ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.3, March 2010, pp.516−527
doi: 10.3724/SP.J.1001.2010.03457

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

基于时间部署的无线传感器网络密钥管理方案*

袁 珽+, 马建庆, 钟亦平, 张世永

(复旦大学 计算机科学技术学院,上海 200433)

Key Management Scheme Using Time-Based Deployment for Wireless Sensor Networks

YUAN Ting+, MA Jian-Qing, ZHONG Yi-Ping, ZHANG Shi-Yong

(School of Computer Science, Fudan University, Shanghai 200433, China)

+ Corresponding author: E-mail: iamyuanting@hotmail.com

Yuan T, Ma JQ, Zhong YP, Zhang SY. Key management scheme using time-based deployment for wireless sensor networks. *Journal of Software*, 2010,21(3):516−527. http://www.jos.org.cn/1000-9825/3457.htm

Abstract: This paper proposes a key management scheme using time-based deployment for wireless sensor networks, which is characterized by a special two-tier random key pre-distribution and elimination mechanism as well as a time-based group deployment method. Each sensor node randomly chooses keys from multiple key pools and deletes related keys when certain conditions are satisfied; All the sensor nodes are organized into deployment groups and are chronologically deployed into the network. Compared with classical key management schemes for wireless sensor networks, The proposed scheme increases node resource efficiency and enhances network resilience against node compromise while ensuring a relatively high node connectivity for pair-wise key generation.

Key words: wireless sensor network; network security; key management; random key predistribution; time-based deployment

摘 要: 提出一种基于时间部署的随机密钥管理方案.该方案采用了特殊的两级随机密钥预分配和清除机制以及按时间顺序的成组部署方法:每个传感器节点从多个密钥池中随机选择密钥并在一定条件下删除相关的密钥;所有传感器节点被组织成部署组并按时间顺序被部署到网络中.与经典的随机密钥管理方案相比,该方案在为成对密钥的生成提供了较高的节点连通度的同时,提高了节点资源利用率并且增强了网络抵抗节点受损攻击的能力.

关键词: 无线传感器网络;网络安全;密钥管理;随机密钥预分配;基于时间部署

中图法分类号: TP309 **文献标识码**: A

无线传感器网络(wireless sensor networks,简称 WSNs)被认为在不久的将来会广泛地应用于完成传统意义上具有挑战性的任务,例如实时交通监控,异常气候条件追踪以及军事传感和跟踪等[1].在这些应用中,组成 WSN 网络的节点可能为了完成某一特定的任务而需要与其他节点相互通信来交换信息,此时信息的安全性就是一个需要被关注的问题.特别地,如果 WSN 网络被部署在不安全的环境中,它更容易受到诸如通信监听、节点捕获和破坏等威胁时,如何使整个网络遭受的破坏最小并能继续执行规定的任务更是一个需要优先考虑的重要问题.为此,节点之间可能发生的通信必须通过密钥以及相应的密钥管理方案加以保护,而密钥管理方案也同

* Supported by the National Natural Science Foundation of China under Grant No.60672113 (国家自然科学基金)
Received 2008-03-18; Revised 2008-07-08; Accepted 2008-08-28

时构成了 WSN 网络的安全基础架构,为诸如安全路由,安全数据聚合以及安全定位等方案提供了实现的安全基础[2].

WSN 网络的安全部署给密钥管理带来了不同于传统有线网络以及某些类型的无线网络的特殊难点.这些难点主要体现在如下几个方面:(1) WSN 节点的物理资源非常有限,这些资源包括电力资源、计算资源、通信资源和存储资源等,分别表示为节点的在线时间、运算速度、通信带宽和距离以及数据存储容量等,例如目前被广泛应用的 MICA 系列 WSN 节点[3];(2) WSN 网络可能没有固定的基础设施来协助实现密钥管理方案,原因可能是依赖于基础设施实现的中心化的密钥管理方案更容易由于基础设施的单点失败(single point failure)而使整个方案无效化;(3) WSN 节点趋向于低成本的设计使其更容易遭到攻击者的物理破坏.对单个 WSN 节点设计成本的约束使得任何保护内部数据的防篡改硬件(tamper-resistant hardware)都无法被集成.攻击者可以很容易地破坏 WSN 节点并对其中的数据进行未授权的操作,从而影响了 WSN 网络任务的正常执行.基于以上几个方面,许多在传统意义上可行的密钥管理方案或协议[4−6]都无法很好地应用于 WSN 网络中.

由于基于非对称密码学(asymmetric cryptography)理论的 Diffie-Hellman[4]和 RSA[5]以及基于在线密钥分发中心(key distribution center,简称 KDC)的 Kerberos[6]都无法适用 WSN 网络,基于对称密码学(symmetric cryptography)的密钥管理方案成为了当前研究的重点.至今,大量研究已经表明,对称密钥管理方案以其简单高效的特点更加符合未来 WSN 网络的安全应用[7].WSN 网络对称密钥管理的核心是密钥预分配(key pre-distribution),其基本实现过程为在网络部署前预先给每一个节点分配一定数量的密钥信息,部署后任何两个需要安全通信的节点使用各自的密钥信息创建出一个共享的成对密钥(pair-wise key)来保护未来产生的通信量.

在此背景下,本文提出了一种适用于大规模 WSN 网络的密钥管理方案,该方案假设考虑的 WSN 网络具有有限的应用周期并且在该周期内网络经历的节点部署事件次数满足一定的阈值约束.该方案使用的密钥预分配方法使得网络抵抗节点受损攻击的能力(resilience against node compromise)与攻击发生的时间相关联,攻击发生的时间越晚,网络抵抗节点受损攻击的能力越强.该方案的主要贡献在于:(1) 提出了一种有效解决大规模节点受损攻击耗尽预分配密钥空间资源的方法;(2) 网络抵抗节点受损攻击的能力随着攻击发生的时间呈增强的趋势;(3) 相比某些已知的密钥管理方案,提供了在高节点连通度下更强的抵抗节点受损攻击的能力.

本文第 1 节介绍无线传感器网络密钥管理研究的相关工作.第 2 节描述我们的方案的系统模型.第 3 节叙述方案的密钥管理过程.第 4 节对方案从节点连通度和抵抗节点受损攻击的能力方面进行分析并对系统模型中相关参数的假设进行讨论.第 5 节总结全文并简述我们今后的工作.

1 相关工作

Eschenauer 和 Gligor 首次提出了基于随机密钥预分配的密钥管理方案[8](本文称为 E-G 方案).在该方案中,每个 WSN 节点都从一个全局的密钥池中随机地预分配一定数量的管理密钥,这些管理密钥构成了每个节点的密钥环,两个需要安全通信的节点通过识别各自密钥环与对方密钥环的公共部分来确定这两个节点的共享密钥集,并从该共享密钥集中选择一个密钥作为会话密钥.通过合理地设置密钥池和密钥环的大小,该方案在 WSN 节点数量足够多的条件下使得任何两个节点之间能够进行安全通信的概率几乎为 1.Chan 提出了 q-composite 方案[9],在 E-G 方案的基础上限制了两节点共享密钥集的大小不得小于 q,并且使用共享密钥集中的所有密钥共同产生一个会话密钥,该方案被证明其抵抗小规模节点受损攻击的能力要强于 E-G 方案.

基于 E-G 方案的随机密钥预分配思想,Du 提出了多 Blom 空间[11]随机密钥管理方案[10].每个 WSN 节点随机地从全局 Blom 空间池中选择固定数量的 Blom 空间并从中分配不同的密钥信息,任何两个共享相同 Blom 空间的节点都可以建立安全通信.Liu 一般化了 Du 的方案,提出了多二元对称多项式随机密钥管理方案[12],用二元对称多项式[13]来代替 Blom 空间并获得了与后者类似的理论和实验结果.这两种方案的缺点在于分别涉及到了矩阵和多项式的运算,在会话密钥协商中较多地消耗了有限的计算资源.

同样基于 E-G 方案,一些利用 WSN 节点部署知识的密钥管理方案被提出.Liu 首先提出了 CPKS 方案[14],

任何两个在部署后预计会成为邻居的节点被预先分配了成对密钥,部署后只要交换节点标识就可以确定它们是否成为了实际的邻居.在同一文献中,Liu 又提出了使用二元对称多项式的改进方案[14],他将节点部署区域划分成了若干矩形子区域,每个子区域对应一个二元对称多项式,预计被部署在某个子区域内的节点将同时拥有包含其所在子区域在内的其相邻的上下左右 4 个子区域的一共 5 个二元对称多项式,每个部署后的邻居节点通过类似于文献[13]中的方法利用这 5 个二元对称多项式创建成对密钥.Du 提出了一种基于部署知识的随机密钥管理方案[15],该方案在类似文献[14]中所描述的矩形子区域内假设节点是按照 Gaussian 分布的形式部署在该区域内的,部署在同一个子区域内的节点被组织成部署组,每个部署组拥有从同一个全局密钥池中分配的子密钥池,子密钥池的生成方法使得相邻子区域的部署组之间的子密钥池拥有满足一定阈值下限的共享密钥.这些基于部署知识的密钥管理方案通过假设 WSN 节点的部署位置,不但提高了邻居节点之间的连通概率, 同时也在一定程度上将节点受损攻击的影响局部化,从而提高了 WSN 网络抵抗节点受损攻击的能力.

Perrig 提出了 SPINS 协议族[16],它使用 SNEP 协议来实现 WSN 节点对之间的安全通信.每个 WSN 节点都和网络中唯一的基站之间共享一个管理密钥,整个会话密钥的协商过程都必须依赖于基站的参与,基站也为此承担了大部分的协商工作,从而有效地减少了协商过程中 WSN 节点的资源消耗.Zhu 提出了 LEAP 方案[17],它定义了多种类型的密钥用于满足不同级别的安全需求.所有节点都预分配了一个全局的初始化密钥 K_I 来进行会话密钥协商.相比于 SPINS,LEAP 弱化了基站在密钥管理中的作用,使其并不参与节点之间的密钥协商过程,因此具备了比 SPINS 更好的网络扩展性和抵抗节点受损攻击的能力.

2 系统模型

2.1 网络模型

我们假设所考虑的 WSN 网络为实现某种应用而被部署在某一指定的区域内,该网络是同构(homogeneous)和静态(static)的,即网络中的所有节点在软硬件的配置上完全相同且一旦被部署就不会发生位置移动,这是现实应用中 WSN 网络最典型的存在形式.由于 WSN 节点的通信半径是有限的,不在通信半径之内的节点(非邻居节点)之间的通信要借助于在通信半径之内的节点(邻居节点)的中转,最终仍然以邻居节点之间的通信作为前提.不失一般性,我们在本文中仅考虑邻居节点之间的通信.由于网络的部署区域并非是安全的,邻居节点之间必须建立安全链路来保护可能发生的通信.为此,我们使用密钥预分配的方法来让邻居节点之间共享一定数量的密钥信息,通信的数据将通过这些密钥信息生成的成对密钥加密后发送给对方节点.考虑到 WSN 网络节点资源有限的特点,其在无人值守情况下的生存时间也是有限的,一旦部分节点由于能源耗尽、硬件故障或节点受损攻击等原因无法工作从而导致整个网络应用无法进行时,我们就需要对网络进行必要的节点资源的补充,通过部署新的节点使其能够继续执行与应用有关的任务.我们假设网络在其应用周期内最多发生 τ 次节点部署事件,其中包括了为建立网络而进行的首次节点部署,每次节点部署事件的持续时间不会超过给定的阈值 T_{est}.此外,我们假设存在一个管理基站 BS,该基站配备了充足的软硬件资源,并且通过装备大功率无线信号发射装置而使其信号传输范围能够覆盖整个网络部署区域,即网络中的所有节点都能够直接收到它发出的信号.BS 的主要功能是将节点部署事件的发生通知网络中的所有节点,因此 BS 仅需要暂时性地访问网络而无须部署在网络中.例如,BS 可以安放在通过空中撒播方式部署节点的飞机上,并从飞机上向网络部署区域发送通知消息.

2.2 攻击模型

在攻击模型中,我们认为攻击者具有很强的节点破坏能力,他可以通过节点受损攻击来破坏节点,从而获取其中存储的密钥信息.这些密钥信息可以被用来计算得到某些未受损节点之间的成对密钥,从而使攻击者能够更隐蔽地监听这些节点之间的通信.由于 WSN 节点更容易被攻击者捕获,我们认为攻击者更倾向于使用节点受损攻击直接获取密钥信息,而非单纯通过被动的监听方式来进行通信量分析(traffic analysis).攻击者尽管可以在网络应用周期中的任何时刻发起攻击,但我们假设其破坏节点并获取密钥信息所需的最小时间 $T_{\min}>T_{est}$.

3 基于节点部署时间的随机密钥管理

根据定义的网络模型,我们所考虑的 WSN 网络最多发生τ次节点部署事件,分别记为 $E_1,E_2,\ldots,E_\tau$.$E_i(1\le i\le\tau)$的持续时间等同于在该次事件中部署的所有节点完成安全链路创建过程所需的时间.该安全链路创建过程包含成对密钥生成和无用密钥清除两个子过程,将分别在第 4.2 和第 4.3 节中加以阐述.我们将 E_i 开始至 E_{i+1} 开始之间的这段时间间隔称为网络的部署状态(network deployment status),记为 C_i.特别地,我们令 C_τ表示网络从 E_τ 开始至网络应用周期结束之间的部署状态.在 E_i 开始时要部署的 WSN 节点集合称为节点部署组(deployment group),记为 G_i,则 G_1 表示为建立网络而进行的首次部署的节点集合.

3.1 随机密钥预分配

在网络首次部署之前,$\tau+\omega$个密钥池被随机地创建,记为 $KP_1,KP_2,\ldots,KP_{\tau+\omega}$,每个密钥池均含有 P 个随机产生的密钥.$G_i(1\le i\le\tau)$中的每个节点都被随机分配 KP_i 中的 R 个密钥作为其初始密钥环的一部分,而 KP_i 被称为 G_i 的内部密钥池(home key pool).除此之外,G_i 还从 $KP_{i+1},KP_{i+2},\ldots,KP_{\tau+\omega}$ 中随机选择ω个密钥池作为其外部密钥池(foreign key pool),记为 $KP_{j_1}^{(i)},KP_{j_2}^{(i)},\ldots,KP_{j_\omega}^{(i)}$,$G_i$ 中的每个节点也从 G_i 的每个外部密钥池中随机选择 R 个密钥作为其初始密钥环的余下部分.这样,每个要部署的 WSN 节点都将拥有$(\omega+1)R$ 个密钥,其中 R 个密钥来自于该节点所在的部署组的内部密钥池,剩余的ωR 个密钥来自于相应的外部密钥池.在本文中,我们将对应于 G_i 的$\omega+1$个密钥池 $KP_i,KP_{j_1}^{(i)},KP_{j_2}^{(i)},\ldots,KP_{j_\omega}^{(i)}$ 称为 G_i 的关联密钥池.

我们在图 1 中给出了前文所提出的随机密钥预分配方法的一个例子.图中灰色的矩形点表示部署组的内部密钥池,白色的矩形点表示部署组的外部密钥池.图 1 中描述的网络包含最多τ=8 次节点部署事件,即一共有 8 个部署组,每个部署组 G_i 除了拥有自己的内部密钥池 KP_i 外,还拥有ω=2 个随机选择的外部密钥池.例如,G_1 拥有内部密钥池 KP_1 和两个外部密钥池 KP_3 和 KP_4.任何 G_i 的内部密钥池都有可能成为另一个 G_j 的外部密钥池,例如,KP_3 既是 G_3 的内部密钥池又是 G_1 的外部密钥池.图中各部署组的内部密钥池标记点(灰色矩形点)连成的轨迹上方没有任何密钥池的标记点,这说明了该密钥预分配方法使得任何给定的部署组 G_i 只含有下标 $j\ge i$ 的密钥池 KP_j.图 2 给出了随机密钥预分配过程的形式化表述,$KP_{associate}(i)$表示部署组 G_i 的关联密钥池集合,$K_I(j)$表示节点 n_j 的初始密钥集合(即初始密钥环),$K_{v_1}^u,K_{v_2}^u,\ldots,K_{v_R}^u$ 表示从 KP_u 中随机选择的 R 个密钥,符号“←”表示语义“包含”.

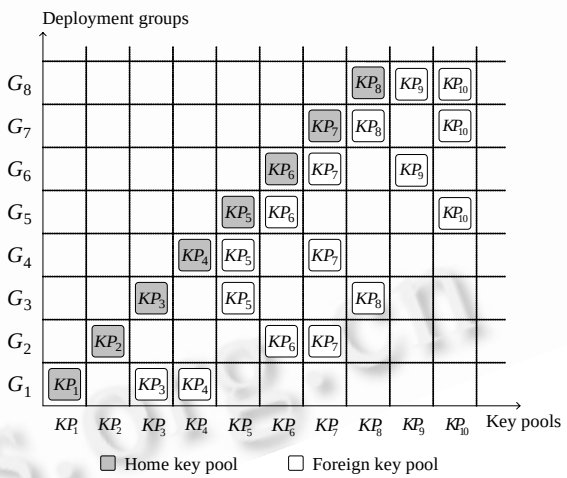

Fig.1 Example of random key predistribution

图 1 随机密钥预分配举例

```
1:  for each deployment group G_i
2:      KP_associate(i) ← KP_i ;
3:      KP_associate(i) ← KP_{j1}^(i), KP_{j2}^(i), ..., KP_{jω}^(i) ;
4:  end
5:  for each node n_j in G_i
6:      for each key pool KP_u in KP_associate(i)
7:          K_I(j) ← K_{v1}^u, K_{v2}^u, ..., K_{vR}^u ;
8:      end
9:  end
```

Fig.2 Procedure of random key predistribution

图 2 随机密钥预分配过程

```
1:  let two nodes n_p ∈ G_i, n_q ∈ G_j
2:  KP_share(i, j) = KP_associate(i) ∩ KP_associate(j)
3:  for each key pool KP_u in KP_share(i, j)
4:      K_share(p, q) ← K_u(p) ∩ K_u(q) ;
5:  end
6:  K_pairwise(p, q) = f_pairwise(K_share(p, q))
```

Fig.3 Procedure of pair-wise key generation

图 3 成对密钥预生成过程

3.2 成对密钥预生成

在事件 E_i 开始时,部署组 G_i 中的所有节点被添加到 WSN 网络中,每个节点向其邻居节点广播自己的密钥信息,方法为广播其密钥环中所含密钥的标识(包括密钥所属密钥池的标识),并试图通过接收邻居节点回应的包含其密钥信息的广播消息来与其建立安全链路.由于假设部署后的节点不会发生位置移动,我们采用成对密钥预生成方法来预先创建与邻居节点之间的成对密钥而不是在未来产生通信需求的时候按需创建.成对密钥的生成方法可以描述为:首先,两个邻居节点寻找其分别所在的部署组之间的共享关联密钥池标识,然后在每个共享关联密钥池中寻找同时分配给它们的共享密钥标识,这样就可以确定这两个节点之间是否有共享密钥以及共享密钥的值,最后两者使用共享的所有密钥共同产生用于安全通信的成对密钥.产生的方法可以为:先对所有的共享密钥进行按位异或操作,然后将操作结果通过一个单向散列函数(one-way hash function)来生成成对密钥,更详细的产生方法见文献[9].以图 1 为例,设两个邻居节点 A 和 B 分别来自于部署组 G_2 和 G_6.A 和 B 之间共享了两个密钥池 KP_6 和 KP_7,这两个节点分别针对 KP_6 和 KP_7 检查是否有共享密钥,最后将分别来自于这两个共享密钥池中的共享密钥组织起来计算得到 A 和 B 之间的成对密钥.图 3 给出了成对密钥预生成过程的形式化表述,n_p 和 n_q 表示两个分别来自于 G_i 和 G_j 的邻居节点,$KP_{share}(i,j)$表示 G_i 和 G_j 之间所共享的关联密钥池集合,$K_u(p)$表示节点 n_p 当前含有的来自于 KP_u 中的密钥集合,$KP_{share}(p,q)$表示 n_p 和 n_q 之间的共享密钥集合,$KP_{pairwise}(p,q)$表示通过计算方法 $f_{pairwise}$ 作用于 $K_{share}(p,q)$而生成的 n_p 和 n_q 之间的成对密钥.

3.3 节点密钥环的后续处理

从成对密钥预生成过程中可以看到,在 E_i 结束时,新部署的 G_i 中的节点已经与各自的邻居节点之间完成了成对密钥的生成,为以后可能发生的通信做好了安全方面的准备.此后,WSN 网络中将有部分不会再被使用到的密钥仍然存在于一些节点的密钥环中,这些密钥应在 E_i 结束后被包含它们的节点从其密钥环中删除.根据随机密钥预分配过程的描述,我们知道在 E_i 结束后所有来自于 $KP_1,KP_2,...,KP_i$ 的密钥都不会在之后的节点部署事件中被用于生成成对密钥,因此它们都应该从有关节点中删除.特别地,在 E_τ结束后,包括 $KP_{\tau+1},KP_{\tau+2},...,KP_{\tau+\omega}$ 在内的来自于所有密钥池的密钥都将被删除,网络中将不存在用于生成成对密钥的任何密钥信息.我们这样做是出于以下两个目的:(1) 释放了节点中有限的存储空间,使其可以用于存放与网络任务有关的数据;(2) 减少了攻击者破坏节点之后获取密钥信息的数量,从而削弱了其对未受损节点之间安全通信的监听能力,提高了整个网络的安全性.

为了确保所有的网络节点都能够在 E_i 结束后及时有效地删除无用的密钥,管理基站 BS 在 E_i 开始时向网络中广播一个部署开始消息,记为 β_i.在定义的网络模型中,我们假设 BS 的信号传输范围能够覆盖整个 WSN 网络的部署区域,因此所有的网络节点都可以直接收到 BS 发出的广播消息而无需其他中间节点的转发,从而将广播消息的传输距离固定在一跳(one-hop).由于单跳传输的延迟非常短,我们将忽略这段时间.节点在收到 β_i 后便开始计时,在时间阈值 T_{est} 到达时停止计时并删除保存的所有来自于 KP_i 的密钥.此外,为了防止攻击者伪造广播消息而使网络节点错误地删除有用的密钥,可以使用基于单向密钥链[18]的验证方法(one-way key chain based authentication)[17]对 β_i 的真实性加以验证.下面简要地描述该方法在本文方案中的应用,原始方法的详细过程见文献[17].在整个网络部署之前,BS 首先生成一个长度为 $m(m>\tau)$的单向密钥链,记为 $\overline{K}=\langle K_0,K_1,...,K_{m-1}\rangle$,$\overline{K}$ 的生成方法是:BS 先随机产生密钥 K_{m-1},然后使用某一单向散列函数 F 生成余下的 $m-1$ 个密钥,即 $K_{i-1}=F(K_i)(1\le i\le m-1)$.在 E_i 开始前,$G_i(1\le i\le \tau)$中的所有节点保存 $\overline{K}$ 中的密钥 K_{i-1}.在 E_i 开始时,BS 除了广播 β_i 外,还同时广播 β_i 的验证码 MAC_i 和用于生成该验证码的密钥 K_i,即广播的消息变为 $\beta_i'=\langle\beta_i,MAC_i,K_i\rangle$.节点在收到 β_i' 后首先使用保存的密钥 K_{i-1} 验证 K_i,即 $F(K_i)$是否等于 K_{i-1},验证成功后再使用 K_i 重新生成 β_i 的验证码并与 β_i' 中的 MAC_i 进行比较,若比较成功则说明 β_i 是 BS 发送的.随后,该节点删除 K_{i-1} 并保存 K_i 用于下一次的验证过程.整个验证过程(包括密钥验证过程和验证码验证过程)主要使用了单向散列函数,因此验证所需的时间很短,可以忽略.通过以上方法,我们能够让所有的网络节点在 $T_{\min}$ 到来之前成功地清除所有无用的密钥,增强了网络抵抗节点受损攻击的能力.

4 分 析

4.1 节点连通度

根据成对密钥预生成过程的描述,两个邻居节点之间要创建成对密钥就必须同时满足两个条件:(1) 两节点分别所在的部署组之间要存在共享的关联密钥池;(2) 至少存在1个共享关联密钥池,使得这两个节点的密钥环中分别来自该密钥池的 R 个密钥之间存在共享密钥.对节点连通度而言,我们关注的是在某一节点部署事件 E_t 开始时,对应的部署组 G_t 中的节点有多大的可能性与其部署后的邻居节点之间存在这样的共享密钥.

先考虑以上的第 1 个条件先求出给定的两个部署组 G_i 和 G_j 之间正好存在 s 个共享关联密钥池的概率,记为 $p_{group}((i,j),s)$,我们不妨设 $i\leq j$,则可以得到:

$$p_{group}((i,j),s)=\begin{cases}\dfrac{C_{\tau-i-1}^{\omega-s}\cdot(C_{\tau+\omega-j}^{s-1}C_{\tau+\omega-j-s+1}^{\omega-s+1}+C_{\tau+\omega-j}^{s}C_{\tau+\omega-j-s}^{\omega-s})}{C_{\tau+\omega-i}^{\omega}C_{\tau+\omega-j}^{\omega}}, & i<j\\ C_s^{\omega+1}, & i=j\end{cases} \tag{1}$$

公式(1)中的 C_n^m 表示在 n 中取 m 的组合数,本文中规定当 $n<m$ 时,$C_n^m=0$.接下来,我们求 G_i 和 G_j 之间至少存在一个共享关联密钥池的概率,记为 $p_{group}(i,j)$,由公式(1)可以直接得到:

$$p_{group}(i,j)=\sum_{s=1}^{\omega+1}p_{group}((i,j),s) \tag{2}$$

由公式(2)可知,若 $i=j$,则 $p_{group}(i,j)=1$.否则,当 $i\geq\tau-\omega$时,$p_{group}(i,j)=1$;当 $i<\tau-\omega$时,$p_{group}(i,j)$可化简为

$$p_{group}(i,j)=1-\frac{C_{\tau-i-1}^{\omega}C_{\tau+\omega-j}^{\omega}}{C_{\tau+\omega-i}^{\omega}C_{\tau+\omega-j}^{\omega}}=1-\frac{C_{\tau-i-1}^{\omega}}{C_{\tau+\omega-i}^{\omega}} \tag{3}$$

我们将以上情况整理后得到,当 $i\leq j$ 时,

$$p_{group}(i,j)=\begin{cases}1, & \tau-\omega\leq i\leq j\\ 1-\dfrac{C_{\tau-i-1}^{\omega}}{C_{\tau+\omega-i}^{\omega}}, & i<\tau-\omega \text{ and } i<j\end{cases} \tag{4}$$

接下来考虑第 2 个条件.参考 E-G 方案[8]可以得到,对于某个共享关联密钥池而言,邻居节点之间至少含有其中的 1 个共享密钥的概率 P_{local} 为

$$p_{local}=1-\frac{C_{P-R}^{R}}{C_P^R}=1-\frac{((P-R)!)^2}{(P-2R)!P!} \tag{5}$$

需要强调的是,这个概率是基于第 1 个条件的条件概率而非绝对概率,只有在存在共享关联密钥池的前提下讨论 P_{local} 才有意义.根据 Stirling $n!$估计公式,在 n 很大时,我们有 $n!\approx\sqrt{2\pi}n^{n+\frac{1}{2}}\mathrm{e}^{-n}$,因此 P_{local} 可化简估计为

$$\hat{p}_{local}=1-\frac{\left(1-\dfrac{R}{P}\right)^{2\left(P-R+\frac{1}{2}\right)}}{\left(1-\dfrac{2R}{P}\right)^{\left(P-2R+\frac{1}{2}\right)}} \tag{6}$$

根据 $\hat{p}_{local}$ 在图 4 中给出了 P_{local} 随 P 和 R 的变化情况,从图中可以看出,对于某个给定的密钥池而言,一个节点只要拥有很少量的密钥就可以获得很高的与其邻居节点的密钥共享概率.例如,在密钥池尺寸 P=50 时,节点拥有的来自该密钥池的密钥数量只要达到 R=10 个,就可以使密钥共享概率 P_{local} 接近于 1;而在 P=1000 时,为了使 P_{local} 达到同样的水平,只要令 R=75 即可.在本文下面的分析中,我们参照公式(5)和图 4,合适地选择 P 和 R 的值,以获得足够高(接近于 1)的 P_{local} 值,从而在一定程度上保证了邻居节点安全链路的创建概率.

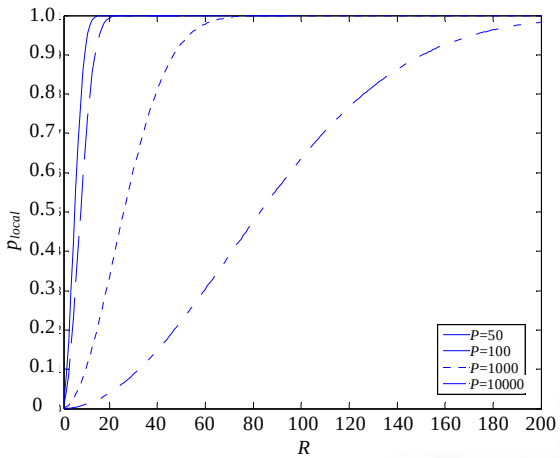

Fig.4 Relationship between p_{local} and R for a given P
图 4 在给定 P 下的 p_{local} 与 R 的关系

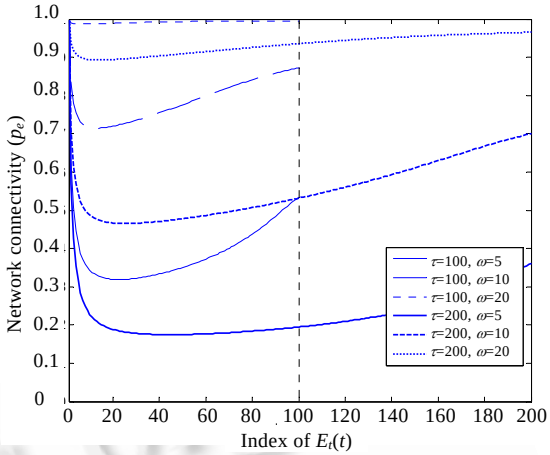

Fig.5 Relationship between p_e and E_t
图 5 p_e 和 E_t 之间的关系

现在我们将本小节开始提出的两个条件结合起来进行考虑.仍然假设 $i\leq j$,若给定的两个部署组 G_i 和 G_j 之间正好存在 s 个共享密钥池,则 G_i 中的节点与 G_j 中的节点之间存在共享密钥的概率为 $1-(1-p_{local})^s$,则 G_i 和 G_j 之间正好存在 s 个共享密钥池且两者的节点之间存在共享密钥的概率为 $p_{group}((i,j),s)\cdot(1-(1-p_{local})^s)$,从而进一步得到对于任意的两个部署组 G_i 和 G_j 而言,G_i 中的节点与 G_j 中的节点之间存在共享密钥的概率为 $\sum_{s=1}^{\omega+1} p_{group}((i,j),s)\cdot(1-(1-p_{local})^s)$.最终,我们结合以上结果,得出了在 E_t 开始时,G_t 中的节点与其部署后的邻居节点(根据第 3.1 节中的方案描述可知,这些邻居节点来自于部署组 $G_1,G_2,\ldots,G_t$)之间存在共享密钥的概率期望 $p_e(t)$如下所示(这里,我们认为节点属于当前的 t 个部署组中任何一个的概率是相同的,即都为 $\frac{1}{t}$):

$$p_e(t)=\frac{\sum_{i=1}^{t}\sum_{s=1}^{\omega+1} p_{group}((i,t),s)\cdot(1-(1-p_{local})^s)}{t} \tag{7}$$

根据公式(7),图 5 给出了 p_e 和 E_t 的关系描述.在该图中,我们令 P=1000,R=75,则 $p_{local}\approx 1$,并在图中保持不变,则公式(7)可化简估计为

$$\hat{p}_e(t)=\frac{\sum_{i=1}^{t}\sum_{s=1}^{\omega+1} p_{group}((i,t),s)}{t}=\frac{\sum_{i=1}^{t} p_{group}(i,t)}{t} \tag{8}$$

如图 5 所示,在节点部署事件阈值 τ不变的条件下,增加每个部署组外部密钥池的数量 ω会提高部署组之间存在共享关联密钥池的概率,从而在 p_{local} 不变的情况下提高了节点连通度 p_e.同理,在 ω不变的条件下,增加 τ会同时减小 p_e.从单个曲线来看,我们考虑的节点连通度 p_e 在网络的整个应用周期中是随着节点的陆续部署不断地发生变化的.p_e 的变化分为明显的两个阶段,节点首次部署事件 E_1 开始时,p_e 达到了其在整个 WSN 应用周期中的最大值,随着节点部署事件的陆续发生,p_e 经历了短暂而迅速的下降并在网络应用周期早期达到了其最小值,之后再渐渐地单调上升并在最后一个节点部署事件 E_τ开始时达到了上升之后的最大值.我们从图 5 中可以看到,合适地选择 τ和 ω的值可以将节点连通度 p_e 保持在一个很高的水平上(例如,取 τ=200,ω=20,则 p_e 几乎保持在 90%以上),从而使得邻居节点之间更容易建立安全链路.

以上我们分析了在节点部署事件发生时,新部署的节点与其部署后的邻居节点之间的连通概率问题,下面讨论该连通概率(即 p_e)与 WSN 网络连通概率的关系问题.根据 Erdös 和 Rényi 的随机图理论,在组成 WSN 网络的节点数量 n 足够大时,有如下关系:

$$\bar{d}=\frac{n-1}{n}\left[\ln n-\ln(-\ln p_{connected})\right]\approx \ln n-\ln(-\ln p_{connected}) \tag{9}$$

其中,$p_{connected}$ 表示网络为连通的概率,$\bar{d}$ 表示任一节点的邻居节点中与之存在安全链路(即存在共享密钥)的节

点的平均数量.根据公式(9),若我们要求 WSN 网络的连通概率为 $p_{connected}$=0.99999(即几乎肯定是连通的),而网络的节点数量为 n=100 000,则每个节点平均要与 $\overline{d}=23$ 个邻居节点之间存在共享密钥.令 n'表示网络的节点密度, 即在同一无线通信半径范围内的节点的平均数量,则我们可以得到 p_e 的另一种表达形式:

$$p_e(t)=\frac{\overline{d}}{n'-1} \tag{10}$$

综合式(9)、式(10)得,我们可以在减小 p_e 的同时增加 n'来保证原有的网络连通概率 $p_{connected}$.从这一点来看,p_e 并不需要保持在一个很高的水平上,我们可以通过增加节点密度的方法来弥补 p_e 的值偏低的不足.

4.2 安 全

在方案的安全性方面,我们集中关注攻击者所发起的节点受损攻击对 WSN 网络中未受损节点之间的安全通信会产生多大程度的影响,这也是以往所有相关研究工作关注的安全焦点.在第 2.2 节定义的攻击模型中,我们假设攻击者可以在网络应用周期中的任何时候发起节点受损攻击.为此,我们考虑任一网络部署状态 $C_t(1\le t\le \tau)$,将 C_t 划分为两个连续而不重叠的时间段,分别记为 C_t^1 和 C_t^2,其中 C_t^1 表示从 E_t 开始到 E_t 结束之间的时间间隔,C_t^2 表示从 E_t 结束到 E_{t+1} 开始之间的时间间隔,如图 6 所示.在图 6 中,T_{t-1},T_t,T_{t+1} 分别表示 E_{t-1},E_t,E_{t+1} 的开始时刻,我们用时间阈值 T_{est} 来估计节点部署事件的结束时刻,即 E_{t-1},E_t,E_{t+1} 的结束时刻分别为 $T_{t-1}+T_{est},T_t+T_{est},T_{t+1}+T_{est}$.若节点受损攻击发生在 C_t^1 时,在此期间节点部署仍在进行,攻击者试图破坏的节点有可能含有来自于 KP_t 的密钥,然而我们的假设 $T_{\min}>T_{est}$ 保证了攻击者在成功获取 KP_t 中的密钥之前,有关节点已经及时地删除了这些密钥;若节点受损攻击发生在 C_t^2 时,则 KP_t 中的密钥已被安全地从网络中删除,攻击者仅能够获得来自于 $KP_{t+1},KP_{t+2},...,KP_{\tau+\omega}$ 的密钥.由此可得,攻击者在网络部署状态为 C_t 时从受损节点中获取的密钥信息仅可能用来破坏全部使用来自于 $KP_{t+1},KP_{t+2},...,KP_{\tau+\omega}$ 的密钥生成的成对密钥所保护的安全通信.

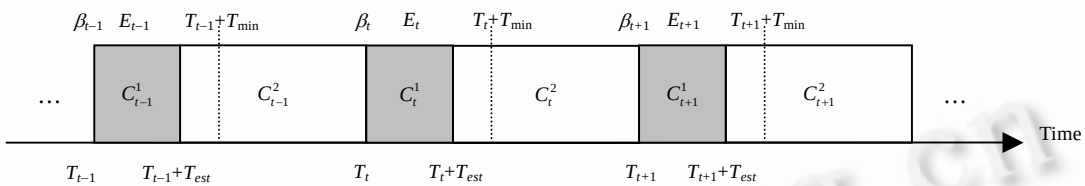

Fig.6 Network status model of time-based deployment

图 6 基于时间部署的网络状态模型

为了量化发生在 C_t 时的节点受损攻击对 WSN 网络的影响,我们需要求得攻击者利用从受损节点中获取的密钥信息能够成功监听任何两个未受损的邻居节点之间的安全通信的概率,称为剩余网络受损概率,记为 p_{comp}.假设在 C_t 时攻击者一共破坏了 x 个节点并成功获取了节点存储的所有密钥信息.随后,攻击者试图对网络中已知的两个未受损的邻居节点 A 和 B 之间的安全通信进行监听,为此则必须得到 A 和 B 之间的成对密钥,更确切地说是生成成对密钥所使用的共享密钥.值得注意的是,这些共享密钥的一部分或全部可能已被删除,在这种情况下攻击者无法通过已获取的密钥信息得到A和B之间的成对密钥,从而无法监听它们之间的安全通信.假设A和 B 分别来自于 G_a 和 G_b,其共享关联密钥池的数量为 s.先考虑来自于其中某一个共享关联密钥池 KP'中的共享密钥,则其他的情况可以类似地考虑.令某个受损节点所在部署组 $G_i(i\le t)$的关联密钥池包含某一密钥池 KP_j 的概率为 $p_{KP}(i,j)$,则

$$p_{KP}(i,j)=\begin{cases}0, & j\le t\\ \dfrac{\omega}{\tau+\omega-i}, & j>t\end{cases} \tag{11}$$

可以得到 p_{KP} 的数学期望 $\mathrm{E}p_{KP}(t)$为

$$\mathrm{E}p_{KP}(t)=\frac{\sum_{1\le i\le t,1\le j\le \tau+\omega} p_{KP}(i,j)}{t(\tau+\omega)} \tag{12}$$

$\mathrm{E}p_{KP}(t)$即为在 C_t 时任一受损节点所在部署组的关联密钥池包含 KP'的平均概率.该受损节点拥有 KP'中某个密钥 K 的条件概率为 $p_K=\frac{R}{P}$,则拥有密钥 K 的绝对概率表示为 $\mathrm{E}p_{KP}(t)\cdot p_K$.假设 A 和 B 中来自于 KP'的共享密钥数量为 k,有 x 个受损节点中的密钥信息不包含这 k 个中的任何一个共享密钥的概率为 $(1-\mathrm{E}p_{KP}(t)\cdot p_K)^x$,则包含这 k 个共享密钥的概率为 $(1-(1-\mathrm{E}p_{KP}(t)\cdot p_K)^x)^k$.令 A 和 B 中来自于 KP'的共享密钥数量为 k 的条件概率为 $p'_K(k)$,则公式(5)中的 p_{local} 也可以表示为 $p_{local}=\sum_{k=1}^{R}p'_K(k)$,且

$$p'_K(k)=\frac{C_R^k C_{P-R}^{R-k}}{C_P^R} \tag{13}$$

因此,x 个受损节点中的密钥信息包含来自于 KP'的所有共享密钥的概率期望 $\mathrm{E}p'_K(t,x)$ 为

$$\mathrm{E}p'_K(t,x)=\sum_{k=1}^{R}(1-(1-\mathrm{E}p_{KP}(t)\cdot p_K)^x)^k\cdot\frac{p'_K(k)}{p_{local}} \tag{14}$$

类似地,假设 $a\le b$,则由公式(1)可知,G_a 和 G_b 之间共享 s 个关联密钥池的概率 $p'_{KP}((a,b),s)=p_{group}((a,b),s)$,且有 $p_{group}(a,b)=\sum_{s=1}^{\omega+1}p'_{KP}((a,b),s)$,则任何两个部署组之间共享 s 个关联密钥池的概率期望 $\mathrm{E}p'_{KP}(s)$ 为

$$\mathrm{E}p'_{KP}(s)=\frac{\sum_{1\le a<b\le\tau}2\cdot p'_{KP}((a,b),s)+\sum_{1\le a=b\le\tau}p'_{KP}((a,b),s)}{\tau^2} \tag{15}$$

而任何两个部署组之间存在共享关联密钥池的概率期望 $\mathrm{E}p'_{KP}$ 为

$$\mathrm{E}p'_{KP}=\frac{\sum_{1\le a<b\le\tau}2\cdot p_{group}(a,b)+\sum_{1\le a=b\le\tau}p_{group}(a,b)}{\tau^2} \tag{16}$$

最后,我们得到这 x 个受损节点中的密钥信息包含 A 和 B 之间所有的共享密钥的概率期望,即剩余网络受损概率 $p_{comp}(t,x)$为

$$p_{comp}(t,x)=\begin{cases}\sum_{s=1}^{\omega+1}(\mathrm{E}p'_K(t,x))^s\cdot\frac{\mathrm{E}p'_{KP}(s)}{\mathrm{E}p'_{KP}}, & t<\tau\\ 0, & t=\tau\end{cases} \tag{17}$$

根据式(17),我们在图 7 中给出了当节点受损攻击发生在 C_t 时的剩余网络受损概率 $p_{comp}(t,x)$,P 和 R 的取值同第 5.1 节中的设置,即 P=1000,R=75.从图中可以看到,节点受损攻击发生的时间越晚,被成功监听的安全通信的比例越低,从而网络受到攻击的影响越小,抵抗攻击的能力越强,这是由于整个网络中的密钥信息量随着无用密钥的陆续删除而不断减少所致.而在 C_τ时,来自 $\tau+\omega$个密钥池的所有密钥全部从网络中删除,则 $p_{comp}(\tau,x)$=0,即攻击者无法破坏剩余网络中的安全通信.此外,随着 ω的增加,p_{comp} 的下降呈加快的趋势,这是因为 ω的增加会使得节点所在部署组之间的共享关联密钥池的数量也呈增长的趋势,相应的共享密钥的数量也趋于增长,从而加大了攻击者获取所有共享密钥的难度,加快了 p_{comp} 的下降趋势.

图 8 给出了不同规模的节点受损攻击对未受损邻居节点之间安全通信的影响,本文所提方案在图中的曲线数据来源于在不同数值的 x 下对 $p_{comp}(t,x)$按 t 在其定义域$[1,\tau]$内取平均值的结果,记为 $\overline{p}_{comp}(x)$,即

$$\overline{p}_{comp}(x)=\frac{\sum_{t=1}^{\tau}p_{comp}(t,x)}{\tau} \tag{18}$$

取平均值的做法是因为我们认为节点受损攻击的发生时间是平均分布于网络应用周期内的,即网络中的任何时刻都有相同的概率会发生这样的攻击.图中本文的方案与 E-G 方案[8]和 q-composite 方案[9](q=1)进行了量化比较,这两种方案的简要描述请参考第 2 节的相关工作.在此,我们选择了 q=1 时的 q-composite(记为 1-composite)方案,该方案规定只要邻居节点之间存在至少 q=1 个共享密钥便可以创建安全链路,这与本文方案的规定相符.从图 8 中可以看出,本文方案在使用相同的初始密钥环存储空间(初始密钥环尺寸均为 200)的条件

下要优于 E-G 方案和 1-composite 方案,这种优势主要得益于以下两个方面:(1) 提供了两级密钥管理机制,在原有的随机密钥预分配基础上对密钥池也进行了随机预分配,通过阶梯状的密钥池分配机制(如图 1 所示)使得节点受损攻击的效率受到了攻击时间的制约,表现为攻击时间越晚攻击效率越低;(2) 对密钥环中无用密钥的后续清除机制不但节约了 WSN 节点中有限的存储空间,而且有效地降低了攻击者可能使用这些无用密钥对已有的安全通信进行成功监听的概率.

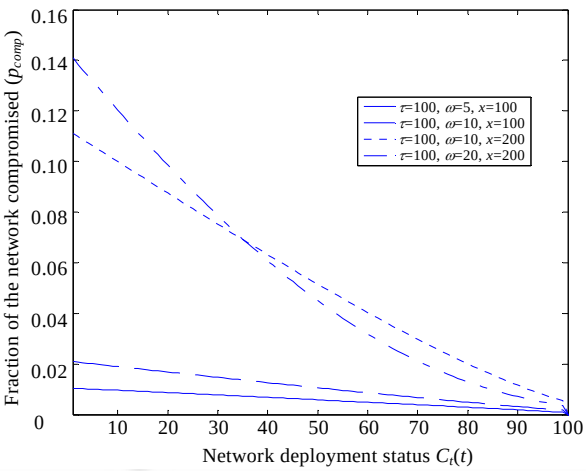

Fig.7 Network resilience against node compromise at C_t

图 7 C_t 时的节点受损攻击对网络抵抗节点受损攻击能力的影响

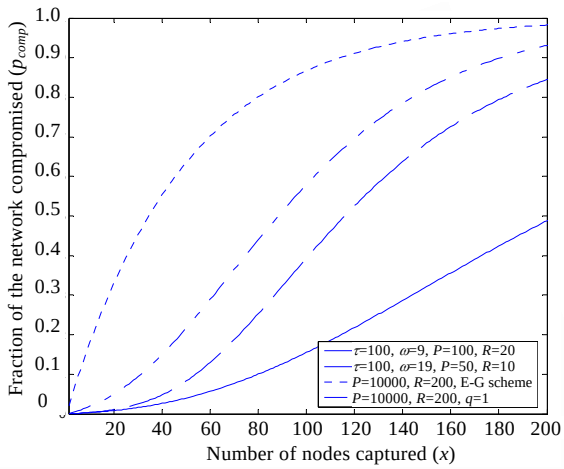

Fig.8 Network resilience against node compromise of various numbers

图 8 不同数量的受损节点对网络抵抗节点受损攻击能力的影响

4.3 讨 论

在前面两节中,我们分析了方案涉及的关键参数 P,R,τ,ω对节点连通度和网络抵抗节点受损攻击能力的影响.由式(7)和式(17)可知,网络实际应用中对节点连通度和网络安全的要求也同样影响着这些参数的设置.此外,由于这些参数的设置直接决定了节点的初始密钥环尺寸(即$(\omega+1)R$),因此其在很大程度上受限于节点用于存储密钥信息的内存空间大小.然而,这些对方案参数的制约因素并不会影响我们对方案本身进行的分析,而在与其他方案的安全性比较分析中,我们使用了相同的初始密钥环尺寸设置以使得比较的结果更加公平合理.

我们对本文方案所做的分析是在之前定义的系统模型下进行的,因此分析的结果只有在满足模型描述的要求时才有意义.在下文中,我们将对模型中定义的参数进行简要的讨论,讨论的焦点集中在对τ,T_{est}和 $T_{\min}$的假设合理性上.

根据网络模型的描述,我们假设所考虑的网络在其应用周期内最多发生τ次节点部署事件.在方案的实际应用中,需要知道或估计τ,从而能够正常执行随机密钥预分配过程,部署后的邻居节点才有可能创建安全链路.如果在节点部署过程中发现预先估计的τ值偏小,无法满足后续的节点部署要求,我们便需要对网络进行必要的重新配置以适应未来额外增加的节点部署事件.为此,我们可以采用以下的方法将τ提高到 2τ:每个节点 n_i 在网络部署之前都保存一个只与管理基站 BS 共享的成对密钥,记为 K_i^{BS}.当最后一个节点部署事件 E_τ结束后,网络中所有节点分配到的来自于$\tau+\omega$个密钥池 $KP_1,KP_2,...,KP_{\tau+\omega}$ 中的密钥都被全部删除.为了重新给节点分配密钥信息用于后续添加的节点部署事件,我们按照随机密钥预分配过程再次生成$\tau+\omega$个新的密钥池,并通过 BS 将分配给 n_i 的密钥信息用 K_i^{BS} 加密后发送给 n_i.n_i 在收到新的密钥信息后便与邻居节点重新开始成对密钥预生成过程,这可以看作是一次新的节点部署事件的发生,我们不妨记为 E_1'.对于还未部署的节点,我们也使用新产生的$\tau+\omega$个密钥池按随机密钥预分配过程对它们进行密钥分配.通过这种方法,我们便将节点部署事件的次数从最多τ次提高到了 2τ次,即 $E_1,...,E_\tau,E_1',...,E_\tau'$.依此类推,可以认为节点部署事件的次数不再受到$\tau$的限

制,从而可以根据网络应用的实际状况按需进行增加.

根据攻击模型的描述,假设 $T_{est}<T_{\min}$,这在方案的实际应用中对大多数典型的 WSN 网络和攻击者而言是可以实现的.我们考虑现在被广泛使用的MICA2 mote[19]传感器节点所组成的WSN网络.T_{est}主要包括部署组节点完成成对密钥预生成过程所需的时间,而由于节点在广播各自的密钥信息时使用的是广播密钥标识的方法,信息量很小,且该广播仅存在于发送节点的邻居区域内,不会被其他节点转发,因而信息传输的时间很短,对 MICA2 mote 节点而言通常只有数秒的时间,而通过使用高效的 CSMA 媒体访问控制协议[20],我们可以使无线信道访问的冲突次数减到很小,极大地缩短了不必要的冲突延迟时间.我们因而认为 T_{est} 可以被控制在数秒之内,而攻击者通常需要长得多的时间($T_{\min}$ 为数百秒)来成功获取节点中的密钥信息.因此,节点部署事件的进行是安全的,能够有效地避免攻击者对节点密钥信息的恶意获取.

5 结束语及未来的工作

本文描述了一种用于大规模无线传感器网络的随机密钥管理方案,该方案使用了两级随机密钥管理机制和密钥清除机制使网络具备了在高节点连通度下比 E-G 方案和 q-composite 方案更强的抵抗节点受损攻击的能力.与后者的两种方案一样,该方案所涉及的资源开销取决于密钥环的尺寸和成对密钥的生成方法,而特有的密钥清除机制使密钥环的尺寸不断地减小并最终达到 0,这使得在使用相同的初始密钥环尺寸和成对密钥生成方法的情况下,该方案比后者的两种方案的资源开销更小,资源的使用效率更高.

作为以后的工作,我们将在即将搭建的 WSN 网络硬件平台上对该方案进行实际的部署并且再次比较其与同时部署的 E-G 方案和 q-composite 方案在性能和安全方面的效果.同时,我们也将试图推广本方案中的密钥管理思想,结合其他一些已知的密钥管理方案设计和实现新的方案,在性能损失可以接受的条件下提供更强的抵抗节点受损攻击的能力.

References:

[1] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A Survey on Sensor Networks. IEEE Communications Magazine, 2002, 40(8):102−114.

[2] 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 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1218.htm

[3] Crossbow Technology. Product feature reference: Sensors and functions. http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/Product_Feature_Reference_Chart.pdf

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

[5] Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 1978,21(2):120−126.

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

[7] Anjum F, Mouchtaris P. Security for Wireless Ad Hoc Networks. John Wiley Publications, 2007.

[8] Eschenauer L, Gligor VD. 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.

[9] 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.

[10] 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.

[11] Blom R. An optimal class of symmetric key generation systems. In: Proc. of the EUROCRYPT 1984. New York: Springer-Verlag, 1984. 335−338.

[12] 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.

[13] Blundo C, De Santis A, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly-Secure key distribution for dynamic conferences. In: Proc. of the CRYPTO 1992. New York: Springer-Verlag, 1993. 471−486.

[14] 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.

[15] 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.

[16] Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. SPINS: Security protocols for sensor networks. Wireless Networks, 2002, 8(5):521−534.

[17] 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.

[18] Lamport L. Password authentication with insecure communication. Communications of the ACM, 1981,24(11):770−772.

[19] Crossbow Technology. MICA2: Wireless measurement system. http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf

[20] Woo A, Culler DE. A transmission control scheme for media access in sensor networks. In: Proc. of the 7th Annual Conf. on Mobile Computing and Networking. New York: ACM Press, 2001. 221−235.

附中文参考文献:

[2] 苏忠,林闯,封富君,任丰原.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. http://www.jos.org.cn/1000-9825/18/1218.htm

袁斑(1981－),男,上海人,博士,主要研究领域为无线自组织网络,无线传感器网络,网络安全.

钟亦平(1953－),女,教授,博士生导师,主要研究领域为网络安全,协议分析与测试.

马建庆(1974－),男,博士,讲师,主要研究领域为无线网络,网络安全.

张世永(1950－),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,信息安全,无线通信,移动计算.