软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(4):873−886 [doi: 10.3724/SP.J.1001.2013.04270]

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

传感器网络中基于随机混淆的组密钥管理机制*

曾玮妮[1], 林亚平[1], 余建平[2], 王 雷[3]

[1](湖南大学 信息科学与工程学院,湖南 长沙 410082)

[2](湖南师范大学 数学与计算机科学学院,湖南 长沙 410081)

[3](湘潭大学 信息工程学院,湖南 湘潭 411105)

通讯作者: 林亚平, E-mail: yplin@hnu.edu.cn

摘 要: 组密钥在传感器网络安全组通信及虚假数据过滤等安全服务中起着重要作用.针对节点可能被大量俘获这一安全威胁研究组密钥管理问题,提出了一种基于随机混淆技术的组密钥管理机制 GKRP(group key management scheme based on random perturbation).首先,提出了一种基站与网络协同的组密钥管理框架;然后,结合秘密共享技术和随机混淆技术构造了组密钥广播函数和局部协作等功能函数,以实现组密钥更新信息的广播传输和多个被俘获节点的撤销;最后,基于上述管理框架和函数,提出了机制 GKRP,使得节点间可以协作进行组密钥更新.理论分析及仿真结果表明,GKRP 在特定的参数设置下不受限于被俘获节点,且该参数易于满足.因此,GKRP 有效突破了门限值问题,提高了网络的抗毁性.同时,由于采取局部广播和全网络广播方式更新组密钥,GKRP 在通信上同样更为有效.GKRP 的存储和计算开销略高于已有同类机制,但仍然较低,适合于传感器网络.

关键词: 无线传感器网络;组密钥管理;节点俘获;秘密共享;随机混淆

中图法分类号: TP393 **文献标识码**: A

中文引用格式: 曾玮妮,林亚平,余建平,王雷.传感器网络中基于随机混淆的组密钥管理机制.软件学报,2013,24(4):873−886. http://www.jos.org.cn/1000-9825/4270.htm

英文引用格式: Zeng WN, Lin YP, Yu JP, Wang L. Group key management based on random perturbation in wireless sensor networks. Ruanjian Xuebao/Journal of Software, 2013,24(4):873−886 (in Chinese). http://www.jos.org.cn/1000-9825/4270.htm

Group Key Management Based on Random Perturbation in Wireless Sensor Networks

ZENG Wei-Ni[1], LIN Ya-Ping[1], YU Jian-Ping[2], WANG Lei[3]

[1](College of Information Science and Engineering, Hu'nan University, Changsha 410082, China)

[2](College of Mathematics and Computer Science, Hu'nan Normal University, Changsha 410081, China)

[3](College of Information Engineering, Xiantan University, Xiangtan 411105, China)

Corresponding author: LIN Ya-Ping, E-mail: yplin@hnu.edu.cn

Abstract: In sensor networks, a group key plays an important role in both secure group communication and some security services such as false date filtering. Considering the security threat that there may be plenty of compromised nodes, a new group key management scheme based on random perturbation and secret sharing techniques is proposed (GKRP for short). In the GKRP, base station and local networks manage group keys cooperatively; additionally, some functions such as the broadcast rekeying function and local collaboration function are constructed. Thus, with GKRP, even if there are plenty of compromised nodes, these nodes can be revoked in real-time to ensure group key security. Extensive analyses and simulations show that GKRP can provide a higher level of security because GKRP is not limited to the compromised nodes under certain conditions, which can be satisfied easily. Moreover, GKRP is also more efficient on

* 基金项目: 国家自然科学基金(60973031, 61173038, 60903168); 国家教育部博士点基金(20100161110025); 湖南省教育厅资助科研项目(10B062); 湖南师范大学青年优秀人才培养计划(ET51102)

收稿时间: 2010-11-19; 定稿时间: 2012-05-10

communication as taking local broadcast and network broadcast to rekey. The storage and computation overheads of GKRP are somewhat higher than some related works; however, they are still lightweight and thus are suitable to sensor networks.

Key words: wireless sensor network; group key management; node compromise; secret sharing; random data perturbation

无线传感器网络(wireless sensor networks,简称 WSNs)在军事和民用领域具有广泛应用,因此,对 WSNs 的研究是一个非常活跃的领域[1].部署于敌对及无人照看环境中的 WSNs 易于遭到各种安全攻击,组密钥能为安全组通信及其他安全服务(例如虚假数据过滤、安全数据聚合)提供基本的技术支持[2−4],具有广泛的应用.然而,组密钥等机密信息在传感器节点被俘获(node compromise)时面临被暴露的危险.一旦组密钥被暴露,将进一步影响到安全组通信及其他安全服务的有效性.为降低节点俘获所引发的负面影响,需要实时更新组密钥以撤销被俘获节点.因此,以组密钥更新为核心的组密钥管理是 WSNs 中一个十分有意义的研究课题.由于传感器节点不具备防篡改设备,易于遭到俘获;又由于传感器节点的资源有限特性,WSNs 中的组密钥管理不但要均衡各项系统开销,而且要考虑大量节点俘获所引发的串谋攻击问题[2],迎来了新的挑战.

WSNs 组密钥管理方面的研究已经取得了一些进展,已有的大部分工作利用了门限秘密共享技术[5−10].其中的典型工作包括 Zhang 等人基于局部节点协作提出的机制 B-PCGR[11]:各节点部署前预置相同的组密钥生成信息;部署后,随机生成秘密信息 E 以加密该信息,并将 E 分为 n 个份额(利用秘密共享技术),分别发送给 n 个邻居节点.各节点在获取了至少门限个邻居节点的关于 E 的秘密份额时,获取新的组密钥.然而,若敌方:(1) 俘获了门限个组密钥;或(2) 俘获了某个节点且俘获了该节点的门限个邻居节点,则能获取所有组密钥,即该组密钥管理系统将被攻破.因此,Zhang 等人针对这两大问题分别提出了增强机制 C-PCGR 和 RV-PCGR[11].

C-PCGR 不同于 B-PCGR 之处在于,其将数据混淆技术引入到了秘密信息 E 的分发中.然而,C-PCGR 虽然解决了组密钥暴露所引发的安全问题,却带来了新的问题:当任意节点 i 的某一个邻居发生故障或被俘获时,该节点将不能成功获取其组密钥.因而,C-PCGR 恶化了节点意外所引发的负面影响.此外,C-PCGR 有着比 B-PCGR 更高的存储及通信开销.RV-PCGR 不同于 B-PCGR 之处在于,各节点还将 E 的秘密份额发送给了其邻居节点以外的节点(邻居节点的邻居节点).这种方法的本质在于,通过增大门限秘密共享中门限值的取值来增强抗节点俘获的能力.也因此,与 B-PCGR 相比,RV-PCGR 的存储及通信开销均有所增加.

此外,Chadha 等人基于门限秘密的私有密钥分发技术(personal key share distribution)[12]提出了一种分布式的组密钥更新机制[5].李林春等人、彭清泉等人分别在私有密钥分发技术[12]中引入双向散列链技术,提出了集中式的组密钥管理机制以解决数据包丢失环境下的密钥修复[6,7].Li 等人则利用私有密钥分发技术和散列链技术提出了一种分布式的组密钥管理机制[8].我们在私有密钥分发技术的基础上构造了一系列功能函数,提出了基于分布式更新权限的组密钥管理机制[9].然而,这些机制的安全性均受限于门限值,即,如果被俘获节点数目超出了某个门限值,那么敌方通过串谋被俘获节点的秘密份额可以攻破该系统.虽然加大门限值的取值可以增大系统被攻破的难度,然而并不能从根本上解决这一问题,且将引发高的系统开销.节点的资源有限性限制了门限值的取值,这意味着 WSNs 不能一味地通过增大门限值去增强安全性,而应采取其他方法.

本文提出一种新的组密钥管理机制 GKRP,试图在保证组密钥更新实时性的同时,实现安全性不受限于门限值的组密钥管理机制.为达到这一目的,采取一种基站与网络协同的管理框架,即由基站和网络共同掌控组密钥更新信息,只有结合两者信息才能获取组密钥.在技术上,为了安全、有效地撤销被俘获节点,将随机混淆技术与秘密共享技术相结合,构造了一系列功能函数,具体如下:(1) 组密钥更新广播函数,用于基站分发所掌控的组密钥信息,并使得敌方无法通过窃听获取该信息,还可以撤销局部网络所不能撤销的被俘获节点;(2) 局部协作函数,用于局部网络协作获取组密钥的第 2 部分信息,且在特定参数下其安全性不受限于被俘获节点;(3) 簇间密钥函数,GKRP 利用簇间通信密钥实现安全的簇间广播通信,为了实时更新被俘获节点所具有的簇间通信密钥,且使得任意簇与其他簇间的簇间通信密钥的安全性不受其他簇中被俘获节点的影响,构造了簇间密钥函数.

理论分析表明,GKRP 在特定的参数设置下不受限于被俘获节点,且该参数易于满足.因此,GKRP 有效突破了门限值问题,提高了网络抗毁性.同时,采取局部广播和全网络广播的方式更新组密钥,使得 GKRP 在通信上同样更为有效;GKRP 的存储和计算开销略高于已有同类机制,但仍然较小,适合于 WSNs.

本文第 1 节给出网络模型和安全假设.第 2 节给出 GKRP 的机制框架,并定义 GKRP 所用到的技术构造.第 3 节是对 GKRP 的详细描述.第 4 节对 GKRP 的安全性进行分析和讨论.第 5 节对 GKRP 的系统开销进行理论分析和仿真实验,并与已有机制进行比较.最后,在第 6 节对全文进行小结.

1 系统模型

1.1 网络模型

考虑典型的 WSNs,即由大量低耦合传感器节点构成的自组织静态网络.低耦合的传感器节点类型如伯克利的 MICA 节点,这种节点通常配有 8MHz 的处理器、128KB 的 ROM、4KB 的 RAM.因此,节点资源虽然严格受限,但是拥有足够的空间用来存放数字节点的组密钥更新信息.所谓静态网络是指节点在部署后的短时间内可能进行位置微调,此后将不再改变其位置的网络.

由于非方形区域总可以分割成方形区域之和,设 WSNs 部署于方形区域,该区域分为多个相等的子区域;节点分子区域通过飞行器部署(即部署于同一子区域的节点通过飞行器一起投放),部署点为子区域中心.于是,一起部署的节点在部署后呈现出以部署点为中心的正态分布[10].图 1 显示了网络部署到 500m×500m 的方形区域(子区域正态分布),整个区域分为 5×5 个子区域,当标准方差σ_x=σ_y=20m 时,整个区域中节点分布的概率密度情况;图 2 则显示了子区域部署 100 个节点的实际部署效果图(子区域正态分布).可见,一起投放的节点在物理位置上彼此靠近.在对偶密钥研究领域,有研究人员正是利用了这一规律对节点进行密钥信息的预置,从而提高了对偶密钥管理的有效性[10].不失一般性,本文提出的 GKRP 同样基于这一规律预置节点的组密钥生成信息.设部署于同一子区域的节点形成一个簇(子区域也称为簇区域,后文不加以区分),每一簇按照轮换机制产生簇头.各节点通过已有机制进行时钟同步[13].

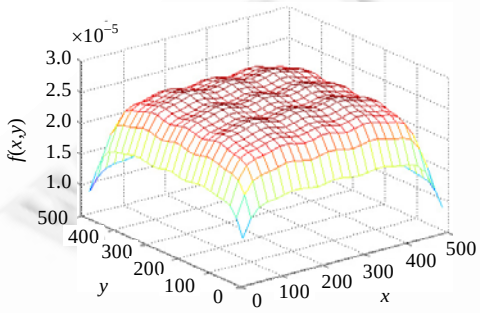

Fig.1 Probability density of the node deployment

图 1 节点概率密度分布图

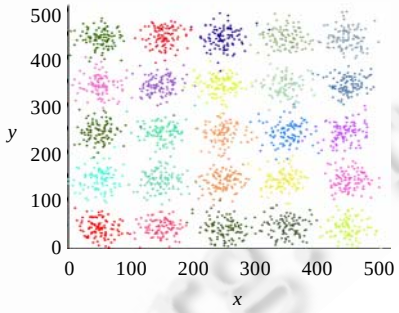

Fig.2 Real distribution of nodes

图 2 节点部署效果图

1.2 安全和威胁假设

假设 WSNs 是被部署在敌对环境中,敌方不仅可以窃听所有网络通信,还可以俘获部分节点并从中获取秘密信息.此外,敌方甚至可以串谋所俘获的所有节点.然而,基站总是安全的,节点可以实时认证基站发布的广播消息[16].各节点利用对偶密钥管理机制实现节点对间信息传输的机密性[14,15].此外,各簇的簇成员共享一个簇密钥以实现簇内共享信息的机密性保护;相邻簇间利用簇间密钥实现簇间通信的机密性保护.

由于敌方俘获节点需要一定的时间,而网络初始化的时间较短,与已有机制[5,11,14]相同,即假设在此期间节点是安全的.被俘获节点的检测和标识不是本文的研究内容,目前已有相应的研究成果[17],与已有机制[5,11,14]相同,我们假设:

(1) 被俘获节点总能被检测到,且未被俘获节点可信赖,也就是说,未被俘获的节点能够正确执行基站指令及预置算法;

(2) 敌方俘获新的节点需要一定的时间,在这个时间内足够进行组密钥更新操作.

2 机制框架及相关技术构造

将 WSNs 的整个生命周期划分为多个阶段(session),并记部署后首次进行的组密钥更新为第 1 轮更新,定义第(*j*–1)轮更新完成与第 *j* 轮更新完成之间的间隔为第 *j* 阶段.由于本文用到的符号较多,故将用到的符号统一归纳,见表 1.

Table 1 Some basic notations

表 1 符号定义

符号	含义	符号	含义
v_k, C_k, CH_k	依次代表 ID 为 k 的节点、簇及簇头	AC	认证中心
S_C	所有簇所构成的集合	$\{n_1^k,...,n_t^k\}$	簇 C_k 的局部认证数
S_{cC}	被俘获簇所构成的集合	$\{N_1^k,...,N_t^k\}$	簇 C_k 的全局认证数
RC_j	被俘获簇所构成的集合	$\{N_1^k,...,N_t^k\}$	组密钥更新阶段 j 的组密钥 GK
CRC	所有 RC 候选集所构成的集合	$K_{i,l}$	节点 v_i 与 v_l 共享的对偶密钥
NC_k	簇 C_k 的邻居簇所构成的集合	$\{M\}_k$	用消息 k 加密 M 后的密文
NNC_k	NC_k 中簇的邻居簇所构成的集合	S_{seed}	组密钥更新种子数集

2.1 机制框架

GKRP 采取基站与网络协同的管理模式,因此,相应地将组密钥生成信息分为两个部分:第 1 部分由基站负责发送,第 2 部分由节点协作获取.GKRP 中的组密钥更新框架如图 3 所示,当阶段(*j*–1)的组密钥更新完成后,基站即将其所掌控的阶段 *j* 的组密钥更新信息发送给整个网络.在阶段 *j*,一旦检测到节点被俘获,则该节点所在局部网络将发起组密钥更新.与此同时,被俘获节点所在簇及其邻居簇协作更新其所具有的簇间通信密钥.随后,组密钥更新中心 RC_j 中各簇协作获取 GK_j,并将 GK_j 分发给局部网络中的节点,即 RC_j 中各簇将 GK_j 分发给其所有邻居簇(通过簇间通信密钥),所有这些邻居簇再将 GK_j 转发给其他邻居簇(通过簇间通信密钥).本文随后几节将给出相关技术构造的详细定义和性质.

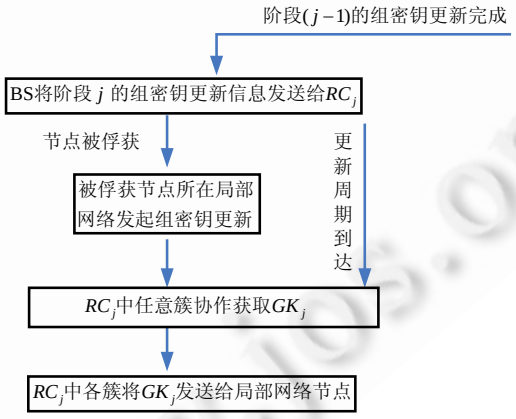

Fig.3 Flowchart of the group rekeying process

图 3 组密钥更新框架图

2.2 组密钥更新中心RC及认证中心AC

组密钥更新中心 RC(re-keying center)由多个簇构成,并负责更新组密钥.因此,组密钥更新所需的通信开销及时延是与 RC 中簇的构成相关的.如图 4 所示,如果 RC 由簇 C_1,C_2,C_3 及 C_4 担当,那么组密钥至少需要在簇间转发 3 轮、进行 8 次转发才能使所有的簇获取组密钥,且转发规则复杂;而如果 RC 由簇 C_1,C_4,C_{13} 及 C_{16} 担当,

那么簇间只需转发 2 轮、进行 4 次转发就能使所有的簇获取组密钥,且转发规则简单.因此,RC 中的簇不能随意构成.

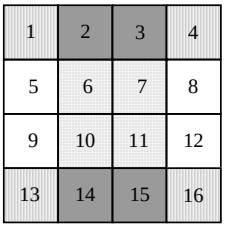

Fig.4 An example of candidates for rekeying center

图 4 RC 的候选集 CRC 的简单实例

记任意簇 C_k 的邻居簇所构成的集合为 NC_k,NC_k 中簇的邻居簇所构成的集合为 NNC_k,称 C_k,NC_k 和 NNC_k 中的簇构成了以 C_k 为中心的局部网络;整个网络可以划分为若干个由 3×3 的子区域构成的局部网络.为了实现较低的时延和开销,需要较少的转发轮数和次数.若选取各个局部网络的中心簇构成 RC,则可以实现最小的时延和开销.然而,为了均衡开销,RC 需由各簇轮流构成.记所有簇构成的集合为 S_C,将 S_C 划分为μ个集合作为 RC 候选集 CRC(candidates for rekeying center),由 CRC 中成员(记为$\{CRC_1,\ldots,CRC_\mu\}$)按照其 ID 轮流担当 RC,即 RC_j 由 $CRC_{j \bmod \mu}$担当.例如μ=4,更新阶段 j=9,则 RC_9 由 $CRC_{9 \bmod 4}=CRC_1$ 担当.因此,S_C 不能随意划分成 CRC.

我们的目标是:在各簇轮流构成 RC 的前提下,任意 RC 中的簇在获取组密钥后,簇间最多转发 2 轮,使得所有的簇获取组密钥.即:对于 CRC 中任意 CRC_i,满足:

(1) $\bigcup_{C_k\in CRC_i}(C_k\bigcup NC_k\bigcup NNC_k)=S_C$;

(2) 若去掉 CRC_i 中的任意一个元素,都不满足(1),即其任意真子集均不满足(1).

获取满足上述条件的 CRC 有多种方式,且不唯一,下面提供一种:将整个网络划分为多个 3×3 的子区域,即划分局部网络(不足 3×3 的边界区域,则与其左侧或上侧相邻局部网络中的子区域构成局部网络);以最左、最上的局部网络作为起始点,按照从左往右、由上往下的次序,依次从相邻局部网络中选取一个簇构成 CRC_i,选取原则为:如果相隔两个子区域的子区域没有被选取,则选取该子区域;否则,选择与之相邻的子区域.此外,在作为起始点的局部网络内部,同样按照从左往右、由上往下的次序,选取没有参与过构成 CRC_i 的子区域依次构成 CRC_i.例如,如图 4 所示,WSNs 所在的方形覆盖区域被划分为 4×4 个簇区域,S_C={1,…,16},则按照上述方法,S_C 被划分为 $CRC=\{CRC_1,\ldots,CRC_4\}$(各 CRC_i 的具体构成如图 4 所示),其中,属于相同 CRC_i 的簇用相同颜色或相同图案的方格表示.以 CRC_1 为例,有

$$\left(\bigcup_{C_k\in CRC_1} NC_k\right)\cup\left(\bigcup_{C_k\in CRC_1} NNC_k\right)=\{2,3,14,15,5,8,9,12\}\cup\{1,4,6,7,10,11,13,16\}=S_C.$$

当节点被俘获等异常情况发生时,被俘获节点所在簇的局部网络将发起组密钥更新.为了实现更新中的认证问题,基站从$\{CRC_1,\ldots,CRC_\mu\}$中选取某个 CRC_a 担当认证中心 AC(authentication center),记 AC 中的簇为$\{ac_1,ac_2,\ldots,ac_{|AC|}\}$.当任意 ac_q 所在的局部网络需要发起组密钥更新时,ac_q 将向整个网络提供更新的可靠性证明.如果某个簇 C_c 被俘获,且 $C_c\in CRC_i$,则基站将从 CRC_i 中删除 C_c,并在 CRC_i 中增加其他簇.

2.3 组密钥函数对

为了提高机制的抗毁性,即提高机制所能容忍的被俘获节点的数目,GKRP 采取基站与网络协同的管理模式.相应地,组密钥设计为只有结合基站分发的组密钥更新信息和局部协作生成的组密钥信息才能被获取.因此,构造有限域 $F(2^{L+l})$上的组密钥函数对如下(有限域 $F(2^{L+l})$上的加法操作为异或操作):

定义 1(组密钥函数对). 组密钥函数对 $GK(x,y)=(GK^1(x,y),GK^2(x,y))$,其中,$GK^1(x,y)$和 $GK^2(x,y)$为有限域

$F(2^{L+l})$上满足 $GK^1(x,y)+GK^2(x,y)=M(y)$的二元多项式(记变量 x 和 y 的次数分别为 d_x,d_y).任意阶段 j 的组密钥 GK_j 等于 $M(seed_j)$的高 L 位数据,其中,$seed_j$ 为这一阶段的密钥种子(见第 2.5 节).

组密钥函数对 $GK(x,y)$可以理解为 GK(簇 ID,阶段密钥种子),其中,$GK^1(x,y)$由基站掌控,包含 $GK^2(x,y)$的信息将预置在节点中.例如,在组密钥更新阶段 j,对于任意簇 C_k,其组密钥更新信息为 $GK^1(k,seed_j)$的高 L 位数据以及 $GK^2(k,seed_j)$的高 L 位数据.这意味着 C_k 只有获取 $GK^1(k,seed_j)$的高 L 位数据及 $GK^2(k,seed_j)$的高 L 位数据,才能获取 GK_j.

必须隐藏 $GK^1(x,y)$和 $GK^2(x,y)$,使得只有合法节点才能获取与之相关的信息.以下两节分别针对这两者展开讨论.

2.4 基站广播

基站掌控 $GK^1(x,y)$,并在阶段$(j-1)$的组密钥更新完成后,将阶段 j 的组密钥更新信息发送给 RC_j.若基站直接发送 $GK^1(k,seed_j)$,那么(d_y+1)个阶段后,$GK^1(x,y)$将会暴露.因此,在任意组密钥更新阶段 j,基站构造有限域 $F(2^{L+l})$上的组密钥更新函数 $B_j(x)$,用于分发下一阶段的组密钥更新信息.构造 $B_j(x)$的目的在于:

(1) 隐藏 $GK^1(k,seed_j)$,避免上述的 $GK^1(x,y)$暴露问题;

(2) 如果存在被俘获簇,使得被俘获簇不能获取 GK_j,而组密钥更新中心 RC_j 中的簇可以获取 GK_j.

定义 2(组密钥更新函数). 第 j 阶段的组密钥更新函数 $B_j(x)=GK^1(x,seed_j)+H_j(x)$,其中,$H_j(x)$为 $\lambda(\lambda\geq d_x)$次多项式,并满足:对于 $\forall C_k\in RC_j, H_j(k)\leq 2^l-1$;而对于 $\forall C_c\in S_{cC}, H_j(c)>2^l$.

记 $|RC_j|=r_j$(即 RC_j 的簇数目为 r_j),RC_j 中的簇 ID 集合为 $\{u_1,u_2,...,u_{r_j}\}$,$|S_{cC}|=r_c$,被俘获簇集合 S_{cC} 的簇 ID 集合为 $\{o_1,o_2,...,o_{r_c}\}$, 则 $H_j(x)$的求解可描述为如下规划问题:

Min: $\lambda(\lambda\geq d_x)$

约束条件:
$$\begin{cases} H_j(u_i)\leq 2^l-1 \\ H_j(o_i)\geq 2^l \end{cases}$$

首先给出引理 1[18]作为求解的理论基础,该引理给出了 n 元不定方程组有整数解的充要条件.

引理 1. 将 n 元不定方程组 $\begin{cases} a_{11}x_1+a_{12}x_2+...+a_{1n}x_n=d_1 \\ a_{21}x_1+a_{22}x_2+...+a_{2n}x_n=d_2 \\ ... \\ a_{m1}x_1+a_{m2}x_2+...+a_{mn}x_n=d_m \end{cases}$ $(n>m)$的系数元和常数项排成如下数表:

$$\begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} & d_1 \\ a_{21} & a_{22} & ... & a_{2n} & d_2 \\ ... & ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} & d_m \end{pmatrix}.$$

对该数表的所有行做行变换,对其前 n 列做列变换,可以变换为

$$\begin{pmatrix} c_1 & 0 & ... & 0 & 0 & ... & 0 & d_1 \\ 0 & c_2 & ... & 0 & 0 & ... & 0 & d_2 \\ ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & ... & 0 & c_m & 0 & ... & 0 & d_m \end{pmatrix},$$

则该方程组有整数解当且仅当 $c_1|d_1,\ldots,c_m|d_m$.

基于引理 1 中条件进行问题求解:

(1) 若 $r_j+r_c\leq d_x+1$,则对应于每个 u_i,随机生成满足引理 1 且小于 2^l-1 的数作为 $H_j(u_i)$;对应于 S_{cC} 中任意簇 o_i,随机生成满足引理 1 且大于 2^l-1 的数作为 $H_j(o_i)$.最后,通过联立方程组即可求得 $H_j(x)$;

(2) 若 $r_j+r_c>d_x+1$,选取 $\lambda'\geq d_x+1$,对应于每个 u_i,随机生成满足引理 1 且小于 2^l-1 的数作为 $H_j(u_i)$;对应于 $o_i(0\leq i\leq d_x-r_j)$,随机生成满足引理 1 且大于 2^l-1 的数作为 $H_j(o_i)$.通过联立不定方程组,可以求得解系

$$\begin{cases} x_1 = A_1 + \alpha_1^1 k_1 + ... + \alpha_{\lambda'-\omega}^1 k_{\lambda'-\omega} \\ x_2 = A_2 + \alpha_1^2 k_1 + ... + \alpha_{\lambda'-\omega}^2 k_{\lambda'-\omega} \\ ... \\ x_{\lambda'} = A_{\lambda'} + \alpha_1^{\lambda'} k_1 + ... + \alpha_{\lambda'-\omega}^{\lambda'} k_{\lambda'-\omega} \end{cases},$$

其中,$A_1,\ldots,A_{\lambda'}$以及 α_i^j 为常数,$\omega \geqslant d_x, k_1,\ldots,k_{\lambda'-\omega}$为任意整数[18].

通过变化 $k_1,\ldots,k_{\lambda'-\omega}$以及$\lambda'$的取值,寻找满足 $H_j(o_i) \geqslant 2^l$ 的 $H_j(x)$.

在数域 $F(2^{L+l})$中,大于 2^l 的数有 $2^l(2^L-1)$个,其他数为 2^l 个.当 $L \geqslant 1$ 时,即有 $2^l(2^L-1) \geqslant 2^l$.一般情况下,当 l 及 L 的取值大于 1 时,$2^l(2^L-1)$将远远大于 2^l.如,取定 l=10,L=10,则小于 2^l 的数为 1 024 个,而大于 2^l 的数有 1 047 552 个.因而,函数值 $H_j(o_i)$大于 2^l 的概率通常远远大于其小于 2^l 的概率.由于簇数目远远小于数域大小,被俘获簇的数目必然不大于簇数目,易于寻找到满足条件的 $H_j(x)$.

定义 3(组密钥更新广播). 阶段 j 的组密钥更新广播 $B_j = \{B_j(x), seed_j, \{rand_j, R_j\}_{GK_j}, MAC\}$,其中,$B_j(x)$为组密钥更新函数,$seed_j$ 为阶段 j 的组密钥更新种子(见第 2.5 节),$H(\cdot)$为密码学上安全的单向散列函数,$rand_j$ 为随机产生的长度为$(L+l)$位的数字,R_j 为 $H(rand_j)$随机的后 l_{rand} 位数字.

$\{rand_j, R_j\}_{GK_j}$ 用于节点检验所收到的组密钥 GK_j 的合法性:记各节点利用所收到的 GK_j 解密 $\{rand_j, R_j\}_{GK_j}$ 所获得的数据为 $\{rand_j', R_j'\}$,如果 $H(rand_j')$ 的后 $|R_j'|$ 位等同于 R_j',则视 GK_j 合法.

2.5 局部协作

包含 $GK^2(x,y)$的信息被预置在网络中.节点被俘获时,被俘获节点所在局部网络将发起组密钥更新,这需要解决 3 个子问题:

(1) 如何使得局部网络获取新的组密钥的第 2 部分,且能容忍节点被俘获;

(2) 如何使得节点得以检验由局部网络发起的组密钥更新请求的合法性;

(3) 局部网络中的各簇如何能够高效地交换新的组密钥.

接下来将围绕上述 3 个子问题的解决展开讨论.

对于问题(1),一种简单、直接的方法是选取满足 $g(x,y,0)=GK^2(x,y)$的函数 $g(x,y,z)$(记 $g(x,y,z)$中变量 z 的次数为 t),并在节点 $v_i(v_i \in C_k)$中预置份额 $g(c,y,i)$.此后,C_k 内节点根据$(i_1, g(k,s_j,i_1)),\ldots,(i_{t+1}, g(k,s_j,i_{t+1}))$,通过拉格朗日插值可以计算出 $g(c,s_j,z)$,进而获取 $g(c,s_j,0)=GK^2(c,s_j)$.然而,如果 C_k 中多于 t 个节点被俘获,敌方将能获取 $GK^2(c,y)$.同理,当敌方获取了多于 d_x 个 $GK^2(c,y)$份额时,必然能获取 $GK^2(x,y)$.此时,基站将丧失对被俘获簇的撤销能力,即组密钥管理系统将被攻破.可以将系统参数 d_x 设为不小于簇数目的值;然而,由组密钥更新函数 $B_j(x)$ 的构造可知,基站广播的通信开销随 d_x 的增长而线性增长.可见,如果采用上述方法,在高的安全性和低的通信开销之间将存在着矛盾.为解决这一矛盾,本文引入混淆函数集 F 及其对应的数集 S_{seed},其中,S_{seed} 是由 $F(2^{L+l})$中的元素所构成的集合;F 是由 $F(2^{L+l})$上多个 d_y 次多项式函数组成的函数集合,且满足:对于任意$\Delta g_i(y) \in F$ 以及 $seed_j \in S_{seed}$,$\Delta g_i(seed_j)$的高 L 位为 0[12].称数集 S_{seed} 为组密钥更新种子集,基于 F 及其对应的 S_{seed},构造局部协作函数如下:

定义 4(局部协作函数). 任意簇 C_k 的局部协作函数 $g_k(y,z)=g(k,y,z)+\Delta g_k(y)$,其中,$g(x,y,z)$中变量 z 的次数为 t 且满足 $g(x,y,0)=GK^2(x,y)$,$\Delta g_k(y) \in F$.对于任意节点 $v_i \in C_k$,其局部协作元为单变量多项式 $g_{k,i}(y)=g_k(y,i)$.

性质 1. 在任意阶段 j,如果 RC_j 中的簇 C_k 获取了 $g_k(seed_j,0)$和 $B_j(k)$,则必能获取 GK_j.

证明:C_k 根据 $g_k(seed_j,0)$可以获取 $GK^2(k,seed_j)$的高 L 位信息.此外,C_k 根据 $B_j(k)$可以获取 $GK^1(k,seed_j)$的高 L 位信息.因此,C_k 可以获取 $M(seed_j)$的高 L 位信息,即可获取 GK_j. □

为了解决问题(2),基于单向散列链(one way hash chain)构造全局认证函数及局部认证函数如下,其中,前者用于各簇向其所在的局部网络证明节点俘获攻击等异常情况的发生;后者用于 AC 中的各簇在节点俘获等异常情况发生时,向整个网络提供证明.

定义 5(认证函数). 簇 C_k 的局部认证函数 $a^k(x,y)$和全局认证函数 $A^k(x,y)$分别为满足 $a^k(i-1,0)=H(a^k(i,0))$

$(1\leqslant i\leqslant t)$和 $A^k(i-1,0)=H(A^k(i,0))(1\leqslant i\leqslant t)$的二元多项式,其中,

- $H(\cdot)$为密码学上安全的单向散列函数;
- x,y 的次数为 t.

记 $a^k(i-1,0)$为 n_{i-1}^k,$A^k(i-1,0)$为 N_{i-1}^k,称 $\{n_0^k,...,n_t^k\}$ 为 C_k 的局部认证数,$\{N_0^k,...,N_t^k\}$ 为 C_k 的全局认证数;$n^k(n^k=H(n_0^k))$ 和 $N^k(N^k=H(N_0^k))$ 分别为 C_k 的局部起始认证数和全局起始认证数.$\{N_0^k,...,N_t^k\}$ 在 C_k 是认证中心 AC 中成员时才被使用,且若 C_k 担当 ac_i,则初始化 N_i 为 N^k.

$a^k(x,y)$及 $A^k(x,y)$由基站负责生成,下面给出其生成算法:

认证函数产生算法.

Step 1. 基于 N_t^k,n_t^k 及单向散列函数 $H(\cdot)$,分别生成单向散列链 $\{N_t^k,N_{t-1}^k,...,N_0^k\}$ 及 $\{n_t^k,n_{t-1}^k,...,n_0^k\}$ 作为其全局认证数和局部认证数;

Step 2. 基于 $(w,A_k'(w)=N_w^k)$ 和 $(w,a_k'(w)=n_w^k)$ $(0\leqslant w\leqslant t)$分别插值获取 $A_k'(y)$ 和 $a_k'(y)$;

Step 3. 分别产生满足 $A_k(0,y)=A_k'(y),a^k(0,y)=a_k'(y)$ 的多项式函数 $A^k(x,y)$和 $a^k(x,y)$.

为了解决子问题(3),构造簇间密钥函数如下:

定义 6(簇间密钥函数). 簇 C_a 的簇间密钥函数 $F_a(y,z)=f(a,y,z)+\Delta f_a(z)$,其中,

(1) $f(x,y,z)=\sum_{i=0}^{i=t}\sum_{j=0}^{j=t}\sum_{k=0}^{k=t}f_{i,j,k}x^iy^jz^k$ 为任意满足 $f_{i,j,k}=f_{k,j,i}$ 的三元函数;

(2) $\Delta f_a(z)$为满足对于$\forall C_b\in NC_a,\Delta f_a(b)$的高 L 位为 0 的函数.

对函数$\Delta f_a(z)$的求解类似于对 $H_j(x)$求解过程中的情况 1(见第 2.4 节),这里不再赘述.簇 C_a 在阶段 j 的簇间密钥函数为 $F_a(j,z)$,与任意邻居簇 C_b 间的簇间密钥 $CK_{a,b}$ 为 $F_a(j,b)$的高 L 位数据.簇 C_a 中的任意节点 v_i 将预置簇间密钥元 $F_a(y,i),F_a(y,i)$用于支持 C_a 的簇间密钥函数的生成.

性质 2. 任意簇 C_a 根据 $F_a(j,z)$可获取与簇 C_b 之间的通信密钥 $CK_{a,b}$;任意簇 C_b 根据 $F_b(j,z)$可获取与簇 C_a 之间的 $CK_{b,a}$,则有 $CK_{a,b}=CK_{b,a}$.

证明:C_a 根据 $F_a(j,z)$可获取 $f(a,j,b)$的高 L 位信息;C_b 根据 $F_b(j,z)$可获取 $f(b,j,a)$的高 L 位信息.由于 $f_{i,j,k}=f_{k,j,i}$,有 $f(a,j,b)=f(b,j,a)$,则有 $f(a,j,b)$的高 L 位信息与 $f(b,j,a)$的高 L 位信息相等.得证. □

3 基于随机混淆的组密钥管理机制 GKRP

基于第 2 节给出的技术构造,利用节点的协作特性,我们提出一种适合于 WSNs 的组密钥管理机制 GKRP.GKRP 分为组密钥生成信息的预置和组密钥的更新两大部分.组密钥信息的预置在网络部署前完成.组密钥的更新则在投放后根据具体情况实施.为便于描述,以一组传感器节点为例进行描述.

3.1 预置组密钥生成信息

此阶段在网络部署前进行.首先,将网络部署区域划分为 m_c 个簇区域,并选取 RC 候选集 $CRC=\{CRC_1,\ldots,CRC_\mu\}$,选择其一作为认证中心 AC.随后,对于任意簇区域 C_k,生成:簇间密钥函数 $F_k(y,z)$;局部以及全局认证函数.最后生成:组密钥函数对$(GK^1(x,y),GK^2(x,y))$;混淆函数集 F 及密钥种子集 S_{seed}.

对于期望部署位置为子区域 C_k 的节点 v_i,预置:

(1) 网络唯一的节点标识 ID,散列函数 $H(\cdot)$和初始化组密钥 GK_0;

(2) 组密钥生成元 $g_{k,i}(y)=g_k(y,i)$、局部以及全局认证函数 $a^k(i,y)$及 $A^k(i,y)$、簇间密钥元 $F_k(y,i)$;

(3) CRC 和 AC 信息、全局认证数$\{N_i(1\leqslant i\leqslant|AC|)\}$(若 C_k 担当 ac_i,则 N_i 初始化为 N^k);

(4) $\{C_b,n^b,0\}$和$\{C_{b'},n^{b'},0\}$,其中,$b\in NC_k,b'\in NNC_k$.

3.2 组密钥更新阶段

以阶段 j 为例描述组密钥更新过程.假设 $v_m\in C_k$ 为被俘获节点,则簇 C_k 将发起组密钥更新.为便于描述,记

C_k 已使用的局部认证数为 n_d^k,C_k 的认证中心 ac_q 由 C_i 担当,并记 ac_q 已使用的全局认证数 N_q 为 $N_q=N_e^i$,组密钥的更新过程如下:

Step 1. C_k 生成局部认证数 n_{d+1}^k.

C_k 中任意节点 v_i 将其局部认证函数份额及簇间密钥函数份额 $\{v_i,\{a^k(i,d+1),F_k(j,i)\}_{K_{i,k}}\}$ 发送给 CH_k.CH_k 在获取了(t+1)个份额后,对这些份额进行拉格朗日插值计算,即可获取 $a^k(x,d+1)$及 $F_k(j,z)$.CH_k根据 $a^k(x,d+1)$获取其局部认证数 $n_d^k=a^k(0,d+1)$,并将 $\{C_k,n_{d+1}^k\}$ 发送给 ac_q 及其相邻簇.

C_k 的相邻簇将 $\{C_k,n_{d+1}^k\}$ 转发给其相邻簇节点.存储了 (k,n_d^k) 的任意节点 v_l 在收到 $\{C_k,n_{d+1}^k\}$ 后验证 $H(n_{d+1}^k)=n_d^k$ 是否成立:如果不成立,则抛弃这一数据;如果成立,则 v_l 存储 (k,n_{d+1}^k) 并删除 (k,n_d^k).

与此同时,CH_k通过对偶密钥将新的簇密钥 CK_k 发送给合法的簇内节点;根据 $F_k(j,z)$获取与各个相邻簇间新的簇间通信密钥,并利用 CK_k 将其加密广播给簇内节点.类似地,C_k 的各个相邻簇也进行簇内协作,以更新与 C_k 间的簇间通信密钥.

Step 2. ac_q 生成全局认证数.

如果 ac_q(ac_q由 C_i担当)中的节点 v_l验证 $H(n_{d+1}^k)=n_d^k$ 成立,则将其全局认证函数份额 $\{v_l,\{A^i(l,e+1)\}_{K_{l,i}}\}$ 发送给 CH_i.CH_i 在获取了(t+1)个份额后,对这些份额进行拉格朗日插值计算,获取 $A^i(x,e+1)$,并由此获取 $N_{e+1}^i=A^k(0,e+1)$.ac_q 新的全局认证数即为 N_{e+1}^i.

CH_i将 $\{q,N_{e+1}^i\}$ 广播给整个网络.任意节点 v_k 在收到 $\{q,N_{e+1}^i\}$ 后,验证 $H(N_{e+1}^i)=N_q$ 是否成立:如果不成立,则抛弃这一数据;否则,将存储的 N_q 替换为 N_{e+1}^i,转 Step 3.

Step 3. 局部网络生成并分发 GK_j.

如果簇 $C_l\in RC_j$,则节点 $v_k\in C_l$ 向 CH_l 发送组密钥更新份额 $\{v_k,\{g_{k,i}(s_j)\}_{K_{k,l}}\}$.$CH_l$ 在获取了(t+1)个份额后,通过插值计算获取 $g_l(s_j,x)$,进而得到 $g_l(s_j,0)$.CH_l 通过计算$(g_l(s_j,0)+B_j(l))$获得 GK_j,并将 $\{GK_j\}_{CK_l}$ 广播给簇内节点.此外,CH_l利用簇间密钥将 GK_j 加密发送给 NC_l中的簇,NC_l中的簇利用簇间密钥将 GK_j 加密转发给 NNC_l中的簇.

各节点利用收到的 GK_j 解密 $\{rand_j,R_j\}_{GK_j}$ 获得 $\{rand_j',R_j'\}$.如果 $H(rand_j')$ 的后 $|R_j'|$ 位与 R_j' 相等,则确定 GK_j 为有效;否则,抛弃收到的 GK_j.

Step 4. 准备下一阶段的组密钥更新:

基站将 $B_{j+1}=\{B_{j+1}(x),s_{j+1},\{r_{j+1},R_{j+1}\}_{GK_j},MAC\}$ 广播给整个网络.各节点通过 MAC 检验所收到信息的完整性.

4 安全性分析

4.1 安全性分析和比较

首先分析敌方攻破组 GKRP 的难度,即无论如何更新组密钥,敌方均能获取新的组密钥的难度.为便于描述,记 $GK^2(x,y)$为 $GK_0^2(x,y)$,记$(GK^2(x,y)+g_i(x))$为 $GK_i^2(x,y)$;$|F|$表示混淆函数集的大小,m_c 表示簇数目.以下定理证明了 GKRP 具有良好的抗节点俘获攻击能力.

定理 1. 敌方要想攻破组密钥管理系统,必须获取组密钥函数 $M(y)$或获取某个 $GK_i^2(x,y)$.

证明:GK_j 等于 $M(seed_j)$的高 L 位数据,敌方如果可以获取 $M(y)$,必然可以获取所有组密钥.

此外,如果敌方俘获了某个节点,由于该节点将被撤销,敌方并不能由此获取新的组密钥.即使敌方可以通过俘获簇 C_r 而获取某个 $GK_i^2(x,y)$ 中的一个份额 $GK_i^2(r,y)$,由于 $M(y)=GK^1(x,y)+GK^2(x,y)$,由 $B_j(x)$的构造可知,敌方如果不能获取 C_r 对应的组密钥更新信息的第 1 部分,必不能获取新的组密钥.基站总是安全的,这意味着敌方不能获取 $GK^1(x,y)$.于是,敌方必须获取某个 $GK_i^2(x,y)$,由此获取 RC 中某个簇对应的组密钥更新信息的第 2 部分,才能使基站针对俘获簇的撤销失效,从而攻破整个系统. □

定理 2. 如果敌方获取了(d_y+1)个组密钥,则敌方通过强力攻击获取 $M(y)$的概率为 $1/2^{(d_z+1)l}$.

证明:任意阶段 j 的组密钥 GK_j 等于 $M(seed_j)$的高 L 位数据,即使敌方获取了 GK_j,但其只能猜测 $M(seed_j)$的低 l 位数据,猜测的空间大小为 2^l.$M(y)$为(d_y+1)次多项式函数,因此,敌方通过强力攻击获取 $M(y)$的概率为 $1/2^{(d_z+1)l}$. □

例如,给定(d_z+1)=21,l=2.5L=80bits,则敌方通过强力攻击获取 $M(y)$的概率为 $1/2^{1806}$,这个概率基本上是可以忽略的.

定理 3. 如果 $d_x(|F|+1)\geqslant m_c$,则无论敌方俘获多少节点,敌方也不能获取任意 $GK_i^2(x,y)$.

证明:由于敌方俘获节点 $v_u\in C_k$后只能获取 $g_k(y,u)$,故其必须俘获簇 C_k中不少于(t+1)个节点才能获取 $g_k(y,z)$(即某个 $GK_i^2(k,y)$).而要想获取任意 $GK_i^2(x,y)$ ($0\leqslant i\leqslant|F|$),敌方必须获取(d_x+1)个类似于 $(k,GK_i^2(k,y))$ 的份额.如果 $d_x(|F|+1)\geqslant m_c$,则任意 $GK_i^2(x,y)$ ($0\leqslant i\leqslant|F|$)被使用的份额数必然小于(d_x+1),敌方必不能获取 $GK_i^2(x,y)$ ($0\leqslant i\leqslant|F|$). □

例如,网络部署于 1000×1000m^2 的监测区域,该区域分为 m_c=10×10 个簇区域,d_x 取值为 20,按照定理 3,如果 $|F|$=4,则无论敌方俘获多少个节点均不能攻破 GKRP.取定 L=10,l=2.5L,执行文献[10]中的算法,结果显示,当$|F|$=4 时,有$|S_{seed}|>2^{10}$.可见,GKRP 在抵抗节点串谋方面得到了有效增强,且可以支持的更新次数是合理的.当密钥长度 L 大于 10 时,类似于文献[10]中的做法,将多个短的密钥数据进行连接即可获取长的密钥数据.例如,将两个长度为 10 的密钥连接可以获取长为 20 的密钥.由于密钥的长度取决于所采用的密钥算法和部署环境等具体因素,本文的主要工作在于组密钥的管理,不对密钥长度进行更多探讨.在后面的开销分析中,用 L 表示密钥长.

定理 4. 敌方要想获取所有的簇间通信密钥,必须获取 $f(x,y,z)$,则必须俘获不少于(t+1)个簇.即使敌方俘获不少于(t+1)个簇,敌方通过强力攻击获取所有的簇间通信密钥的概率为 $1/2^{((t+1)l+(t-4)L)(t+1)}$.

证明:如果敌方俘获了一个簇 C_a,则其可以获取 $F_a(y,z)=f(a,y,z)+\Delta f_a(z)$,并由此获取任意 $f(a,j,b)$的高 L 位数据(其中,$b\in NC_a$).然而,敌方只能猜测 $f(a,j,b)$的低 l 位数据,猜测的空间大小为 2^l.对于任意 $f(a,j,c)$(其中,$c\notin NC_a$),敌方必须猜测 $f(a,j,c)$的(L+l)位数值,猜测的空间大小为 2^{L+l}.$f(a,j,z)$为(t+1)次多项式函数,因此,敌方通过强力攻击获取 $f(a,j,z)$的概率为 $1/2^{(t+1)l+(t-4)L}$.由于 $f(x,y,z)$中 x 的次数为 t,敌方只有获取了(t+1)个(a,$f(a,y,z)$)份额才能获取 $f(x,y,z)$.因此,即使敌方俘获了(t+1)个簇,但其通过强力攻击获取其他簇间的通信密钥的概率为 $1/2^{((t+1)l+(t-4)L)(t+1)}$.定理 4 得证. □

例如,给定(t+1)=21,l=2.5L=80bits,则敌方通过强力攻击获取 $f(x,y,z)$的概率为 $1/2^{46704}$,这个概率基本上是可以忽略的.可见,即使敌方俘获了一个簇,也不会影响到其他簇间的安全通信.

节点的被俘获,特别是多个节点的被俘获,是 WSNs 安全所面临的巨大威胁.在 B-PCGR 中,如果某个节点及其 t 个邻居节点被俘获,那么该组密钥管理机制将被攻破.在 RV-PCGR 中,如果某个节点的 t 个邻居节点被俘获,且这些邻居节点的 t 个邻居节点也被俘获,那么该组密钥管理机制将被攻破.由于节点间共享多个邻居节点,本质上,C-PCGR 所能容忍的被俘获节点数目将远远小于 t^2.在 DRA 中,如果某个阶段的被俘获节点数目多于 t 个,那么该组密钥管理机制将被攻破.对于本文引言中提到的其他基于秘密共享的组密钥管理机制,同样面临着这一 t 门限问题.而对于 GKRP,定理 1~定理 4 证明,它可以更好地对抗节点俘获攻击.

此外,敌方还可能发起以下两种攻击:

(1) 利用被俘获节点发起组密钥更新;

(2) 利用被俘获节点篡改认证数、基站广播等组密钥更新消息包.

对于攻击(1),GKRP 可以很好地对抗.因为 GKRP 中任何被俘获的节点都不能获取新的认证数,从而不能成功发起组密钥更新.此外,该节点发出的更新请求在局部范围内将被抛弃,因而对整个网络没有影响.即使攻击者俘获了一个簇,最坏的情况就是该簇没有被检测到被俘获,此时攻击者最多能发起 t 次更新,之后,该簇将被视为被俘获簇;否则,如果该簇被检测为被俘获簇,所有合法簇将忽略该簇的认证数及其发起的更新.

对于攻击(2),如果被俘获节点篡改了认证数,合法节点经过散列运算即可检测到该篡改,并抛弃该消息包.如果被俘获节点篡改基站发出的广播包,合法节点通过 MAC 码同样可以实现检测.如果被俘获节点篡改组密

钥更新信息包,合法节点通过解密源自于基站的组密钥广播包即可实现检验.因此,被俘获节点通过篡改消息包对组密钥管理系统进行的所有攻击均是无效的.

4.2 相关讨论

由于组密钥更新种子集合 S_{seed} 为有限集合,当大量节点被俘获时,在最坏情况下,可能 S_{seed} 中的种子会被耗尽.对于这个问题,由于 $g(x,y,z)$的安全性可以保证(见定理 1),可以通过产生多个满足条件的(F,S_{seed})来解决.不妨对所产生的多个(F,S_{seed})进行编号,并记编号为 i 的(F,S_{seed})为 (F^i,S^i_{seed}),记 F^i 中函数$\Delta g_k(y)$为 $(\Delta g_k(y))_{F^i}$.如果某个 S^i_{seed} 中的种子耗尽,则基站将广播 $\{(\Delta g_k(y))_{F^i}+\Delta g_{k+1}(y)_{F^{i+1}}\}$.对于任意节点 v_i,设其组密钥生成元 $g_{k,i}(y)$基于 $(\Delta g_k(y))_{F^i}$ 生成,则 v_i 更新 $g_{k,i}(y)$为 $g_{k,i}(y)+(\Delta g_k(y))_{F^i}+\Delta g_{k+1}(y)_{F^{i+1}}$.此后,基站即可利用 S^{i+1}_{seed} 中的种子进行组密钥的更新.

对于被俘获簇存在合法节点不能协作更新这一问题,值得注意的是,由于彼此靠近的节点易于被同时俘获,在某个合法节点所在簇的成员被大量俘获的情况下,通常难以判断该合法节点是否被俘获.如果其邻居簇视该区域的所有节点为被俘获节点,路由等相关的通信行为绕开该簇进行,不仅更为安全,而且可以避免引发相关的开销.如果某个被俘获簇中的合法节点基于相关信任策略被其邻居节点视为可信节点,则可以加入其邻居节点所在簇,并获取新的组密钥.信任机制的研究不是本文的研究内容,这里不再深入探讨.

5 开销评估

本节从存储、计算以及通信这 3 个方面分析 GKRP 的系统开销,并与同类分布式机制 B-PCGR 和 DRA 进行比较.Zhang 等人基于秘密共享技术提出了分布式机制 B-PCGR,并针对节点俘获问题提出了增强机制 RV-PCGR,由于 RV-PCGR 的系统开销高于 B-PCGR,本节仅与 B-PCGR 的开销进行比较.为便于分析和比较,记整个网络的节点数为 N,RC_j 大小为 r_j,簇数目为 m_c,广播消息包抵达整个组所需的转发次数为 r,簇内平均通信跳数为 h,密钥长度为 L 位.不失一般性,将共享份额的门限值 t 设定为簇大小的一半.如下文所分析和比较,GKRP 的存储开销和计算开销高于 DRA,低于 B-PCGR;然而,其在通信上更为有效.

5.1 存储开销

GKRP 中节点需要存储局部协作函数元、全局和局部认证函数、局部认证数和全局认证数、簇间密钥元,故每个节点的存储开销为$[(d_y+t+2)(L+l)+2(t+5+(m_c/4))L]$bits.DRA 的存储开销为 $12L$bits;B-PCGR 中各节点的存储开销为 $n(t+1)L$bits.因而,虽然 GKRP 的存储开销高于 DRA,但仍然适合于传感器节点.下面给出部分典型网络参数下,GKRP 及 B-PCGR 存储开销的具体数据实例(取 d_y=10,并取 l=2.5L).

(1) 设部署区域为 600×600m^2,相应簇数目 m_c 为 36(认证中心 AC 含有 8 个簇),簇大小为 30(t=15),则 GKRP 和 B-PCGR 的存储开销分别为 18.8L 字节和 60L 字节;

(2) 设部署区域为 1000×1000m^2,相应簇数目 m_c 为 100(认证中心 AC 含有 16 个簇),簇大小为 30(t=15),则 GKRP 和 B-PCGR 的存储开销分别为 20.8L 字节和 60L 字节;

(3) 设部署区域为 1000×1000m^2,相应簇数目 m_c 为 100(认证中心 AC 含有 16 个簇),簇大小为 20(t=10),则 GKRP 和 B-PCGR 的存储开销分别为 15.3L 字节和 27.5L 字节.

可见,在典型的网络参数设置下,GKRP 的存储开销低于 B-PCGR.当网络覆盖区域的大小及门限值分别发生变化时,GKRP 的存储开销随之变化得并不敏感.此外,不难发现,即使部署于 1000×1000m^2 的区域,t=15,GKRP 的存储开销也适合于传感器节点.因此,GKRP 的存储开销是适合于传感器节点的.

5.2 计算开销

GKRP 的计算开销主要源于以下 4 个部分:

(1) 被俘获节点所在簇及其邻居簇更新簇间通信密钥;

(2) RC_j 中节点协作获取 GK_j;

(3) 节点解密收到的消息包获取 GK_j;

(4) 被俘获节点所在簇发起组密钥更新.

因此,整个网络所需的计算开销为$[(t+1)(6+r_j)+6N/2t]$次加密/解密、有限域 $F(2^{L+l})$上复杂度为 $O(t^2)$的乘/除运算以及 N 次散列运算.DRA 的计算开销主要为有限域 $F(q)$上复杂度为 $O(t^2)$的乘/除运算;B-PCGR 的计算开销主要为$(t+1)N$ 次加密/解密、有限域 $F(q)$上复杂度为 $O(t^2)$的乘/除运算.因而,GKRP 的计算开销低于 B-PCGR,高于 DRA;但其计算开销仍然较小,适合于传感器节点.

5.3 通信开销

GKRP 组密钥更新的通信开销主要源于以下 5 个部分:

(1) 基站广播 B_j 所需的通信开销为$(d_x+5)(L+l)r$bits;

(2) RC_j 中各簇协作获取 GK_j 并发送给局部网络,所需通信开销最高为$[n_a(t+1)h+m_c(h+4)](L+l)$bits;

(3) 被俘获节点所在簇 C_k 对 CK_k 进行更新,并产生新的认证数,所需的通信开销最高为 $4thL$bits;

(4) 被俘获节点所在簇及其邻居簇更新簇间通信密钥,所需通信开销为 $5h(t+1)(L+l)$bits;

(5) 担当认证中心的簇产生认证数并广播给整个网络,所需的通信开销为$[(t+1)h+r]L$bits.

GKRP 总的通信开销为上述 5 部分之和.

B-PCGR 的通信开销为 $2tNL$bits,DRA 的通信开销为$[(19t/2)+8]rL$bits.

从以上分析可以看出,GKPR,B-PCGR 及 DRA 的通信开销均与网络密度和区域大小相关.为研究网络密度、区域大小变化对三者的影响,设计如下仿真实验:基站位于区域角落,节点通信半径为 50m,整个网络分为 $100\times100\text{m}^2$ 的多个簇单元.由于网络通过飞行器部署,设各簇节点服从标准方差为$\sigma_x=\sigma_y=20$ 的二维高斯分布.实验分两组:(1) 部署区域固定为 $600\times600\text{m}^2$,节点数在 1 000~2 200 之间变化.因此,共有 36 个簇,每个簇的节点数在 28~60 之间变化;最大的更新中心 RC 包含 8 个簇,最小的包含 4 个簇;(2) 每个簇的大小固定为 40,部署区域在 $600\times600\text{m}^2$~$1000\times1000\text{m}^2$ 之间变化,相应的节点数在 1 400~4 000 之间变化.当部署区域为 $1000\times1000\text{m}^2$ 时,相应的簇数目为 100,其密钥更新中心含有 16 个簇.取 $l=2.5L$,$d_x=20$,CRC 中成员轮流担当 RC,簇头随机选取,最后的更新开销为平均值.

图 5 给出了 GKRP,B-PCGR 和 DRA 在不同实验条件下通信开销的变化情况.由图 5 可以看出,GKRP 的通信开销低于 B-PCGR 及 DRA.这是由于 B-PCGR 采取单播方式传送更新信息,DRA 中广播更新的数据包较大.GKRP 的通信开销由组密钥更新广播及局部节点协作引发,组密钥更新广播的开销由于混淆技术的采用得到了有效控制.此外,各簇内节点共享簇密钥,簇间共享簇间通信密钥,因而局部网络更新组密钥的开销也得到了有效控制.

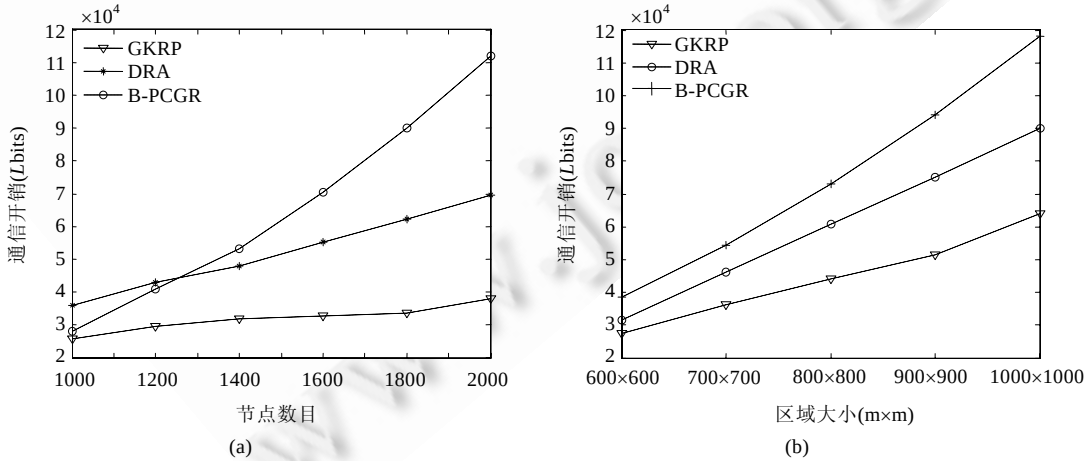

Fig.5 Communication overheads of GKRP, DRA and B-PCGR schemes

图 5 GKRP,DRA 及 B-PCGR 的通信开销比较

图5(a)显示了网络覆盖区域固定而节点密度变化时,GKRP,B-PCGR和DRA通信开销的变化情况.从图5(a)可以看出,GKRP 的通信开销随密度的增加变化不大,其随节点密度增加而增大的幅度要小于后两者.这是由于,GKRP 的通信开销主要源于基站发送的组密钥更新信息,而区域固定时,即使节点密度增加,基站广播的通信开销基本上相同.而 B-PCGR 和 DRA 中消息包的大小随系统参数 t 的增长而增长,t 随节点密度增长.图 5(b)显示了节点密度固定而网络覆盖区域变化时,GKRP,B-PCGR 和 DRA 通信开销的变化情况.从图 5(a)可以看出,三者的通信开销随区域的增长基本上呈线性增长,然而 GKRP 的通信开销随区域增长而增长的幅度小于后两者.这是由于,GKRP 的组密钥更新广播信息随区域的增长而增长得缓慢,且 B-PCGR 和 DRA 在单位区域内的通信开销均高于 GKRP 局部协作所需的通信开销.

6 结 论

本文提出了一种适用于 WSNs 的组密钥管理机制 GKRP,GKRP 具有以下特点:

(1) 能对被俘获节点做出实时反应,对组密钥进行实时更新;

(2) 通过将随机混淆技术引入到门限秘密共享思想的多项式技术中,巧妙地构造了组密钥更新函数以及局部协作函数,与已有基于秘密共享的组密钥管理机制相比,不受门限值的限制,提高了安全性;

(3) 与同类基于秘密共享的典型分布式机制 B-PCGR 和 DRA 相比,由于 GKRP 采取明文广播方式进行更新信息的发送,且通过引入混淆技术降低了更新信息的数据量,而 B-PCGR 采取单播方式进行更新信息的传送;DRA 的更新数据包数量较大,GKRP 的通信开销与 B-PCGR 以及 DRA 相比均有所降低.虽然 GKRP 在存储以及计算方面的开销高于 DRA,但依然较小,因而 GKRP 更适合于 WSNs.

References:

[1] Chan HW, Perrig A. Security and privacy in sensor networks. IEEE Computer, 2003,36(10):103−105. [doi: 10.1109/MC.2003.1236475]

[2] Li P, Lin YP, Zeng WN. Search on security in sensor networks. Ruanjian Xuebao/Journal of Software, 2006,17(12):2577−2588 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/2577.htm [doi: 10.1360/jos172577]

[3] Ye F, Luo HY, Lu SW, Zhang LX. Statistical en-route filtering of injected false data in sensor networks. IEEE Journal on Selected Areas in Communications, 2005,23(4):839−850. [doi: 10.1109/JSAC.2005.843561]

[4] Castelluccia C, Mykletun E, Tsudik G. Efficient aggregation of encrypted data in wireless sensor networks. In: Proc. of the MobiQuitous 2005. Los Alamitos: IEEE Computer Society, 2005. 109−117. http://www.ics.uci.edu/~gts/paps/mobiq-2005.pdf [doi: 10.1109/MOBIQUITOUS.2005.25]

[5] Chadha A, Liu YH, Das SK. Group key distribution via local collaboration in wireless sensor networks. In: Proc. of the 2005 2nd Annual IEEE Communications Society Conf. on Sensor and Ad Hoc Communications and Networks (SECON 2005). Santa Clara: Institute of Electrical and Electronics Engineers Computer Society, 2005. 46−54. [doi: 10.1109/SAHCN.2005.1556863]

[6] Li LC, Li JH, Pan J. Self-Healing group key management scheme with revocation capability for wireless sensor networks. Journal on Communicaitons, 2009,30(12):12−17 (in Chinese with English abstract).

[7] Peng QQ, Pei QQ, MA JF, Pang LJ. A self-healing group key management scheme in wireless sensor networks. Acta Electronica Sinica, 2010,38(1):123−128 (in Chinese with English abstract).

[8] Li H, Chen KF, Zheng YF, Wen M. A locally group key management with revocation and self-healing capability for sensor networks. In: Proc. of the 2nd Int'l Conf. on Systems and Networks Communications (ICSNC 2006). Piscataway: Institute of Electrical and Electronics Engineers Computer Society, 2006. 29. [doi: 10.1109/ICSNC.2006.3]

[9] Zeng WN, Lin YP, Hu YP, Yi YQ, Li XL. A group key management scheme based on distributed rekeying authority in sensor networks. Journal of Computer Research and Developmeng, 2007,44(4):606−614 (in Chinese with English abstract). [doi: 10.1360/crad20070409]

[10] Du WL, 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 2004. Piscataway: IEEE Press, 2004. 586−597. [doi: 10.1109/INFCOM.2004.1354530]

[11] Zhang WS, Cao GH. Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach. In: Proc. of the IEEE INFOCOM 2005. Piscataway: IEEE Press, 2005. 503−514. [doi: 10.1109/INFCOM.2005.1497918]

[12] Liu DG, Ning P, Sun K. Efficient self-healing group key distribution with revocation capability. In: Proc. of the ACM Conf. on Computer and Communications Security. Washington: Association for Computing Machinery, 2003. 231−240. [doi: 10.1145/948109.948141]

[13] Greunen J, Rabaey J. Lightweight time synchronization for sensor networks. In: Proc. of the 2nd ACM Int'l Workshop on Wireless Sensor Networks and Applications (WSNA 2003). Association for Computing Machinery, 2003. 11−19. [doi: 10.1145/941350.941353]

[14] Zhu SC, Satia S, Jajodia S. LEAP: Effcient security mechanisms for large-scale distributed sensor networks. In: Proc. of the ACM Conf. on Computer and Communications Security. Washington: Association for Computing Machinery, 2003. 62−72. [doi: 10.1145/948109.948120]

[15] Zhang WS, Tran M, Zhu SC, Cao GH. A random perturbation-based scheme for pairwise key establishment in sensor networks. In: Proc. of the Int'l Symp. on Mobile Ad Hoc Networking and Computing ACM (MobiHoc). New York: Association for Computing Machinery, 2007. 90–99. [doi: 10.1145/1288107.1288120]

[16] Zhang WS, Subramanian N, Wang GL. Lightweight and compromise-resilient message authentication in sensor networks. In: Proc. of the IEEE INFOCOM 2008. Piscataway: IEEE Press, 2008. 1418−1426. [doi: 10.1109/INFOCOM.2008.200]

[17] Wang GL, Zhang WS, Cao GH, Porta TL. On supporting distributed collaboration in sensor networks. In: Proc. of the 2003 IEEE Military Communications Conf. (MILCOM 2003). IEEE Press, 2003. 752−757. [doi: 10.1109/MILCOM.2003.1290206]

[18] 王丽萍,魏炜.*n* 元一次不定方程组的整数解.数学通报,2003,5:41−42.

附中文参考文献:

[2] 李平,林亚平,曾玮妮.传感器网络安全研究.软件学报,2006,17(12):2577−2588. http://www.jos.org.cn/1000-9825/17/2577.htm [doi: 10.1360/jos172577]

[6] 李林春,李建华,潘军.无线传感器网络中具有撤销功能的自愈组密钥管理方案.通信学报,2009,30(12):12−17.

[7] 彭清泉,裴庆祺,马建峰,庞辽军.无线传感器网络中自治愈的群组密钥管理方案.电子学报,2010,38(1):123−128.

[9] 曾玮妮,林亚平,胡玉鹏,易叶青,李小龙.传感器网络中一种基于分布式更新权限的组密钥管理方案.计算机研究与发展,2007,44(4):606−614. [doi: 10.1360/crad20070409]

[18] 王丽萍,魏炜.*n* 元一次不定方程组的整数解.数学通报,2003,5:41−42.

曾玮妮(1982－),女,湖南邵阳人,博士,高级工程师,CCF 会员,主要研究领域为传感器网络.
E-mail: viol_v@hotmail.com

余建平(1979－),男,博士,副教授,CCF 会员,主要研究领域为传感器网络.
E-mail: jianpinghn@163.com

林亚平(1955－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为通信网络,机器学习.
E-mail: yplin@hnu.edu.cn

王雷(1973－),男,博士,教授,CCF 会员,主要研究领域为通信网络.
E-mail: phd.leiwang@gmail.com