基于单向散列链的定点布设无线传感器网络密钥分配方案

覃荣华[1,2] 何亮明[2] 李宝清[1,2] 袁晓兵[1,2]
(中科院上海微系统与信息技术研究所微系统技术重点实验室 上海 200050)[1]
(中科院上海微系统与信息技术研究所无线传感器网络与通信重点实验室 上海 200050)[2]

摘 要 针对有重部署需求的定点布设无线传感器网络,提出基于单向散列链、支持身份认证的密钥分配方案。方案采用密钥链分段激活方式,可以有效抵制节点俘获攻击造成的安全威胁,安全性能好;支持节点重部署,从而可以保障有良好的网络覆盖率。

关键词 单向散列链,定点布设,节点重部署,密钥分配,无线传感器网络
中图法分类号 TP393 **文献标识码** A

Key Distribution Scheme in Designated Manually Deployed Wireless Sensor Networks Based on One-way Hash Chain

QIN Rong-hua[1,2] HE Liang-ming[2] LI Bao-qing[1,2] YUAN Xiao-bing[1,2]
(Science and Technology on Microsystem Laboratory, Shanghai Institute of Micro-system and Information Technology, Chinese Academic of Science, Shanghai 200050, China)[1]
(Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Micro-system and Information Technology, Chinese Academic of Science, Shanghai 200050, China)[2]

Abstract Aiming at the case of manually deployed wireless sensor networks(WSNs), we introduced a key distribution scheme based on one-way hash chain. By employing the mechanism of key chain partly activation, our scheme can effectively weaken the threat of node capture, be resilience against node replication or node forgery. Besides of good security properties, the scheme supports node redeployment and promises good network coverage rate.

Keywords One-way hash chain, Designated manually deployment, Node redeployment, Key distribution, Wireless sensor networks

1 引言

无线传感器网络(Wireless Sensor Networks, WSN)是由大量有信息感知能力的传感器节点构成的自组织网络。由于它常常应用在敏感任务场景,因此保障网络数据安全是WSN研究的一个很重要的问题。WSN本身的一些独有特点,使其密钥管理方案的设计遇到更多新的困难与挑战[1]。

将位置信息作为密钥素材的一部分,可以更有效地应对节点俘获攻击,特别是选择性节点俘获攻击[2-5]。尽管随机布设方式提供了更好的网络部署便利性,定点布设仍然在很多实际应用中占据一席之地[6,7]。在无线传感器网络的一些应用中,比如说停车场车位监控系统、防入侵围界等,节点可以手工布设或者借助机器人进行布设。这些应用的网络系统运行周期一般较长,节点死亡、失效以及被俘等原因会导致网络覆盖率变差,从而需要进行节点重部署。本文针对定点布设WSN场景,设计安全高效的支持节点重部署的网络密钥管理方案。

本文第2节提出定点布设WSN的典型应用及其密钥管理的需求特点;第3节为研究进展;第4、5节为网络模型假设、相关策略及密钥分发方法的介绍;第6节分析方案的效率与性能;最后总结全文。

2 典型应用场景与需求特点

2.1 定点布设WSN的典型应用场景

本文主要针对长时期使用的定点布设无线传感器网络进行密钥分配方案的设计,以下列举4种相关的定点布设应用场景。

场景A:建筑物监控(见图1) 智能家居使用WSN可以实现房子及周边相关感知因素的监测,也可以对家用电器进行智能控制。建筑物安全指标的监测最常见的是对大桥、高架、高楼和隧道等建筑物关于安全使用情况及寿命等的监测。在这些应用中,节点布设通常也需要针对特定监测点进行。

场景B:公路及轨道监测(见图2) 对于公路、轨道的监测是非常重要的。在关键位置或事故多发路段,有效的监测

到稿日期:2012-03-12 返修日期:2012-05-27 本文受国家重点基础研究发展计划(2011CB302906)资助。
覃荣华(1985—),男,博士生,主要研究方向为无线传感网密钥管理,E-mail:qinronghua07@mails.gucas.ac.cn;**何亮明**(1984—),男,博士生,主要研究方向为多媒体无线传感网与数据处理;**李宝清**(1972—),男,博士,研究员,主要研究方向为无线传感网与数据处理;**袁晓兵**(1969—),男,博士,研究员,主要研究方向为无线传感网与通信系统。

可以减小交通事故的发生，也可以优化交通环境。

场景C：停车场车位监测（见图3） 停车场管理系统一方面用于提醒车主空余车位情况及路线导航；另一方面方便管理整个停车场的具体使用情况。使用无线传感器网节点对各个车位上是否已在使用进行实时感知并周期性地上报汇总，对于停车场车位管理系统的设计将是重大的优化。

场景D：防入侵围界监测（见图4） 防入侵围界系统应用在国防边防、机场围界以及敏感区域的围栏系统中。使用WSN进行防入侵围界系统的设计，可以有效地利用无线传输的优势及节点部署方便的特点，大大降低系统部署与维护的成本。围界长度较长的场景下，WSN尤其显得一枝独秀。

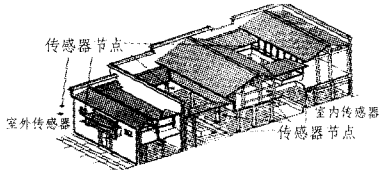

图1 建筑物监控场景示意图

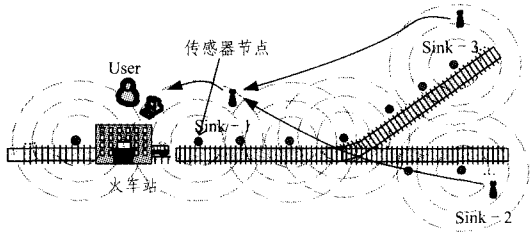

图2 铁道线监测场景示意图

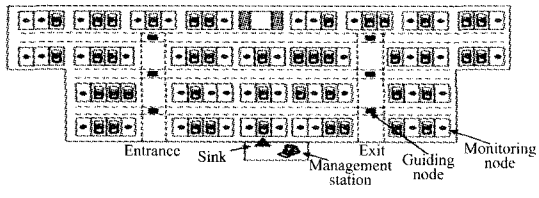

图3 停车场车位监控场景示意图

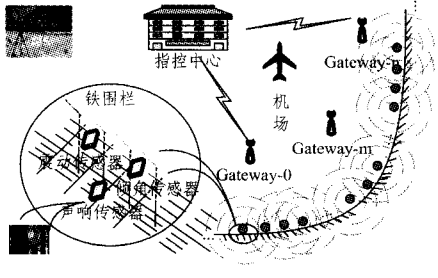

图4 防入侵围界场景示意图

2.2 密钥管理的需求特点

纵然定点布设WSN的应用场景涉及的监测区域相对不那么敌对，甚至可能允许定期维护，但仍然可能出现节点俘获/妥协攻击。通过相关措施保障密钥素材的安全很有必要。

节点重部署或多次部署是保障长周期运作的网络系统监测覆盖的必要手段。针对重部署，进行密钥素材的相关处理以防止有效素材的泄露，进行节点身份认证以防止节点复制/伪造攻击，至关重要。

3 相关研究进展与单向散列链

3.1 相关研究进展

无线传感器网络密钥管理方案至今已有不少的研究成果。其中大部分很有应用价值，但通常也有各自的不足，随机密钥分配方案RKP就是其中之一[8]。针对RKP方案的不足，后续有不少的改进方案被提出，比如q-composite/多路径增强[9]、RKP-H[10]等。q-composite/多路径增强通过邻居节点间的协作强化安全性能的弹性。RKP-H通过对EG密钥池提取密钥哈希的简单处理，达到更好的网络安全性，减小节点俘获攻击的密钥素材丢失的安全威胁。另外，还有基于多项式共享[11]、基于矩阵[12]、结合使用部署知识[13]等密钥方案。综述文章对这些方案进行了总结[14]。

文献[14]特别指出，将部署知识方法与已有方法进行结合可以形成诸多高效安全方案，使得密钥素材存储空间变小、网络连通度变大等等。定点布设是更加精确地使用部署知识的网络部署方法。目前，有关定点布设WSN密钥分配方案已有不少文献支撑。但它们或者设计在较强的系统假设下，或者有应用限制，大部分在真实环境下不实用[7]。

3.2 单向散列链简介

迭代使用单向散列函数形成的散列序列构成单向散列链，结构如图5所示。

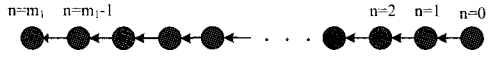

图5 后向散列链结构示意图

该散列链满足函数关系：

$Hash(BHC(k))=BHC(k+1)$

其中，$Hash()$表示单向散列函数，BHC表示后向单向散列链。

4 相关模型假设及相关策略

4.1 网络模型

将每个节点所在的特定区域称为Cell，每个Cell中布设一个节点。假设网络部署区域可以分为N个Cell，每个Cell可以进行有效通信的邻居Cell个数最大值为M。整个网络的生命周期内，同一个Cell中节点重部署次数不超过m_1。节点有效的生命周期中，支持邻居Cell中节点重部署次数最大为m_2（其中$m_1>m_2$）。正在布设的节点称为部署节点，邻居Cell中节点称为邻居节点。部署管理节点资源非常丰富并且是安全的，可以通过GPS或者其他定位技术进行地理位置定位[7]，用于辅助节点布设，并负责整个网络的管理。

4.2 密钥池的形成及网络拓扑构建

方案使用的相关符号表示如表1所列。密钥池创建及网络拓扑规划均由部署管理节点负责完成，具体过程如下。

表1 相关的符号表示及其意义描述

Notation	Description
$Cell_i$	Id为i的Cell
BHC_{id}	用于节点身份认证，节点的Id认证链
$BHC_i\langle k\rangle$	Id为i的Cell对应的BHC_{id}，对应于$Cell_i$第k次重部署节点的Id
BHC_{ij}	$Cell_i$的密钥单元，邻居$Cell_j$重部署时以分段形式分配给节点
$BHC_{ij}\langle k\rangle$	BHC_{ij}中的第k个序列值
$BHC_{ij}\langle(m_1-k)m_2,(m_1-k+1)m_2-1\rangle$	$Cell_j$中第k次部署的节点分配得到BHC_{ij}的激活片段

a. 生成$(M+1)N$个随机数作为种子。选取其中N个生成长度为m_1的散列链BHC_{id}，另外MN个种子生成长度为m_1*m_2的散列链BHC。以1个BHC_{id}与M个BHC作为一

个密钥单元，从而得到 N 个密钥单元的密钥池。

b. 建立 N 个 Cell 的网络拓扑结构，给每个 Cell 分配 Id。随机给每个 Cell 分配一个密钥单元，并以该 Cell 的 Id 作为其密钥单元的 Id(与 BHC_{id} 相对应)。

4.3 身份认证策略

本方案利用散列链的单向性设计节点的身份认证。在节点的预部署阶段，部署管理节点给部署节点分配对应 Cell 的 BHC_{id} 最新未使用序列值作为该节点 Id。在节点重部署阶段，部署节点需要公布其 Id，邻居节点检验其合法性。以 $Cell_i$ 的第 k 次重部署为例，部署管理节点分配给部署节点身份序列值 $BHC_i\langle m_1-k\rangle$，邻居节点保存着 $BHC_i\langle m_1-k+1\rangle$。在 $Cell_i$ 的重部署阶段，部署节点公布身份认证序列值 $BHC_i\langle m_1-k\rangle$，邻居节点通过检验 $Hash(BHC_i\langle m_1-k\rangle)=BHC_i\langle m_1-k+1\rangle$ 是否成立来验证部署节点的身份合法性。

4.4 密钥分配策略

各 BHC 分段激活使用，部署管理节点负责对所有 Cell 的密钥单元使用状态进行管理。若 $Cell_x$ 为 $Cell_i$ 的邻居网格，$Cell_i$ 中第 k_1 次节点重部署时分配得到 $BHC_{xi}\langle(m_1-k_1)m_2,(m_1-k_1+1)m_2-1\rangle$。实际应用中，部署管理节点只需向 $Cell_i$ 的部署节点分配激活片段的第一个序列值，即 $BHC_{xi}\langle(m_1-k_1)m_2\rangle$。

部署节点需要与邻居 $Cell_x$ 中节点建立对密钥，该对密钥值取值于邻居 $Cell_x$ 中节点存储着的激活片段 BHC_{ix} 中的一个最新未使用序列值。部署节点在其预部署阶段由部署管理节点分配得到该对密钥值。在节点部署阶段，邻居节点通过认证部署节点所需散列运算的次数来确定对密钥值在激活片段中的位置，以该位置的序列值作为两者间的对密钥。

设 $Cell_j$ 为 $Cell_i$ 的邻居，$Cell_j$ 进行着第 k_2 次节点重部署，$Cell_i$ 中目前在网节点是第 k_1 次重部署节点，且在该节点生命周期中已经历过一次 $Cell_j$ 的节点重部署事件。则 $Cell_j$ 的部署节点分配到的对密钥素材如图 6(a)中圈出来的部分所示，包括激活的片段 $BHC_{ij}\langle(m_1-k_2)m_2,(m_1-k_2+1)m_2-1\rangle$ 和对密钥 $BHC_{ji}\langle(m_1-k_1+1)m_2-2\rangle$，使用 $BHC_{ji}\langle(m_1-k_1+1)m_2-2\rangle$ 作为二者的对密钥。图 6(b)表示在 $Cell_j$ 中再次出现节点重部署事件，使用 $BHC_{ji}\langle(m_1-k_1+1)m_2-3\rangle$ 作为二者的对密钥，$Cell_j$ 的 BHC_{ij} 有效片段更新为 $BHC_{ij}\langle(m_1-k_2-1)m_2,(m_1-k_2)m_2-1\rangle$。图 6(c)表示在 $Cell_i$ 中出现节点重部署事件，使用 $BHC_{ij}\langle(m_1-k_2)m_2-1\rangle$ 作为对密钥，同时 $Cell_i$ 的 BHC_{ji} 片段更新为 $BHC_{ji}\langle(m_1-k_1-1)m_2,(m_1-k_1)m_2-1\rangle$。

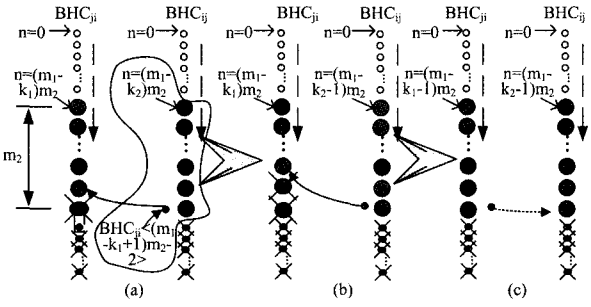

图 6 $Cell_i$ 与邻居 $Cell_j$ 密钥分配策略

下面以 $Cell_i$ 与 $Cell_j$ 为例，分析 $Cell_i$ 节点被俘对安全造成的影响。一方面，$Cell_i$ 中节点被俘，则节点从网络中掉线，重新加入网络通信则需要重新入网。但被俘节点在其部署完成后，所拥有的认证链序列值已经失效。因此，由于身份认证机制，被俘节点无法重新入网。另一方面，$Cell_i$ 中节点被俘获，则 $BHC_{ji}\langle(m_1-k_1)m_2,(m_1-k_1+1)m_2-1\rangle$ 被泄露。

若 $Cell_i$ 与 $Cell_j$ 中都没有发生重部署事件，$Cell_j$ 由于 $Cell_i$ 中节点失效，不会进行通信。

若 $Cell_i$ 与 $Cell_j$ 依次发生重部署事件，则在 $Cell_i$ 完成重部署而 $Cell_j$ 尚未重部署的情形下，$Cell_i$ 中新节点与 $Cell_j$ 按照密钥分配协议应该以 $BHC_{ij}\langle(m_1-k_2+1)m_2-1\rangle$ 作为对密钥(如图 7(b)所示)，该序列值不存在于泄露素材中。而当 $Cell_j$ 也完成重部署后，$Cell_i$ 与 $Cell_j$ 中节点之间应该以 $BHC_{ji}\langle(m_1-k_1)m_2-1\rangle$ 作为对密钥(如图 7(c)所示)，该序列值不存在于泄露的素材中。

若 $Cell_j$ 与 $Cell_i$ 依次发生重部署事件，则在 $Cell_j$ 完成重部署而 $Cell_i$ 尚未重部署的情形下，$Cell_j$ 认为 $Cell_i$ 中节点失效，不会与之进行数据通信(如图 7(d)所示)。而当 $Cell_i$ 也完成重部署后，$Cell_i$ 与 $Cell_j$ 中节点之间以 $BHC_{ij}\langle(m_1-k_2)m_2-1\rangle$ 作为对密钥(如图 7(e)所示)，该序列值不存在于泄露素材中。

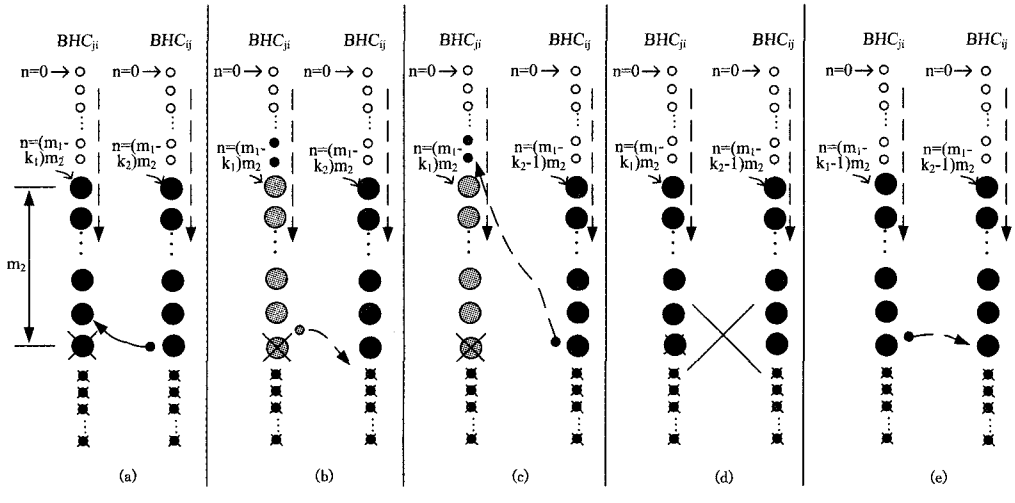

图 7 $Cell_i$ 中节点被俘对邻居 $Cell_j$ 对密钥素材的影响

可见，节点被俘所导致的密钥素材泄露对网络通信安全不构成影响。

5 部署节点的密钥分发方法

本方案中，节点布设的流程分为两个阶段：节点预部署阶段和节点部署阶段。以 $Cell_i$ 的第 k 次重部署为例，设邻居 $Cell_x$ 的下一次重部署为第 k_x 次，具体如下。

5.1 节点预部署阶段

在此阶段，部署节点与部署管理节点间的通信以离线下载方式进行。主要实现部署管理节点给部署节点分发认证和密钥素材，包括 4 部分素材：

material:a　节点 Id:$BHC_i\langle m_1-k\rangle$，用于身份认证。

material:b　邻居节点 Id，用于对邻居 Cell 重部署节点进行身份认证。

material:c　邻居 Cell 对应的 BHC_{xi} 最新激活片段的首部序列值 $BHC_{xi}\langle(m_1-k)m_2\rangle$。

material:d　与在网邻居节点建立的对密钥，以及该序列值在 $BHC_{ix}\langle(m_1-k_x)m_2,(m_1-k_x+1)m_2-1\rangle$ 中的对应位置。

5.2 节点部署或重部署阶段

该阶段实现节点部署时与邻居节点进行身份认证及对密钥建立。部署节点向邻居节点广播图 8 所示的消息报文，其中 $Cell_{id}$ 为部署节点对应的网格号，$BHC_i\langle m_1-k\rangle$ 为部署节点的 Id，MAC 表示消息认证码。包括 4 个步骤：

a. 在网邻居节点提取 $BHC_i\langle m_1-k\rangle$，认证当前部署节点的身份。

b. 若通过认证，邻居节点将 $BHC_i\langle m_1-k+1\rangle$ 更新为 $BHC_i\langle m_1-k\rangle$。

c. 部署节点直接使用预分配得到的与邻居节点的对密钥作为相互间的对密钥。

d. 邻居 $Cell_x$ 中在网节点根据认证所需散列运算次数确定对应的对密钥值在激活片段 $BHC_{ix}\langle(m_1-k)m_2,(m_1-k+1)m_2-1\rangle$ 中的位置，使用该序列值作为二者对密钥。

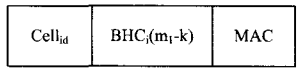

图 8　部署广播消息结构图

6 效率与性能分析

6.1 效率分析

a. 存储开销：部署节点需要保存的内容包括邻居节点 Id、入网时与各邻居使用的对密钥值和各邻居的密钥链激活片段。最多有 M 个邻居，共需要 $3M\times\lg q$ 的存储空间（q 为散列函数值域的阶次）。

b. 计算开销：布设节点时，在网邻居节点需要计算与部署节点的对密钥。每个对密钥的计算需要不多于 m_2 次散列运算。散列运算的开销很小，可以忽略不计。

c. 通信开销：设网格号的字长为 2 个字节，则本方案在布设节点时，部署节点广播消息报文的开销为 $2\lg q+2$ 字节。

6.2 安全分析

本方案在安全性能上有 3 方面的突出优势：首先，通过使用 BHC_{id} 提供高强度的身份认证机制，杜绝非法节点加入网络。其次，邻居节点间对密钥的建立，不进行密钥素材的直接信息交换，充分保障密钥素材的安全。最后，节点俘获攻击导致密钥素材信息的泄露，无法对网络造成安全威胁。

从信息论角度，分析节点俘获攻击的影响。$Cell_j$ 是 $Cell_i$ 的邻居，$Cell_j$ 中当前在网节点为第 $k_{j,t\Delta}$ 次重部署节点，且该节点经历了 $Cell_i$ 中 $0\leqslant\delta<m_2$ 次重部署行为。设 $t\triangledown>t\Delta$，用 $X_{i,k_{i,t\Delta},t\Delta}$ 表示 $t\Delta$ 时刻 $Cell_i$ 中节点是第 $k_{i,t\Delta}$ 次重部署节点的密钥素材。泄露的素材包括 4 个部分，即：

$$X_{i,k_{i,t\Delta},t\Delta}=\begin{cases}\langle1\rangle\{BHC_i\langle m_1-k_{i,t\Delta}\rangle\}=\{\text{material:}a\}\\ \langle2\rangle\{BHC_j\langle m_1-k_{j,t\Delta}\rangle\}=\{\text{material:}b\}\\ \langle3\rangle\{BHC_{ji}\langle(m_1-k_{i,t\Delta})m_2,(m_1-k_{i,t\Delta}+1)m_2-1\rangle\}=\\ \quad\{\text{material:}c\}\\ \langle4\rangle\{BHC_{ij}\langle(m_1-k_{j,t\Delta}+1)m_2-\delta-1\rangle\}=\{\text{material:}d\}\end{cases}$$

一方面，对于 $Cell_i$ 中后续重部署节点，由于散列函数的单向性，$Cell_i$ 中第 $k_{i,t\Delta}$ 次重部署节点对于第 $k_{i,t\triangledown}$ 次重部署节点的密钥素材没有信息知识，即 $H(X_{i,k_{i,t\triangledown},t\triangledown}\mid X_{i,k_{i,t\Delta},t\Delta})=H(X_{i,k_{i,t\triangledown},t\triangledown})$。

所以，被俘节点所泄露的密钥素材对 $Cell_i$ 中后续重部署节点密钥素材的信息量为零。

另一方面，由于 $Cell_i$ 与 $Cell_j$ 的密钥素材有一定关联性，需要分析 $X_{i,k_{i,t\Delta},t\Delta}$ 对 $Cell_j$ 认证及生效对密钥的影响：

(1)假设 $t\Delta\sim t\triangledown$ 间 $Cell_i$ 先发生了 σ 次重部署，然后 $Cell_j$ 才发生重部署。

在 $Cell_i$ 完成重部署而 $Cell_j$ 未发生重部署的情况下，对于 $Cell_j$，只涉及与 $Cell_i$ 建立的对密钥，即$\{BHC_{ij}\langle(m_1-k_{j,t\Delta}+1)m_2-\delta-\sigma-1\rangle\}$。而 $H(\{BHC_{ij}\langle(m_1-k_{j,t\Delta}+1)m_2-\delta-\sigma-1\rangle\}\mid X_{i,k_{i,t\Delta},t\Delta})=H(\{BHC_{ij}\langle(m_1-k_{j,t\Delta}+1)m_2-\delta-\sigma-1\rangle\})$，可见在这种情况下，泄露素材对于 $Cell_j$ 的对密钥建立信息量为零。

在 $Cell_i$ 完成重部署，$Cell_j$ 也完成重部署的情况下，对于 $Cell_j$，涉及身份认证和与 $Cell_i$ 建立的对密钥，即$\{BHC_j\langle m_1-k_{j,t\triangledown}\rangle\}$和$\{BHC_{ji}\langle(m_1-k_{i,t\triangledown}+1)m_2-1\rangle\}$。又因 $BHC_j\langle m_1-k_{j,t\triangledown}\rangle=BHC_j\langle m_1-k_{j,t\Delta}-1\rangle$，则 $BHC_{ji}\langle(m_1-k_{i,t\triangledown}+1)m_2-1\rangle=BHC_{ji}\langle(m_1-k_{i,t\Delta}-\delta-\sigma+1)m_2-1\rangle$。

易见，在这种情况下，泄露素材对于 $Cell_j$ 的对密钥建立信息量为零。

(2)假设 $t\Delta\sim t\triangledown$ 间 $Cell_j$ 先发生了 σ 次重部署，然后 $Cell_i$ 才发生重部署。

在 $Cell_j$ 完成重部署，$Cell_i$ 未发生重部署的情况下，$Cell_j$ 不与 $Cell_i$ 进行通信，泄露的素材没有任何效用。

在 $Cell_j$ 完成重部署，$Cell_i$ 也完成重部署的情况下，对于 $Cell_j$，涉及身份认证和与 $Cell_i$ 建立的对密钥，即$\{BHC_j\langle m_1-k_{j,t\triangledown}\rangle\}$和$\{BHC_{ij}\langle(m_1-k_{j,t\triangledown}+1)m_2-1\rangle\}$。又因 $BHC_j\langle m_1-k_{j,t\triangledown}\rangle=BHC_j\langle m_1-k_{j,t\Delta}-\sigma\rangle$，则 $BHC_{ij}\langle(m_1-k_{j,t\triangledown}+1)m_2-1\rangle=BHC_{ij}\langle(m_1-k_{j,t\Delta})m_2-1\rangle$。

易见，在这种情况下，泄露素材对于 $Cell_j$ 的对密钥建立信息量为零。

综上所述，节点被俘攻击无法威胁到本方案的网络安全。

结束语　本文针对定点布设的无线传感器网络，着眼于节点俘获攻击，提出基于单向散列链密钥管理方案。本方案支持节点重部署，具有良好的网络扩展性；提供身份认证，保障在网节点的合法性；进行密钥分配所需要的资源开销较小。本文方案对于定点布设的无线传感器网络密钥分配方案设计

（下转第 67 页）

San Antonio: IEEE Communications Society, 2001: 2926-2931

[5] Nicolescu D, Nath B. DV based positioning in ad hoc networks [J]. Journal of Telecommunication Systems, 2003, 22(1-4): 267-280

[6] Ji Wei-wei, Liu Zhong. Study on the application of DV-Hoplocalization algorithms in random sensor networks [J]. Journal of Electronics & Information Technology, 2008, 30(4): 970-974

[7] Chen Dai, Wang Wei, Zhou Yong. An Improved DV-Hop Localization Algorithm in Wireless Sensor Networks[C]// 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering (CCTAE 2010). Volume 2, School of Computer Science China University of Mining and Technology. Xuzhou, China, 2010

[8] Lin Jin-zhao, Chen Xiao-bing, Liu Hai-bo. Iterative algorithm for locating nodes in WSN based on modifying average hopping distances[J]. Journal on Communications, 2009, 30(10): 107-113

[9] Zhu Min, Liu Hao-lin, Zhang Zhi-hong, et al. An improved localization algorithm based on DV-HOP in WSN[J]. Journal of Sichuan University (Engineering Science Edition), 2012, 44(1): 93-98

[10] Liu Yan-heng, Liu Bing-ri, Sun Da-yang, et al. Improved DV-Hop algorithm in localization accuracy in WSN[J]. Journal of Jilin University: Engineering and Technology Edition, 2010, 40(3): 763-768

[11] Liu Yan-wen, Wang Fu-bao, Duan Wei-jun, et al. A localization system based on DV-Hop localizationalgorithm and RSSI ranging technique[J]. Journal of Coumputer Applications, 2007, 27(3): 516-518

[12] Li Rui-xue, Fang Zhi-yi, Yi Ting-ting. Improved DV-Hop localization algorithm based on regularly moving anchor(RMAN) and received signal strength indicator(RSSI) and its performance analysis[J]. Journal of Jilin Uiversity: EngineeringandTeehnologyEdition, 2011, 41(2): 435-441

[13] 赵虹，孙光，秦姣华，等. 夹角修正的 DV-hop 传感器网络节点定位研究[J]. 计算机工程与应用，2009，45(13)：100-102

[14] Chen Hong-yang, Sezaki K, Deng Ping, et al. An improved DV-Hop localization algorithm for wireless sensor networks[C]// Proc of the 3rd IEEE Conference on Industrial Electronics and Applications(ICIEA). Singapore: IEEE, 2008: 1557-1561

[15] Chan Y T, Ho K C. A simple and efficient estimator for hyperbolic location [J]. IEEE Transactions on Signal Processing, 1994, 42(8): 1905-1915

[16] Arias J, Lazaro J, Astarloa A. Location algorithm for wireless sensor networks in industrial applications [C]// IEEE International Conference on Industrial Technology (ICIT). Vol. 2, Hammamet (Túnez), 2004: 757-762

[17] 田金鹏，施惠昌. 无线传感器网络节点定位改进算法[J]. 上海大学学报：自然科学版，2009，15(3)：225-229

[18] Spec: Smartdust chip with integrated RF communications[OL]. http://www.jlhlabs.com/jhill_cs/spec/, 2001

(上接第 44 页)

很有吸引力。

参 考 文 献

[1] Chen Chi-yuan, Chao H-C. A survey of key distribution in wireless sensor networks [J]. Security and Communication Networks, 2011, doi: 10.1002/sec.354

[2] Huang D, Mehta M, Medhi D, et al. Location-aware Key Management Scheme for Wireless Sensor Networks [C] // Proc. SASN'04. Washington, DC, USA, 2004: 29-42

[3] Younis M F, Ghumman K, Eltoweissy M. Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks[J]. IEEE Transactions on parallel and distributed systems, 2006, 17(8): 865-882

[4] Liu Fang, Rivera M J, Cheng Xiu-zhen. Location-aware Key Establishment in Wireless Sensor Networks[C]// Proc. IWCMC'06. British Columbia, Canada, 2006: 21-26

[5] Ren Kui, Lou Wen-jing, Zhang Yan-chao. LEDS: Providing Location-aware End-to-end Data Security in Wireless Sensor Networks[C]// Proc. INFOCOM. 2006: 1-12

[6] Stoleru R, He T, Stankovic J. Walking GPS: A practical solution for localization in manually deployed wireless sensor networks [C]// Proc. 29th Annual IEEE International Conference on Local Computer Networks. Tampa, Florida, USA, 2004: 480-489

[7] Mi Q, Stankovic J, Stoleru R. Secure Walking GPS: A secure localization and key distribution scheme for wireless sensor networks[C] // Proc. the third ACM conference on wireless network security (WiSec'10). Hoboken, New Jersey, USA, 2010: 163-168

[8] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks[C] // Proc. the 9th ACM Conference on Computer and Communication Security. Washington, DC, USA, 2003: 41-47

[9] Chan H, Perrig A, Song D. Random key pre-distribution schemes for sensor networks[C]// Proc. the 2003 IEEE Symposium on Security and Privacy. Berkeley, CA, USA, 2003: 197-213

[10] Shan T, Liu C. Enhancing the key pre-distribution scheme on wireless sensor networks[C]// Proc. the 3rd IEEE Asia-Pacific Conference on Services Computing. Yilan, Taiwan, China: IEEE Computer Society, 2008: 1127-1131

[11] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks[C] // Proc. the 10th ACM Conference on Computer and Communication Security. Washington, DC, USA, 2003: 52-61

[12] Du W, Deng J, Han Y, et al. A pairwise key pre-distribution scheme for wireless sensor networks[C]// Proc. the 10th ACM Conference on Computer and Communication Security. Washington, DC, USA, 2003: 42-51

[13] Du W, Deng J, et al. A key management scheme for wireless sensor networks using deployment knowledge[C]// Proc. the 23rd Annual Joint Conference of the IEEE Computer and Communication Societies. Hong Kong, China, 2004: 586-597

[14] Jr M A S, Barreto P S, et al. A survey on key management mechanisms for distributed Wireless Sensor Networks[J]. The International Journal of Computer and Telecommunications Networking, 2010, 54(15): 2591-2612