无线传感器网络及移动 sink 安全

张旭彬[1] 刘志宏[2]

(西安电子科技大学通信工程学院 西安 710071)[1] (西安电子科技大学计算机学院 西安 710071)[2]

摘 要 处于恶劣环境中的无监护传感器网络面临安全威胁。由于无人值守,传感器节点必须临时保存检测数据,而缺乏抗毁保护的节点面临保护数据安全的难题。在无监护传感器网络中,网络管理者定期派遣移动 sink 收集检测数据,如果移动 sink 被赋予过多的特权,它会成为攻击目标,由此必须要限制移动 sink 的特权。此外,安全的密钥管理是保障传感器网络数据机密性、完整性和通信安全的基础。针对以上安全问题,提出适用于移动 sink 场景的密钥分发方案和移动 sink 特权限制方法。

关键词 密钥预分配,移动 sink,安全,无线传感器网络

中图法分类号 TP393 **文献标识码** A

Security in Wireless Sensor Networks with Mobile Sink

ZHANG Xu-bin[1] LIU Zhi-hong[2]

(School of Telecommunications Engineering, Xidian University, Xi'an 710071, China)[1]

(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)[2]

Abstract Unattended wireless sensor networks operating in hostile environments face the risk of compromise. Given the unattended nature, sensors must safeguard their sensed data of high value temporarily. However, saving data inside a network creates security problems due to the lack of tamper-resistance of sensors and the unattended nature of the network. In some occasions, a network controller may periodically dispatch mobile sinks to collect data. If a mobile sink is given too many privileges, it will become very attractive for attack. Thus, the privilege of mobile sinks should be restricted. Additionally, secret keys should be used to achieve data confidentiality, integrity, and authentication between communicating parties. To address these security issues, we present mAKPS, an asymmetric key predistribution scheme with mobile sinks, to facilitate the key distribution and privilege restriction of mobile sinks.

Keywords Key predistribution, Mobile sink, Security, Wireless sensor network

1 引言

无线传感器网络(Wireless Sensor Network, WSN)可以应用于包括军事及民用等多方面的不同场合[1]。近期,无监护传感器网络(Unattended Wireless Sensor Network, UWSN)的安全问题引起了研究者的注意[2-5]。与普通 WSN 不同,无监护传感器网络中的传感器节点不能实时与基站或 sink 节点通信,传感器节点收集并保存本地检测数据,等待某个外部信号后,才把检测数据上传至基站(或移动 sink)。传感器节点不能实时上报检测数据。

如果传感器节点不能及时上传检测数据,它将面临另一种危险:存储在节点中的数据很可能被敌手修改、删除或替换。传感器节点通常代价低廉,大批量生产,不可能给每个节点安装抗毁组件,单个的传感器节点很容易被敌手俘获。在很多 WSN 应用中,移动 sink(Mobile sink,或 Mobile soldier, Mobile worker)常用来处理网络业务,如查询、收集检测数据、对网络进行维护操作等。

本文假设传感器节点临时存储检测数据,网络管理者定期派遣移动 sink 来收集节点的检测数据。然而,采用移动 sink 给网络带来了新的安全威胁:一旦某个移动 sink 被敌手俘获,赋予移动 sink 的某些特权很可能被敌手滥用[5,6]。例如,假设管理者派遣一个移动 sink 收集网络特定区域或特定类型的检测数据,如果对移动 sink 没有适当的特权限制,敌手通过攻陷某个移动 sink 就可以对网络进行非法操作。

对 UWSN 而言,另一个关键的需求是网络通信的安全。因为传感器节点拥有的资源有限,且对称密码技术占用的计算、存储等资源较少(相对公钥算法而言),效率较高,一般采用对称密码技术来保证系统安全。但是,对称密码技术需要通信双方共享同一个密钥,如何利用传感器节点有限的资源来为节点建立和分配初始共享密钥,是对称密码技术首先需要解决的一个问题。本文重点关注通过移动 sink 收集节点检测数据的 UWSN 的安全问题,提出一个适用于移动 sink 场景、采用非对称密钥预分配协议[7]的安全机制(Asymmetric Key Predistribution Scheme with Mobile Sinks, mAKPS)。

本文受国家自然科学基金(61173135)资助。

张旭彬(1991-),女,主要研究方向为无线通信与网络,E-mail:xbzhang1991@gmail.com;刘志宏(1967-),男,博士,副教授,主要研究方向为网络与信息安全。

mAKPS可以用来为通信的传感器节点提供密钥分配，并能够限制移动 sink 的特权。

协议着眼于保护 UWSN 网络中传感器节点存储的检测数据和节点间的通信。移动 sink 不仅完成管理者安排的网络任务，如收集检测数据，而且要协助传感器节点完成密钥分配。传感器节点负责常规的检测任务，移动 sink 在穿越网络执行收集任务的过程中，为邻近的传感器节点提供建立共享密钥所需的密钥材料(Keying Material)。我们采用非对称的密钥预分配机制(Asymmetric Key Predistribution Scheme, AKPS)[7]来处理 UWSN 的密钥建立问题，通过把大量的存储开销转移到资源相对更充足的移动 sink，来降低传感器节点的存储开销。为了能有效限制移动 sink 的特权，在 mAKPS 中添加了移动 sink 特权限制机制，可以把移动 sink 的特权限制到只能访问部分传感器节点，或特定的数据类型，或特定传感器节点的特定数据类型。

2 网络假设

假设在 UWSN 中，网络由一个离线的控制者(TA)和传感器节点组成，每个节点具有惟一的标识。无监护(Unattended)意味着传感器节点不能根据自己的意图或需要随时与 sink 通信。网络部署到检测区域以后，处于一种无人照看或监管状态。每个传感器节点有一定的存储空间，可以暂存近期的检测数据，这些检测数据可以由授权的移动 sink 检索。

移动 sink 可以是战场环境中的士兵、公园中的游客，或者野外保护区中的动物学家等。每个移动 sink 具有惟一的标识 ID，有较丰富的资源(如计算、存储、能量等)。

图 1 是一个应用实例，TA 派遣一个移动 sink 收集网络检测数据。500 个传感器节点随机分布在边长为 500 米的二维区域中，传感器节点和移动 sink 的通信范围均为 50 米。图中蓝色小方块表示被移动 sink 访问过的传感器节点，线条表示移动 sink 的行进路线。

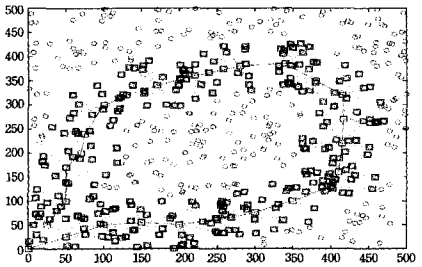

图 1 移动 sink 收集网络检测数据实例

假设传感器节点和移动 sink 均不具备抗毁能力。节点或移动 sink 如果被敌手俘获，保存的所有机密信息泄露。

3 mAKPS

mAKPS 是一个密钥预分配协议，通过移动 sink 辅助完成密钥分配工作，且能限制移动 sink 的特权不被滥用。下面首先简单介绍非对称密钥预分配协议(AKPS)[7]和 Lighton-Micali 提出的密钥协商协议[8]。这两部分是 mAKPS 的主要组件。

3.1 非对称密钥预分配协议

设 TA 表示网络管理者，KMS 表示密钥材料服务器，$\omega=\{U_1,\cdots,U_n\}$表示用户集合。$2^\omega$表示用户集合 ω 的所有子集，定义 $\mathcal{P}\subseteq 2^\omega$为特权用户子集(privileged subset)，子集中的用户能计算得到共享密钥，用于保护集合内用户的通信；定义 $\mathcal{F}\subseteq 2^\omega$为禁止用户子集(forbidden subset)，子集中的用户不能获得特权用户子集的通信密钥。

AKPS 由两个步骤组成：密钥分配阶段和密钥计算阶段。在密钥分配阶段，TA 首先给每个用户分配秘密密钥，此后把公开密钥材料装入 KMS 中。在密钥计算阶段，特权用户子集 $P\in\mathcal{P}$中的用户，利用自己存储的秘密密钥和从 KMS 获取的公开密钥材料，计算出此特权用户子集 $P\in\mathcal{P}$的共享通信密钥；任何与特权用户子集不相交的禁止用户子集 $F\in\mathcal{F}$中的用户，得不到任何与子集 P 共享密钥有关的信息。

设用户 U_i 的秘密密钥用 S_i 表示。对每一个特权子集 $P\in\mathcal{P}$，设 K_P 是其共享的通信密钥，此密钥由 TA 事先根据某种算法设定；设 M_P 是特权子集 $P\in\mathcal{P}$中的用户计算共享密钥所需的公开密钥材料。对每个用户 $U_i\in P$，共享通信密钥 K_P 由 M_P 和 S_i 确定。

设随机变量 $\boldsymbol{S}_i$，$\boldsymbol{M}_P$，$\boldsymbol{K}_P$ 分别表示用户 U_i 的秘密密钥 S_i，公开密钥材料 M_P 和特权子集 P$\in\mathcal{P}$的内部通信密钥 K_P。以上 3 个随机变量的概率分布由 TA 根据 AKPS 的密钥预分配协议采用的算法确定，并假设通信密钥 K_P 从密钥空间 K 中随机选取，并服从均匀分布。利用以上定义和熵函数$H(\cdot)$，AKPS 定义如下：

$(\mathcal{P},\mathcal{F})$-非对称密钥预分配协议(简称为 $(\mathcal{P},\mathcal{F})$-AKPS)具有以下性质：

单独从用户的秘密密钥或者 KMS 存储的公开密钥信息得不到任何有关密钥 K_P 的信息，即对所有特权用户子集 $P\in\mathcal{P}$而言，

$$H(\boldsymbol{K}_P\mid\boldsymbol{S}_1\cdots\boldsymbol{S}_n)=H(\boldsymbol{K}_P\mid\boldsymbol{M}_{P_1}\cdots\boldsymbol{M}_{P_{|\mathcal{P}|}})=H(\boldsymbol{K}_P)$$

特权用户子集 P 中的每个用户 U_i，利用在密钥分配阶段获得的秘密密钥 S_i 和从 KMS 得到的公开密钥材料 M_P，能独立计算出特权用户子集 P 共享的通信密钥 K_P，即对所有用户 $U_i\in P$ 而言，

$$H(\boldsymbol{K}_P\mid\boldsymbol{S}_i\boldsymbol{M}_P)=0$$

任何与特权用户子集 P 不相交的禁止用户子集 F 中的用户，即使能得到所有属于特权子集 P 的公开密钥材料，也不能获得任何有关 K_P 的信息。即对所有 P$\in\mathcal{P}$，如果 $F\in\mathcal{F}$且 $P\bigcap F=\phi$，

$$H(\boldsymbol{K}_P\mid\boldsymbol{S}_F\boldsymbol{M}_{P_1}\cdots\boldsymbol{M}_{P_{|\mathcal{P}|}})=H(\boldsymbol{K}_P)$$

其中，$\boldsymbol{S}_F$ 表示子集 F 中所有用户的秘密密钥。读者可以参阅文献[7]来了解 AKPS 的熵界和构造方法。

3.2 Leighton-Micali 密钥协商协议

Leighton 和 Micali 在文献[8]中提出了不需要公钥密码操作的密钥协商方法。其中一种方法可以使通信双方通过使用一些公开信息，就能进行密钥的协商和建立。以下是所提协议的简要描述：

TA 随机产生两个主密钥 K 和 K'，并利用这两个主密钥为每个用户 U_i 生成密钥交换密钥(key exchange key) K_i 和认证密钥(individual authentication key) K_i'，使得

$$K_i=h(K,i),K_i'=h(K_i,i)$$

其中，$h(\cdot)$是单向 Hash 函数。

当用户 U_i 需要发送消息给用户 U_j 时，用户 U_i 首先向

TA 请求获得对密钥(pair key) P_{ij} 和认证密钥(authentication key) A_{ij}：

$$P_{ij}=h(K_i,j)\oplus h(K_j,i),A_{ij}=h(K_i',h(K_j,i))$$

然后，用户 U_j 可以计算出密钥 K_{ij}：$K_{ij}=P_{ij}\oplus h(K_i,j)=h(K_j,i)$，并验证密钥的真实性，即验证 $h(K_i',K_{ij})=A_{ij}$ 是否成立。

显然，用户 U_i 同样能得到密钥 K_{ij}，因为它有密钥 K_j，并且知道用户 U_i 的标识。所以，用户 U_j 能用此密钥解密消息。Leighton-Micali 协议可以扩展到采用多个主密钥。此时，敌手必需攻陷所有主密钥，才能获得网络的秘密信息。

3.3 mAKPS

本文主要目标是设计一个适用于 UWSN 的安全机制，能够为传感器节点分配通信密钥，且能限制移动 sink 的特权，当移动 sink 被敌手攻陷时，不会对网络造成很大的影响。在 mAKPS 中，移动 sink 被当作 AKPS 协议中移动的 KMS。在系统初始化时，每个传感器节点预先装载部分密钥信息(如 Lighton-Micali 协议中的用户密钥交换密钥和认证密钥)，传感器节点之间建立共享密钥所需的公开密钥信息(如 Leighton-Micali 协议中的 P_{ij} 等)保存在移动 sink 中。此后，网络管理者把已经初始化的移动 sink 派遣到网络中，执行密钥材料的分发和其它网络任务(如收集检测数据等)。如果两个相邻的传感器节点需要建立共享的通信密钥，两者之一可以向邻近路过的移动 sink 发出请求，获得所需的公开密钥材料。

当移动 sink 被派遣到网络中执行数据收集处理任务时，它的具体任务必需事先指定，即通过某种策略限制移动 sink 的特权。我们通过安全机制来实现安全策略，给派遣的移动 sink 赋予一定的特权，除能完成赋予的任务以外，移动 sink 不能做权利以外的工作。我们首先考虑一个简单的策略，假设移动 sink 沿着网络中指定的路径运动，它只被赋予访问指定路径上传感器节点的权利。

设 $\omega=\{1,2,\cdots,n+m\}$ 是网络中全部节点集合。集合 ω 中的节点分为两个子集，子集 $\mathscr{A}=\{1,2,\cdots,n\}$ 表示传感器节点集合，子集 $\mathscr{B}=\{n+1,\cdots,n+m\}$ 表示移动 sink 组成的集合。假设网络管理者 TA 已知移动 sink 在网络中行进的路径，并限制此移动 sink 的特权，使其只能访问指定路径沿途的传感器节点。

设集合 $\mathscr{C}=\{c_1,\cdots,c_j\}(1\leqslant c_1,\cdots,c_j\leqslant n)$ 是移动 sink 沿途的传感器节点，则它只能访问集合 $\mathscr{C}$ 中的节点，对于其它任何节点 $u\notin\mathscr{C}$，移动 sink 无权访问或操作。以下是 mAKPS 的初始化阶段：

初始化阶段：TA 选择一个安全的 Hash 函数 $h(\cdot)$，一个主密钥 K 和一个认证密钥 ${}^aK$(与 Lighton-Micali 协议类似)。对集合 ω 中的每个节点 $i\in\{1,2,\cdots,n+m\}$，TA 为其装入 Hash 函数 $h(\cdot)$ 以及秘密密钥 K_i 和 ${}^aK_i$。其中，$K_i=h(K|i)$，${}^aK_i=h({}^aK|i)$，$|$ 表示级联操作。

TA 产生公开密钥材料 $M_{ij}=(i,j,P_{ij},A_{ij},A_{ji})(i=1,\cdots,n,j=1,\cdots,n,i<j)$，其中 $P_{ij}=h(K_i|j)\oplus h(K_j|i)$，$A_{ij}=({}^aK_i|h(K_j|i))$，$A_{ji}=h({}^aK_j|h(K_i|j))$。TA 把产生的公开密钥材料 M_{ij} 装入移动 sink，用来为传感器节点之间建立通信密钥。

此后，TA 为移动 sink 构造密钥链 KR，用于移动 sink 访问指定集合 $\mathscr{C}=\{c_1,\cdots,c_j\}$ 中的传感器节点。假设移动 sink 的 ID 是 $v,v\in\mathscr{B}=\{n+1,\cdots,n+m\}$，移动 sink v 的密钥链为 $KR=\{P_{c_1},\cdots,P_{c_j}\}$，其中，$P_{c_j}$ 表示 (c_j,P_{v,c_j})，$c_j\in\mathscr{C}$，且 $P_{v,c_j}=h(K_v|c_j)\oplus h(K_{c_j}|v)$。

如果移动 sink 被授权访问集合 $\mathscr{C}$ 中的传感器节点，此移动 sink 在沿指定路径穿越网络时，执行密钥材料的分发和数据收集任务。具体操作如下：

密钥分发和计算：移动 sink v 广播 HELLO 消息(消息中包含节点的 ID v 和最大转发跳数 hop)，通知网络中的传感器节点移动 sink 的到来。如果传感器节点 i 收到此广播消息，首先执行 hop——，如果 $hop>0$，则继续转发收到的广播消息；否则，停止转发。节点 i 沿收到广播消息相反的路径，向移动 sink v 发送一个响应消息 $RESP(i)=(i,i_1,\cdots,i_t,\{i,R_i\}_{k_{i,v}})$，表示此传感器节点希望与它的邻居节点 $i_1,\cdots,i_t$ 建立通信密钥。在响应消息 $RESP(i)$ 中，R_i 是一个随机数，$k_{i,v}$ 采用以下方式计算得到 $k_{i,v}=h(K_i|v)$，$\{i,R_i\}_{k_{i,v}}$ 表示用密钥 $k_{i,v}$ 加密消息 i,R_i。

收到传感器节点的响应之后，移动 sink 查找保存的密钥链 KR，如果 $i\in\mathscr{C}$，表明移动 sink v 有权利访问传感器节点 i。此时，移动 sink 在其密钥链 KR 中找到 $P_i=(i,P_{v,i})$，计算 $k_{i,v}=P_{v,i}\oplus h(K_v|i)=h(K_i|v)$，并解密 $RESP(i)$ 消息，获取随机数 R_i。此后，移动 sink v 向传感器节点 i 发送查询消息 $Q_{(i)}$ 和节点 i 请求的公开密钥材料 $P_{(i)}$：

$$Q_{(i)}=(v,\{REQ,R_i\}_{k_{i,v}})$$

$$P_{(i)}=(M_{i,i_1},\cdots,M_{i,i_t})$$

其中，REQ 表示移动 sink 的任务描述(或者移动 sink 能够收集数据的种类、执行的操作等)，R_i 是节点 i 向移动 sink v 发送的响应消息 $RESP(i)$ 中附带的随机数，M_{i,i_t} 是节点 i 和它的邻居节点 i_t 之间建立通信密钥所需的公开密钥材料。如果 $i\notin\mathscr{C}$，则表明移动 sink v 无权访问传感器节点 i。在这种情况下，移动 sink v 只发送节点 i 请求的公开密钥材料 $P_{(i)}=(M_{i,i_1},\cdots,M_{i,i_t})$。

如果传感器节点 i 收到移动 sink v 的查询消息 $Q_{(i)}$，首先验证此消息，即验证消息中的随机数 R_i 是否等于节点发送的消息 $RESP(i)$ 中的随机数。如果相同，节点 i 则帮助移动 sink 完成 REQ 中定义的任务；否则，传感器节点丢弃此查询消息。

如果传感器节点 i 只收到来自移动 sink 的公开密钥材料 $P_{(i)}$，节点则根据 Lighton-Micali 协议，验证每个 M_{i,i_t} 是否正确，此后，与邻居节点 $i_1,\cdots,i_t$ 建立共享密钥。

3.4 安全和性能评估

安全性分析：mAKPS 是一个计算安全的 AKPS，其安全性依赖于 Hash 函数 $h(\cdot)$ 的安全强度。mAKPS 利用 Lighton-Micali 密钥协商协议作为其一个构成模块，继承了 Lighton-Micali 协议良好的特性，如果假设密码分析(或蛮力攻击)不可行，敌手无法窃听两个正常节点的通信，无论敌手攻陷多少个其它网络节点(传感器节点或者移动 sink)(读者可以参见文献[8]中 Lighton-Micali 协议的安全性证明)。

此外，mAKPS 协议也限制了移动 sink 的特权。移动 sink 只能访问由 TA 授权的传感器节点。移动 sink v 因为不知道主密钥 K 和 ${}^aK$，如果在它的密钥链 KR 中没有 $P_i=(i,P_{v,i})$，则移动 sink v 无法伪造一个合格的查询消息 $Q_{(i)}$，而此消息能被传感器节点 i 接受。

为进一步增强 mAKPS 的安全性能，可以采用多个主密钥 $K^1,\cdots,K^r$（和相应的认证密钥 ${}^aK^1\cdots,,{}^aK^r$）来保护网络。在这种情况下，敌手必需获得全部主密钥，才能攻陷整个网络。

存储代价：为分析简单，以下只考虑采用单个主密钥的情形。如文献[7]所述，如果采用计算安全的 AKPS，节点的存储开销很小。在 mAKPS 协议中，每个传感器节点（如节点 i）只需存储两个初始密钥值，大量的存储代价转移到移动 sink 中。协议 mAKPS 中的移动 sink（如移动 sink v）需要存储 3 部分密钥材料：两个密钥值（K_u 和 ${}^aK_u$），公开密钥材料 M_{ij}（$1\leqslant i,j\leqslant n$）（用于辅助传感器节点建立通信密钥）和一个密钥链 $KR 用于控制此移动 sink 的特权）。如果 mAKPS 协议需要为网络中任意传感器节点对提供公开密钥材料，对于一个包含 n 个传感器节点的网络，则需要保存 $\frac{1}{2}n(n-1)M_{ij}$。因此，第二部分存储开销为 $O(\frac{3}{2}n(n-1))$。根据前面 mAKPS 协议采用的移动 sink 特权限制策略，第三部分存储开销为 $O(j)$，其中，$j=|\mathscr{C}|=|\{c_1,\cdots,c_j\}|(1\leqslant c_j\leqslant n)$。这一部分存储开销因采用的不同特权限制策略而异。

以上 3 部分存储开销中，第二部分最大。为了减少移动 sink 的存储代价，TA 可以根据不同任务需求，给移动 sink 预存部分公开密钥材料，如 $\lambda\cdot\frac{1}{2}n(n-1)M_{ij}$（$0<\lambda\leqslant 1$）。因子 λ 越大，移动 sink 的存储开销越大，传感器节点之间能够建立共享密钥的概率越大；λ 越小，移动 sink 的存储开销越小，感器节点之间能够建立共享密钥的概率也相应减小。可以根据不同需求来选择适当值。

计算和通信代价：mAKPS 协议在密钥计算阶段只包含的 Hash 计算，且一对节点进行密钥协商时所需的 Hash 计算次数很少。mAKPS 协议中，传感器节点的计算代价较低。对于移动 sink 而言，计算代价除了进行 Hash 计算以外，还有一部分来源于在大量的公开密钥材料中查找节点请求的密钥材料。

节点的通信开销主要来源于与移动 sink 的通信，节点请求移动 sink 提供公开密钥材料，并接收移动 sink 的响应，或者为其它节点转发通信数据。在 mAKPS 中，移动 sink 只与附近的节点（2～3 跳范围内）通信，引入的通信代价不大。此外，传感器节点可以通过一次请求，获得与所有邻居节点建立共享密钥所需的密钥材料。

4 移动 sink 特权限制

为了能限制移动 sink 的特权，在协议中应使传感器节点能够验证移动 sink 被赋予的任务。以下提出 3 类策略，用于限制移动 sink 的访问特权。

4.1 基于传感器的特权限制

TA 如果知道移动 sink 的行进路线和沿途的传感器节点的位置信息，则可以限制移动 sink 的特权，使其只能访问（如收集检测数据等）这一部分传感器节点。如前面 mAKPS 协议所述，$\mathscr{C}=\{c_1,\cdots,c_j\}$ 表示移动 sink 被授权能够访问的传感器节点集合，对于任何不属于此集合的传感器节点，此移动 sink 都无权访问。

4.2 基于数据的特权限制

以上基于传感器的特权限制策略要求网络管理者（TA）具有网络全局的拓扑知识，而对于大型的传感器网络而言，TA 很难得到全局的网络拓扑信息。通常而言，传感器节点采集的环境数据可以分为不同的种类或等级（types or levels），一个授权的移动 sink 可以限制其只能访问某种（或部分）类型的节点检测数据。例如，如果 TA 希望能得到检测区域某种类型的数据（如温度或湿度等），则它可以派遣移动 sink 来负责采集网络中这些种类的数据，并限制移动 sink 的任务权利，使其只能获得规定类型的检测数据。

假设传感器节点的检测数据分为 s 种类型（或等级），$t_1,\cdots,t_s(t_i\leqslant t_{i+1})$。在初始化阶段，TA 选择一个 Hash 函数 $h(\cdot)$ 和一个主密钥 K^T。在部署前，TA 给每个节点，如节点 u，预存 Hash 函数 $h(\cdot)$ 和 s 个秘密值，$\{K_{t_i}^T=h(K^T|t_i)|i=1,\cdots,s\}$，每一个秘密值与传感器节点存储的数据类型相对应。

如果移动 sink v 被授权查询类型为 t_i 的检测数据，TA 给移动 sink v 一个密钥 $K_v^T=h(K^T|v)$ 和一个值 P_{v,t_i}，由 $h(K_v^T|t_i)\oplus h(K_{t_i}^T|v)$ 计算得到。

当移动 sink v 向传感器节点 i 发送查询消息 $Q_{(i)}$ 时（见 mAKPS 协议），$Q_{(i)}=(v,\{REQ,R_i\}k_{iv})$，其中的 REQ 字段由以下方式构造：

$$REQ=(t_i,\{t_i\}k_{v,t_i}^T)$$

其中，$k_{v,t_i}^T=P_{v,t_i}\oplus h(K_v^T|t_i)=h(K_{t_i}^t|v)$。

传感器节点 i 可以验证 REQ 的有效性，因为它拥有秘密值 $K_{t_i}^T$，能由此获得 K_{v,t_i}^T。

显然，此方法的安全性与 mAKPS 协议的安全性相同。移动 sink 因为不知道主密钥，无法仿造一个合法的 REQ 字段。

4.3 基于传感器与数据的特权限制

以上两种方法可以结合使用，为移动 sink 提供不同粒度的特权限制。移动 sink 可以被限制为只能访问存储在特定传感器节点中的特定类型的检测数据。例如，移动 sink v 只能收集特定传感器节点 u 中存储的特定类型的数据 $t_i(1\leqslant i\leqslant s)$。在这种情况下，TA 可以给传感器节点 u 预存秘密值 $\{K_{u,t_i}^T=h(K^T|u|t_i)|i=1,\cdots,s\}$。

当移动 sink v 被网络管理者授权查询传感器节点 u 中类型为 t_i 的检测数据时，网络管理者 TA 给移动 sink v 预存秘密值 $K_v^T=h(K^T|v)$ 和密钥材料。

$$P_{v,u,t_i}=h(K_v^T|u|t_i)\oplus h(K_{u,t_i}^T|v)$$

然后，当移动 sink v 发送查询消息 $Q_{(u)}$ 给传感器节点 u 时，查询消息 $Q(u)$ 中的 REQ 字段构造如下：

$$REQ=(u,t_i,\{u,t_i\}_{k_{v,u,t_i}^T})$$

其中，$k_{v,u,t_i}^T=P_{v,u,t_i}\oplus h(K_v^T|u|t_i)=h(K_{u,t_i}^T|v)$。

传感器节点 u 利用保存的秘密值 K_{u,t_i}^T，可以很容易计算得到 $k_{v,u,t_i}^T=h(K_{u,t_i}^T|v)$，验证 REQ 的合法性。

显而易见，此方法和 mAKPS 具有相同的安全特性，但对移动 sink 安全性的控制粒度更细。在存储开销方面，假设移动 sink 被授权访问 m 个传感器节点中存储的 t 类检测数据，则对移动 sink 而言，这部分额外的存储开销为 $O(m\times t)$。对普通传感器节点而言，如果传感器节点存储有 s 类数据，则需要的存储开销为 $O(s)$。

以上移动 sink 的特权限制机制可以扩展到任意数据属

（下转第 21 页）

TDMA 调度方案时，网络中每个节点在完成规定任务时的平均能耗和平均时隙。在多目标粒子群 Pareto 优化方法中，权重因子 W 取为 1.5，C_1、C_2 取为 2.0，微粒群的大小取为 40，最大进化代数取为 600。

从表 1 不难看出 PAPSO1 是时间性能上表现最好的，当然能量性能是 7 个解中最差的，而 PAPSO7 则是能量指标表现最突出的，同样其时间表现又是 7 者之中最次的。它们之间分布着其余 5 个解。

表 1　NBSA 算法和 PAPSO 算法的结果列表

算法	平均时隙(个)	平均能耗/(mJ)
NBSA	1.436	6.625
PAPSO1	1.056	6.567
PAPSO2	1.138	6.523
PAPSO3	1.195	6.480
PAPSO4	1.327	6.450
PAPSO5	1.519	6.425
PAPSO6	1.540	6.437
PAPSO7	1.796	6.427

由于这 7 个解的分布情况是均匀的，同时考虑到其均匀分布性质，选择 PAPSO4 的解作为双目标 f_1，f_2 的折中解。依 Pareto 优化概念对各算法的结果进行分析，显见，PAPSO(1—4)对 NBSA 构成支配。可见多目标粒子群 Pareto 优化方法能得到比 NBSA 更好的调度结果。

结束语　无线传感器网络中，需要利用数据融合技术来减少数据传输量，节省节点的能量，延长节点的生命周期。为降低融合过程中的时延和能量消耗，提出网络数据传输最短路径算法，并结合 Pareto 优化方法和搜索能力强的 PSO 算法，对集中式 TDMA 调度问题提出了 PSO-Pareto 优化方法，从而在信息传输的路径和每个节点完成规定任务所需的平均时隙、平均能耗两个方面论述了减少网络的时延和能耗，最大化了网络的生存周期和最小化了网络的延时。

参 考 文 献

[1] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. Wireless sensor networks[J]. Computer Networks, 2010, 38(4): 393-422

[2] Gungor V C, Lu Bin, Hancke G P. Opportunities and Challenges of Wireless Sensor Networks in Smart Grid[C]// IEEE Transactions on Industrial Electronics, VOL. 57, 2010: 3557-35-64

[3] Khedo K K, Perseedoss R, et al. A Wireless Sensor Network Air Pollution Monitoring System[J]. International Joural of Wireless & Mobile Networks(IJWMN), 2010, 15(5)

[4] 杜菲. 无线传感器网络中数据融合算法的研究[J]. 信息与电脑，2011，6：162-164

[5] 掌明. 基于最大生存周期的无线传感器网络能量模型研究[J]. 现代电子技术，2007，21：38-40

[6] Shih E, Cho S H, Ickes N, et al. Energy-efficient link layer for wireless microsensor networks[C]// Proc of the Workshop on VLSI 2001. Orlando, 2001: 16-21

[7] Ergen S C, Varaiya P. TDMA scheduling algorithms for sensor network[R]. Berkeley: Department of Electrical Engtineering and Computer Sciences, University of California, 1970

[8] Gandham S, Zhang Ying, Huang Qing-feng. Distributed minimal time convergecast scheduling in wireless sensor networks[C]// The 26th Int Conf Distributed Cmoputing Systems(ICDCS06). Lisboa, 1999

[9] Deb K. Evolutionary algorithms for multi criterion optimization in engineering Design[C]// Proc of Evolutionary Algorithms in Engineering and Computer Science (EUROGEN-99). John Wily&Sons, Chichester, 1999: 135-161

[10] 李闻，林亚平，童调生. 传感网络中一种基于蚂蚁算法的分布式数据汇集路由算法[J]. 小型微型计算机系统，2005，26(5)：788-792

(上接第 7 页)

性，如基于事件类型，或地理位置等。

结束语　传感器网络由于资源严格受到限制，很难处理好各种资源之间的关系，通常是在各种限制之间，根据传感器网络的应用需求，寻找一种适当的折中方法。本文针对 UWSN 和移动 sink 这种场景，提出密钥分发和移动 sink 特权限制协议 mAKPS。通过把大量的存储开销转移到功能较强的移动 sink 上，降低了普通传感器节点的存储要求。

参 考 文 献

[1] Chen Xiang-qian, Makki K, Yen Kang, et al. Sensor network security: a survey [J]. IEEE Communications Surveys & Tutorials, Second Quarter 2009, 11(2): 52-73

[2] Ma Di, Tsudik G. Extended abstract: Forward-secure sequential aggregate authentication[C]// IEEE Symposium on Security and Privacy, 2007. Berkeley, CA: IEEE, 2007: 86-91

[3] Di Pietro R, Mancini L V, Soriente C, et al. Catch me (if you can): Data survival in unattended sensor networks[C]// Sixth Annual IEEE International Conference on Pervasive Computing and Communications, PerCom' 08, 2008. Hong Kong: IEEE, 2008: 185-194

[4] Ma Di, Tsudik G. Dish: Distributed self-healing (in unattended sensor networks)[C]// SSS 2008, LNCS 5340, 2008. Berlin Heidelberg: Springer-Verlag, 2008: 47-62

[5] Rasheed A, Mahapatra R N. The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(5): 958-965

[6] Zhang Wen-sheng, Song Hui, Zhu Sen-cun, et al. Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks[C]// Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc' 05), 2005. New York, NY, USA: ACM, 2005: 378-389

[7] Liu Zhi-hong, Ma Jian-feng, Huang Qi-ping, et al. Asymmetric key pre-distribution scheme for sensor networks [J]. IEEE Transactions on Wireless Communications, 2009, 8(3): 1366-1372

[8] Leighton T, Micali S. Secret-key agreement without public-key cryptography[C]// Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology(CRYPTO' 93), 1993. London, UK: Springer-Verlag, 1993: 456-479