储 $f(x,i)$, i 为节点标志符,仅仅需要邻居节点的标志符 j 即可独立计算 $f(i,j) = f(j,i)$。应用于传感器网络时,由于节点的能耗要求严格,而该方式所需的计算量大,当网络规模增大时,可用性不强。

Liu 和 Ning[22] 基于上述思想将之扩展到多维的空间,每个节点从中预先存储几个空间,在部署阶段由发现共享密钥改为发现共享空间,若有相同的空间时实施上述计算。其主要目的是为了降低 t 的次数,以降低节点上的计算负担。该方式具有唯一密钥,抗 t 次合谋攻击,虽然与 Blundo 方式相比,计算量有很大的降低,但仍然保持相当的计算量,通信量增加。

Shih-I Huang[23] 提出了一种基于预先存储单向函数来计算密钥对的方式。其基本思想是在无线传感器节点上,每个节点 SN_i 都有一个唯一的标志符 ID_i,首先给每个节点分配一个单向函数 F_i,并预先存储部分节点标志符和密钥,每个节点随机选取 d 个其他节点的标志符存储于节点之上。其中, d 满足图的连通性;每个被选择的节点按照 $K_j = F_{v_j}(ID_i)$ 来计算密钥,并存储于节点上。过程如下:

SN_i 广播 $SN_i \rightarrow SN_j$: { ID_i} ;

SN_j 验证密钥环,若 SN_i 与密钥环中的某个密钥 K_s 相对应,则 $SN_j \rightarrow SN_i$: { $ID_j \parallel E_{K_s}$[Request Message] } ;

SN_i 收到后,计算 $K_s = F_i(ID_j)$,解密信息,并发送 ACK: $SN_i \rightarrow SN_j$: { E_{K_s}[ACK and Challenge Message] } ;

SN_j 收到后,响应信息: $SN_j \rightarrow SN_i$: { E_{K_s}[Response for the Challenge] 。

该方式与 E&G 协议相比,在同样存储需求的条件下能达到更高的连通性;另外一个改进是提供了不重复的密钥对,降低了因为单点失效对于网络安全性的影响。但是其通信开销和计算开销比基本方式大,可适用于存储能力较低的传感器网络。

(3) 基于网络部署知识密钥管理方案[24]。在预分配方案中,密钥池的大小 $|S|$ 是一个重要的调节参数。 $|S|$ 大时,网络抗毁性增大,而网络的连通性能下降,同时为了提高连通性,内存需求 m 也增大。文献[24] 提出的方案旨在解决如何在大的 $|S|$ 下保持高连通性;或者是在相同的 $|S|$ 下,需要更少的内存和更高的连通性以及网络抗毁性。基于上述目的,提出一种新的密钥预分配观点,即根据部署的知识来指导密钥的预分配。节点在部署的过程中虽然是随机的,但是根据部署的方式,节点之间成为邻居还是呈现一定概率分布的,而根据这些概率密度函数来指导预先存储于节点上的密钥,避免了节点上不必要的密钥预存储。基本的密钥预分配方案中,通常默认地假设节点是单个部署或者服从均匀分布的,于是无法判断节点之间的远近概率。然而当概率密度函数 $f(x,y)$ 是非均匀分布时,如服从正态分布,节点落于 3σ范围内的概率大于 0. 99,当两组节点之间的距离超出 6σ时,则成为邻居的概率相当低。

该方案同 E&G 方式相比,在相同的条件下,本地连通性能提高七倍。网络抗毁性: K 代表链路之间未被攻破的会话密钥,当 x 个节点被攻破时, K 不被攻破的概率为 $(1 - m/|S|)^x$,则整个密钥被攻破的概率估值为 $1 - (1 - m/|S|)^x$。从上式中也可以直观地看出,需要的 m 越小,则网络的抗毁性越高,同时对存储器的需求也降低了。

2.3　基于分组/簇方案

将 WSN 分割成多个组/簇,基于组/簇来实施密钥管理,目前主要有基于单向函数分组[25]、基于分簇[26]、多层次密钥 LEAP[27]。

文献[25] 对文献[23] 进行了扩展,将全网的节点预先分成几个子组,每个子组共享一个组标志符 GID_i,节点预先选取几个组密钥存储,组间密钥对的计算为 $k_{ij} = F_j(GID_i)$。基本算法如下:

(1) 如果 $GID_i = GID_j$,并且存在共享密钥,则节点间的会话密钥 $k_s = k_i \bar{1}$ sharedkeys;否则, $k_s = k_i$。

(2) 如果 $GID_i \neq GID_j$,当节点 A 上有 k_{ij}, B 上有 k_{ji}(k_{ij}和 k_{ji} 根据单向函数计算得来[23]),则 $k_s = k_{ij} \bar{1} k_{ji}$;当只有一个节点能够计算出组间密钥时, $k_s = k_{ij}$,否则节点之间无法计算出会话密钥。

其存储需求比起基本的 E&G 方式大约能节省 60%,但是随着网络规模的增加,这种优势急剧下降。该方式对于小规模攻击提供了较好的网络抗毁性,但是当攻击规模增大时,对于网络的影响呈指数上升。它采取了分组的方式,节点上预先存储量减少,因此对于支持更大型的网络能力增加,可扩展性较好;但其计算开销比较大,且当节点被俘获后,无法继续支持网络节点的加入,因为存储于节点上的相关密钥素材已全部泄露。

LEAP[27] 首次提出了在传感器网络中,针对不同的数据提供不同的安全机制。设计该协议的驱动来源于以下的观察: 不同的消息类型有不同的安全需求,单一的密钥无法满足多种需求。因此 LEAP 协议建立了四种类型的密钥,即私钥、密钥对、簇密钥和全组密钥;同时 LEAP 还包含一个基于单向密钥链实现的广播验证协议。

(1) 私钥,每个节点与基站共享的密钥,用来加密节点到基站的通信。

(2) 组密钥,由网络中的所有节点和基站共享,基站使用该密钥发布指令以及询问等。从加密效率的角度来看,使用多个密钥来分别加密广播消息是低效的,但是对于单个节点被攻

破后,密钥更新时必须使用单个密钥来分别加密广播消息。

(3) 簇密钥,节点与直接邻居共享,主要用来加密本地广播消息,如路由控制信息、加密传感器报文。建立过程如下:节点 u 随机产生簇密钥 K_c^u,并利用节点密钥对分别加密发送给邻居节点,邻居节点在收到信息后,解密存储簇密钥,并且发送自己的簇密钥给节点 u。当撤销网络中的某个节点时,删除相应的节点簇密钥,并且重复上述过程。

(4) 节点间密钥对,用来加密需要保密或者源验证的消息,如加密聚集数据、发送簇密钥等。其建立的方式与基于单向函数的方式相类似。

该协议的优点在于能够支持多种传感器网络的通信模式,同时能够在一定程度上支持内网处理技术。不足之处是通信开销大、单点失效问题没有解决好、存储需求较大;对于簇以及簇密钥生成、更新阶段十分低效;簇交替覆盖率高,在实际的传感器网络的一个时期内,对于网络中的分簇并不需要同时高的簇交替覆盖率,另外在实际应用中,簇是动态变化的。

Tassos 和 Ioannis[26] 提出了另外一种思路,即将 WSN 分成若干个簇,并且这个过程是在网络部署后、初始化阶段完成的。簇内成员共享一个簇密钥,簇之间的通信通过邻居节点(指被多个簇的通信范围所覆盖)来完成,即在簇间节点上存储多个密钥来从事类似“翻译”的任务,这样全网就连通了。图 7 所示的节点 17、25、5 和 1 为三个簇的邻居。

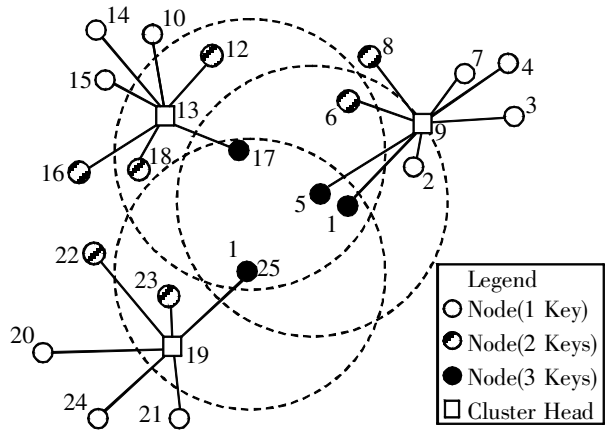

图 7 将 WSN 分成若干簇

该方案的存储需求大大减小,计算负担减少,通信量较小,以簇的方式更加贴近应用。簇操作在初始化阶段完成,在网络的运行阶段并没有发生簇的变动。另外一个尚未解决的问题,即有效的簇密钥更新和单点失效问题。试验表明,对于以该方式建立的典型网络,邻居节点的比率随着网络中邻居节点的增加大约从 4 开始递增。也就是说,网络中的节点失效后,影响的范围至少是三个簇以上,对于该种协议,单点失效节点所在的簇将彻底不可用,必须全部;而对于删除相对集中的一个簇,极有可能引起网络拓扑图的不连通,导致整个网络的不可用。

2.4 小结

表 1 为上述大多数方式的一个基本比较。其中,n 为网络规模,n 为邻居节点个数,d 为节点的度,p 是两个节点之间存在链路的概率,c 为参与节点数目,k 为节点密钥护环大小,λ 代表安全门限,ω为空间个数,τ为所选取的空间个数,g 为一次密钥产生包含的节点个数;另外,F 代表单向函数计算开销,RF 代表伪随机函数计算开销,H 代表哈希函数计算开销,S 代表搜寻共享密钥开销。

表 1 各种方式的基本比较

解决方案	扩展性	连通概率	抗毁性	内存需求	计算开销	通信开销
SPINS	一般	1	n	1	1 个 RF	1
TESLA	一般	1	一般	高	2 个 MAC	同网络规模相关
μ-TESLA	较好	1	一般	较低	1 个 H + 1 个 MAC	同网络规模相关
轻量级	一般	1	较好	$4 + 2g$	S	$2d + 2$
C&R	一般	1	1	$n' - 1$	2 个 MAC	3
All Pair-wise	一般	1	n	$2(N - 1)$	S	2
E&G	较好	$\frac{[(kp - k)!]^2}{(kp - 2k)!\ kp!}$	k/kp	$2k$	S	$k + dk$
Q-composite	一般	较低	$\binom{k}{q} \Big/ \binom{kp}{q}$	$2k$	S	$k + dk$
Random Pair-wise	较好	$np/(n - 1)$	差	$2np$	S	$1 + d$
Blom 's	较好	1	λ	$2(λ + 1)$	$(λ + 1)$ 次矩阵行列运算	$(λ + 1) \times (d + 1)$
Blom & 多空间	较好	$\frac{((ω - τ)!)^2}{(ω - 2τ)!\ ω!}$	见文献	$2τ(λ + 1)$	S, $(λ + 1)$ 次矩阵行列运算	$2(λ + 1) \times (d + 1)$
Blom + E&G	较好	同 E&G	λ	$λ + 1 + k$	$(λ + 1)/2$	$k + dk$
多项式	差	1	t	$t + 1$	多项式计算	t
多项式 & 多空间	较好	1	见文献	$2(t + 1)$	S, 多项式计算	$2(d + 1)$
基于部署概率	好	根据不同分布而定	k/kp	$2k$	S	$d(k + 1)$
Si-huang	一般	$1 - (1 - \frac{d}{n - 1})^2$	一般	见文献	d 个 F	$2d + 1$
分组方式	较好	根据分组而定	一般	见文献,根据分组多少而定	S + F	$2d + 1$
分簇方式	较好	1	差	2	S	2
LEAP	一般	1	差	4	1 个 MAC + m 个加密开销	$6 + m$

3 总结和展望

根据上述分析,针对不同的网络假设和需求,当前已经提出了一系列的管理协议,它们有各自的优点和适用的网络环境,也都存在一些不足。而随着工艺和计算机及其网络技术的发展,WSN 必将越来越广泛地得到应用,迫切地需要高效、轻量的密钥管理协议。将来 WSN 密钥管理研究方向和问题主要集中于以下几个方面:

(1) 传统网络的密钥管理研究已经进展了多年,也取得了相当的成果。但是由于 WSN 与传统网络的计算能力和能耗限制差别较大,直接移植过来无法满足 WSN 的需求。在研究现有普通网络中的密钥管理方式,并考虑如何结合传感器网络的特性进行改造时,主要应该考虑 WSN 的两个特性,即无法预知网络拓扑和协议必须有较低的能耗。

(2) WSN 基于无线信道是具有一定丢包率的网络[28]。目前绝大部分的方案都是假设网络不存在丢包的情况来实现密钥管理的。而很多密钥协议的密钥生成、更新阶段,对于信息包交换的可靠性却是要求很高的,如上面讨论过的大部分密钥管理协议。因此在密钥管理协议设计中,由于无线链路的特性,应该结合考虑到网络的不可靠性,即允许一定丢包率的现实情况来实现密钥管理协议。

(3) 结合传感器网络的应用技术,如簇相关的生成、选举和轮转协议,降低密钥管理协议对网络应用的影响。因此带来的挑战是如何根据动态簇的变化来生成和更新簇密钥问题,使得密钥管理协议满足能量均匀分布和内网应用技术。

(4) 目前对于 WSN 的密钥更新问题,包括有效的节点撤

销和加入问题研究得较少, 而对于传感器网络无人照料的特性, 这些问题又是密钥管理中不可避免的。对于 WSN, 没有明确的边界区分内部网络和外部网络, 容易遭致物理攻击, 如物理改变、俘获等。一旦这样的攻击成功, 节点上的秘密信息将全部泄漏, 因此对于 WSN, 密钥的有效撤销是保障网络持续可用的必要手段。但当前比较系统和专门考虑这个问题的仅有文献[29]。

(5) WSN 的主要弱点来源于开放的分布式架构, 不像有线网络中有专门的路由设备, WSN 中的每个节点都有可能成为转发数据报文的临时路由, 而无线信道的特性又是开放的, 这对 WSN 的安全协议提出了更高的要求[30]。在设计 WSN 的安全协议时, 不仅要考虑到应用层的数据报文安全, 同时也应该考虑到类似路由信息、控制信息的安全, 分析不同报文的不同安全需求。因此应该结合网络层安全路由协议, 整体地来设计和实现具有层次性的密钥管理协议。

(6) 进一步探索如何有效地减小管理协议对内存的需求, 提高网络的抗毁性能, 以降低计算量和通信量。

参考文献:

[1] KYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, *et al*. A survey on sensor network[J]. **IEEE Communications Magazine**, 2002, **40**(8): 102-114.

[2] HILL J, SZEWCZYK R, WOO A, *et al*. System architecture directions for networked sensors: proc. of ASPLOS IX[C]. [S. l.]: [s. n.], 2000.

[3] Crossbow Technology Inc. http://www.xbow.com[EB/OL].

[4] INTANAGONWIWAT C, GOVINDAN R, ESTRIN D. Directed diffusion: a scalable and robust communication paradigm for sensor networks: proc. of MobiCOM '00[C]. Boston: [s. n.], 2000.

[5] FENG Z, JAEWON S, JAMES R. Information-driven dynamic sensor collaboration for target tracking[J]. **IEEE Signal Processing Magazine**, 2002, **19**(2): 61-72.

[6] HE Tian, KRISHNAMURTHY S, STANKOVIC A J, *et al*. Energy-efficient surveillance system using wireless sensor networks: MobiSYS '04[C]. [S. l.]: [s. n.], 2004.

[7] KARLOF C, LI Y, POLASTRE J. ARRIVE: an architecture for robust routing in volatile environments, UCB/CSD-03-1233[R]. Berkeley: University of California at Berkeley, 2003.

[8] CARMAN D, KRUUS P, MATT B. Constraints and approaches for distributed sensor network security[R]. [S. l.]: NAI Labs, 2000.

[9] SUNG P, ANDREAS S, MANI B S. Simulating networks of wireless sensors: proceedings of the 2001 Winter Simulation Conference[C]. [S. l.]: [s. n.], 2001.

[10] PERRIG A, SZEWCZYK R, WEN V, *et al*. SPINS: security protocols for sensor networks: proc. of the 7th Annual Int'l Conf. on Mobile Computing and Networks[C]. Rome: ACM Press, 2001: 189-199.

[11] MENEZES A J, OORSCHOT P C, VARSTONE S A. Handbook of applied cryptography[M]. [S. l.]: CRC Press, 1997.

[12] DUTERTRE B, CHEUNG S, LEVY J. Lightweight key management in wireless sensor networks by leveraging initial trust, SRI-SDL-04-02[R]. [S. l.]: [s. n.], 2004.

[13] CHENG B, SUNGHA D. Reduce radio energy consumption of key management protocol for wireless sensor networks: ISLPED '04, ACM[C]. [S. l.]: [s. n.], 2004.

[14] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks: proceedings of the 9th ACM Conference on Computer and Communications Security[C]. [S. l.]: [s. n.], 2002: 41-47.

[15] SPENCER J. The strange logic of random graphs[M]. [S. l.]: Springer-Verlag, 2000.

[16] CHAN H, PERRIG A, SONG D. Random key pre-distribution schemes for sensor networks: IEEE Symposium on Security and Privacy[C]. [S. l.]: [s. n.], 2003: 197-213.

[17] CHAN C-F A. Distributed symmetric key management for mobile Ad hoc networks: IEEE INFOCOM[C]. [S. l.]: [s. n.], 2004.

[18] BLOM R. An optimal class of symmetric key generation systems. THOMAS B, NORBERT C, INGEMAR I. Advances in Cryptology: Proceedings of EUROCRYPT '84, Lecture Notes in Computer Science[C]. [S. l.]: Springer-Verlag, 1984: 335-338.

[19] DU Wenliang, DENG Jing. A pairwise key pre-distribution scheme for wireless sensor networks: CCS '03[C]. [S. l.]: [s. n.], 2003.

[20] ALAN P, KRISTIE K, SAMIR C. A secure key management scheme for sensor network: proceedings of the 10th Americas Conference on Information System[C]. [S. l.]: [s. n.], 2004.

[21] BLUNDO C, SANTIS D A, HERZBERG A, *et al*. Perfectly-secure key distribution for dynamic conferences: Cryptology-CRYPTO '92, LNCS 740[C]. [S. l.]: [s. n.], 1992: 471-486.

[22] LIU D, NING P. Establishing pairwise keys in distributed sensor networks: proceedings of the 10th ACM conference on Computer and communication security[C]. [S. l.]: [s. n.], 2003: 52-61.

[23] WU S Y, SHIEH S P. Adaptive random key distribution schemes for wireless sensor networks: proc. of the Workshop on Advanced Developments in and Systems Security[C]. [S. l.]: [s. n.], 2003.

[24] DU Wenliang, DENG Jing, HAN Y S, *et al*. A key management scheme for wireless sensor networks using deployment knowledge: IEEE INFOCOM[C]. [S. l.]: [s. n.], 2004.

[25] CHUANG Po-jen, CHAO Tun-hao, LI Bo-yi. A scalable grouping random key pre-distribution scheme for large scale distributed sensor networks: proceedings of the 3rd International Conference on Information Technology and Applications[C]. [S. l.]: [s. n.], 2005.

[26] TASSOS D, IOANNIS K, LOCALIZED A. Distributed protocol for secure information exchange in sensor networks: proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS '05)[C]. [S. l.]: [s. n.], 2005.

[27] ZHU S, SETIA S, JAJODIA S. LEAP: efficient security mechanisms for large-scale distributed sensor networks: proceedings of the 10th ACM Conference on Computer and Communication Security[C]. Washington D C: [s. n.], 2003: 62-72.

[28] DANIEL A, BICKET J, SANJIT B. Link-level measurements from an 802.11b mesh network: SIGCOMM '04[C]. [S. l.]: [s. n.], 2004.

[29] CHAN Haowen, GLIGOR D V, PERRIG A, *et al*. On the distribution and revocation of cryptographic keys in sensor networks[J]. **IEEE Transactions on Dependable and Secure and Secure Computing**, 2005, **2**(3): 233-247.

[30] YANG Hao, LUO Haiyun, YE Fan, *et al*. Security in mobile Ad hoc networks: challenges and solutions[J]. **IEEE Wireless Communications**, 2004, **11**(1): 38-47.

[31] LAI B, KIM S, VERBAUWHEDE I. Scalable session key construction protocol for wireless sensor networks: IEEE Workshop on Large Scale Realtime and Embedded Systems[C]. [S. l.]: [s. n.], 2002.