doi:10.11959/j.issn.1000-436x.2015153

基于分布式密钥共享的 UWSN 安全分簇方案

仲红[1,2]，张庆阳[1,2]，田立超[1,2]，王良民[1,2]
(1. 安徽大学 信息保障技术协同创新中心，安徽 合肥 230601；2. 安徽大学 计算机科学与技术学院，安徽 合肥 230601)

摘 要：针对无照料的无线传感网（UWSN, unattended wireless sensor network）收集效率和安全问题，提出一种安全的 UWSN 分簇方案，实现了一种三角形网格图的网络拓扑分簇算法，并可完成簇头对移动节点的认证。该方案利用三角形的性质提高了网络的连通度，折中数据收集效率与能耗；将分布式密钥共享方案与分簇算法无缝结合，在网络中高效地搜索移动节点公钥信息，从而在本地不存有对应公钥信息的情况下验证签名信息。实验结果表明，该算法在节点密度越大的情况下分簇越趋近于正三角形网格图，且分簇后的网络对于低于 20%节点变节有 95%以上概率抵御攻击。

关键词：无照料的无线传感网；移动汇聚节点；分簇算法；分布式密钥共享
中图分类号：TP393.0 **文献标识码**：A

Distributed key sharing based scheme for security clustering in unattended wireless sensor network

ZHONG Hong[1,2], ZHANG Qing-yang[1,2], TIAN Li-chao[1,2], WANG Liang-min[1,2]
(1. Center of Information Support and Assurance Research, Anhui University, Hefei 230601, China;
2. School of Computer Science and Technology, Anhui University, Hefei 230601, China)

Abstract: For unattended wireless sensor network (UWSN), considering the collecting and efficiency and security problems, a secure clustering scheme for UWSN was proposed, which implements a clustering algorithm with the secure authentication of mobile nodes. The clustering algorithm uses triangle's characteristic to improve connectivity, balances collect efficiency and power consumption. The distributed key sharing scheme is used to improve the security of the clustering algorithm, in which mobile node's public key is able to be searched with high efficiency in the distributed static nodes, and the signature of mobile nodes will be checked by using the searched public key. Simulation results show that the clustering algorithm is tend to triangular meshes when node density is increasing, and more than 95% attacks are tolerated when compromised nodes are less than 20%.

Key words: unattended wireless sensor network; mobile sinks; clustering algorithm; distributed key sharing

1 引言

无照料的无线传感器网络(UWSN, unattended wireless sensor network) 包含三类节点：静态节点、移动节点及基站。静态节点分布在监控区域采集并存储数据信息，基站定期或不定期地派出移动节点，充当汇聚节点，收集静态节点所感知的信息数据[1~3]。UWSN 网络结构如图 1 所示，它与普通无线传感网络的区别在于基站不能一直在线的照料静态节点，即静态节点不能主动地发送消息联系基站，需要等待移动节点周期性或者非周期性的访问。这样自然带来 2 个问题：一个是效率问题，移动节点逐个访问静态节点，无疑是耗时耗能低效的；另一个是安全问题，静态节点如何认证移动节点，即如何判断移动节点是基站派出还是敌手派出。

收稿日期：2014-07-16；**修回日期**：2014-09-15
基金项目：国家自然科学基金资助项目（61173188，61272074）；安徽省科技计划基金资助项目（1401B042015）
Foundation Items: The National Natural Science Foundation of China (61173188, 61272074); The Science and Technology Plan of Anhui Province (1401B042015)

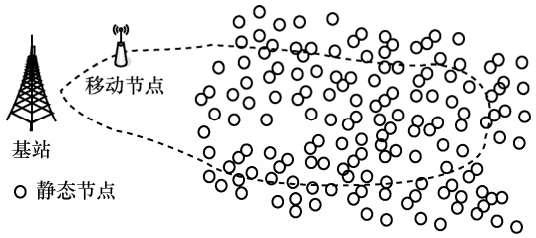


图 1 UWSN 模型

针对效率问题，当前研究常用分簇方法解决，即将静态节点分为若干感知子区域，每个子区域选举一个簇头，簇头提前收集该区域内的感知信息。这样移动节点只要访问簇头，就可以提取全部需求信息，大大提高收集的效率。这类方法中，以基于 Voronoi 图的区域划分方法为代表，其中最为典型的算法如 LEACH[4]和 HEED[5]，分别适用于单跳网络和多跳网络。

但是，上述分簇方法通常是针对传统无线传感网的，而不能直接应用到 UWSN 中。不能应用的最主要原因是没有一个在线的基站，节点与节点、节点与移动节点之间的信任关系无法建立，尤其是在分簇及数据采集阶段。这样网络结构导致安全发生了变化。目前，关于 UWSN 安全常用的方法是假设移动节点是绝对可信的[6,7]。

在实际中，移动节点也可能由敌手派出，故 UWSN 需要对移动节点进行认证。本文提出一种基于分布式密钥共享的安全分簇方案，通过三角形的性质提高了簇头节点的连通度，折中移动节点收集效率和能耗，通过分布式密钥共享的技术，完成移动节点的认证，保证了安全性。本文的主要贡献是提出一种适用于 UWSN 的分簇算法，且将移动节点认证和分簇算法无缝结合，在提高收集效率的同时可以保证较好的安全性。

2 相关工作

无线传感网中通过分簇算法，使部分静态节点成为簇头节点，其余静态节点受最邻近的簇头节点管理。此后静态节点可进入节能状态或者降低无线发射功率，使全网络能耗降低，以提高网络生存时间[8~10]。

经典的分簇算法有 LEACH[4]、HEED[5]等算法。LEACH 算法中，每个节点均有概率 p 成为簇头节点，然而其只可用于单跳网络。HEED 以剩余能量和网络可达能量作为簇头选举标准，算法适用于大范围多跳网络，由于使用固定簇半径，无法保证所有簇头节点均有较高的连通度。Wang 等[11]提出了一种 Sink 节点按照预定路径移动，并指导网络进行分簇的算法，其可以达到较好的分簇效果，然而算法要求 Sink 节点一直处于在线状态。El-Saadawy 等[12]在 LEACH 算法的基础上提出一种安全的分簇算法 MS-LEACH，考虑到了节点间通信的安全。但是，以上研究未考虑到 UWSN 的网络环境以及 UWSN 中 MS 节点的认证问题，故无法很好地直接应用于 UWSN 中。

对于无线传感网中的节点认证问题，Li 等[13]提出一种轻量级认证方案，根据预先存储的信息，使用对称密钥和硬件执行算法的方式完成节点的认证；Peng[14]提出适用于分簇网络的基于身份的认证方案，在认证时，节点需要通过邻居节点的认证；Xue 等[15]提出一种基于证书的多认证方案，可以通过存储节点与网关上的信息认证用户和节点；Delgado 等[16]提出一种轻量级的认证模式，通过主密钥与子密钥关系来完成节点认证；王良民等[17]提出一种移动节点漫游认证协议，移动节点在移动区域内注册一次即可漫游于整个网络且协议满足组合安全，然而节点漫游后需要传输相应的认证材料；Savola 等[18]提出一种 ad hoc 网络的认证方案，节点负责自身认证，但其部分认证操作需要可信第三方的存在。以上研究均未考虑到 MS 节点移动性或普通节点易被读取内部密钥信息的问题[19]。

在早期的无线传感网中，由于节点资源较为匮乏，节点只能使用对称加密，使用非对称加密将大量损耗资源。但是随着技术的发展，一些轻量级非对称加密可以使用在无线传感网中[20, 21]。由于普通节点易被读取内部信息，若使用对称加密，密钥很容易被攻击者知道，故基于对称密钥体系的身份认证方案并不适合 UWSN，而非对称密钥由于其通过公钥无法简单地得到私钥而使其在 UWSN 中具有一定的使用价值。本文结合 Yuan 等[22]的研究，采用非对称密钥体系，提出一种基于分布式密钥共享的安全分簇方案。

3 一种保证连通度的分簇算法(CA)

本节提出一种利用三角形的性质保证连通度的分簇算法(connectivity-assuring clustering algorithm)。通过该算法，网络中形成一个高连通的骨干网络，降低网络的路由表存储开销以及整个网络的通信开销。但由于 MS 节点未经验证会使数据泄露，

故在后续章节中对该分簇算法进行改进可以对 MS 节点的合法性进行验证，以提高网络的安全性。

CA 分簇算法包括以下几个过程：初始化阶段、成簇阶段、补充阶段和簇头更新阶段。在算法描述过程中，使用到的符号如表 1 所示。

表 1　　分簇算法符号

符号	定义
$LN(i)$	i 的邻居节点列表
$LN(i,j)$	i 和 j 公共邻居节点
$OM(i,j)=\|LN(i,j)\|$	i 和 j 的重叠指数
CGMSG	成簇消息
ACMSG	通知入簇消息
CL	成簇顺序队列
TLN	临时邻居列表

在节点部署前，由系统指定一个节点，当节点部署后，由其广播初始化网络消息 IMSG，对整个网络进行初始化操作，并由其开始执行成簇算法。当存在节点超过一定时间，周边簇头数量还未达到 3 个，该节点进入补充节点，请求成簇，以保证整个网络中任意非簇头节点均处于 3 个簇头的通信范围内，从而形成一种高连通的骨干网络。随着时间变化，簇头节点能量消耗过大，当其能量低于一定阈值时，进入簇头更新阶段，替换簇头节点，使网络仍然可以正常工作。

3.1　初始化阶段

指定节点在网络部署后，广播初始化网络消息 IMSG。对于收到 IMSG 消息的节点，将来源节点 *ID* 存储与自身的 *LN* 列表中，然后广播 IMSG 消息。随着初始化阶段的进行，非孤立节点生成自身的邻居列表 *LN*，而对于孤立节点，由于未收到 IMSG 消息，则其在整个网络生存时间中，不会收到任何网络消息。

3.2　成簇阶段

指定节点在初始化阶段开始执行一段时间后，进入成簇阶段。首先广播 CGMSG 消息，对于收到 CGMSG 消息并且在 CGMSG 消息中提及的节点，返回其 *LN* 列表。然后通过算法 1 计算附近 6 个或多个簇头节点并按序广播成簇消息，并根据其生成顺序，告知其延迟一定时间再进行成簇，给予其广播 CGMSG 消息的权限。对于继承到广播 CGMSG 消息权限的节点，首先根据周边簇头信息计算当前 *CL* 队列的顺序，然后按照算法 1 的思想成簇，并根据 *CL* 列表以及未得到广播 CGMSG 消息节点列表，继续授予广播 CGMSG 消息的权限。如此反复，直到整个网络成簇结束。

对于成簇阶段算法 1 的描述如下，其中节点 i 为当前广播 CGMSG 消息的节点。

算法 1　分簇算法

1) prepares *CL* and if *CL*'s size >5 broadcast ACMSG then exit
2) Node *i* broadcast the CGMSG
3) receives all replies or timeout then prepares *TLN*
4) if *CL*'s size < 2 then prepares *CL*'s first and second node
5) While(j_n can communicate with j_1)
6) Prepares j_n
7) If j_n cannot communicate with j_1 then
8) add j_n into *CL*
9) end if
10) end while
11) prepares j_{n+1} and add j_{n+1} into *CL*
12) broadcasts ACMSG and authorities permission to node in *CL*
13) end if

如果节点 i 的 *CL* 列表大于 5，则广播 ACMSG 消息，通知通信范围内节点入簇，并退出算法，否则发送 CGMSG 消息，获取自身 *LN* 列表中节点的 *LN* 列表。当所有的节点均返回邻居列表或等待返回时间超过操作时长后，节点 i 将返回 *LN* 列表的节点集合与 $LN(i)$进行与运算获得临时 *TLN* 列表。如果 *CL* 列表小于 3，则根据列表情况以及式(1)和式(2)准备 *CL* 列表中前 2 个节点 j_1 和 j_2 的信息。

$$j_1 \leftarrow \min(\{OM(i,j) \mid j \in TLN\}) \tag{1}$$

$$j_2 \leftarrow \min(\{OM(i,j_1,j) \mid j \in TLN\}) \tag{2}$$

接着，使用 *CL* 列表中最后 2 个节点 j_{n-1} 和 j_{n-2} 作为参考节点，根据式(3)寻找节点 j_n，直至寻找到的 j_n 可与 j_1 节点通信。

$$j_n \leftarrow \min(\{OM(j_{n-2},j) \mid j \in TLN \cap LN(j_{n-1})\}) \tag{3}$$

为保证簇头间存在一定距离，此时的 j_n 不作为簇头节点。簇头 i 根据当前时刻 *CL* 列表中最后一个节点 j_{last} 和第一个节点 j_1 作为参考节点，根据式

(4)寻找节点 j_{n+1}，使节点 i 周边簇头节点可以完成闭合。

$$j_{n+1} \leftarrow \min(\{OM(i,j) \mid j \in LNCollection\}) \quad (4)$$

其中，

$$LNCollection = TLN \cap LN(j_1) \cap LN(j_{\text{last}}) \quad (5)$$

最后广播 ACMSG 消息，通知通信范围内节点入簇，并根据成簇顺序告诉周边簇头节点广播 CGMSM 消息的顺序。

通过计算重叠指数来判断节点间距离，给出如下证明：在定理 1 中证明节点数目与区域面积相关；在定理 2 中证明节点间重叠指数 $OM(i,j)$与距离的关系。

定理 1 节点随机分布的部署区域，不考虑边缘区域影响时，任意节点 i 的邻居节点数的期望值与通信面积近似成正比。

证明 假定部署区域内节点数目为 N，部署区域面积为 S，节点 i 的通信面积为 s，节点 i 的邻居节点数的期望值为 E_i。

由于每个节点部署过程属于独立过程，则对于节点落在节点 i 通信范围 s 中的概率 P_i 有

$$P_i = s/S \quad (6)$$

所以对于节点 i 的邻居节点数的期望值 E_i 有

$$E_i = Ns/S \quad (7)$$

由式(7)可得，在不考虑边缘区域影响时，任意节点 i 的邻居节点数的期望值与通信面积近似成正比。

定理 2 节点随机分布在部署区域中，可通信节点间的距离与重叠指数近似成反比，即

$$d \propto 1/OM(i,j) \quad (8)$$

证明 如图 2 所示，假定节点通信半径为 R，节点 i、j 之间的距离为 d 其中$\angle AiD=\theta$，重叠面积为 S。

$$\begin{aligned} S &= 4(S_{AiM} - S_{\Delta AiD}) \\ &= 2\theta R^2 - 2R^2 \sin\theta\cos\theta \\ &= R^2(2\theta - \sin 2\theta) \end{aligned} \quad (9)$$

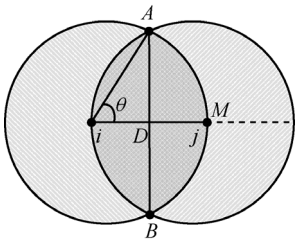


图 2 节点距离与重叠指数关系

因为 2θ~$\sin 2\theta$ 在[60°, 90°]上为单调递增，所以 $\theta \propto S$。由式(10)和式(11)

$$\theta = \cos^{-1}\frac{d}{2R} \quad (10)$$

$$\cos^{-1}\frac{d}{2R} \propto S \quad (11)$$

可得

$$d \propto 1/S \quad (12)$$

由定理 1 中 $N \propto S$ 可知，节点数的期望值正比于面积，则有 $S \propto OM(i,j)$，故可得证式(8)。

3.3 补充阶段

如果节点 h 经过一段很长时间后，周边仍然没有 3 个簇头节点，则主动进入补充阶段，提出成簇请求。与周边的单个簇头节点协商成簇，以保证网络中每个节点至少与 3 个簇头保持连通。

3.4 簇头更新阶段

簇头节点在监测到自身能量低于某阈值后，发出簇头更新的请求。能量较低的簇头，通过计算重叠指数选择一个最靠近自己的节点，作为自己的替代节点。由定理 2 可知，2 个节点的重叠指数越高，距离越近。

簇头节点 i 向 $LN(i)$发送请求 LN 的消息，周围节点 $j_1 \cdots j_w \cdots j_n$ 发送自己的 $LN(j_w)$。簇头节点 i 通过式(13)来计算最靠近 i 的节点，并且计算与 k 最近的 2 个簇头节点 C_1 和 C_2，告知节点 k。

$$OM(i,k) = \max(\{OM(i,j_w) \mid j_w \in LN(i)\}) \quad (13)$$

节点 k 如果能量充足，则向 C_1 和 C_2 发出消息，C_1 和 C_2 收到消息后，更新自己的周边簇头节点信息，同时 i 广播簇头失效的消息。

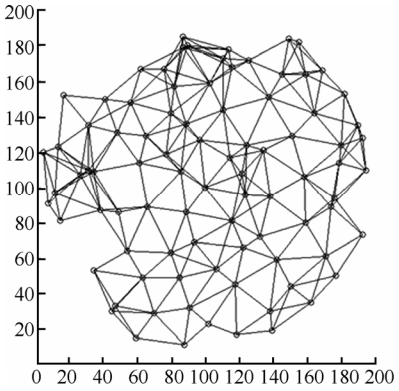
由于 k 可能无法与 i 节点周边的 6 个簇头均在通信范围内，故更新后，可能存在节点不受 3 个簇头控制，此时会有节点进入簇头补充阶段，从而完成网络骨干网的自愈合。

4 高连通的分簇算法分析

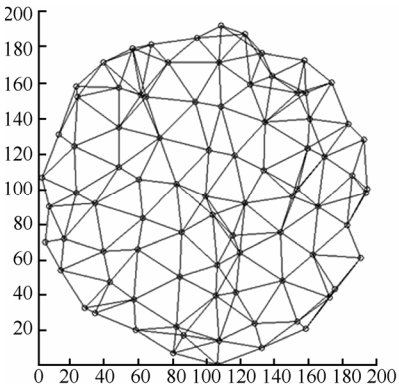
通过实验仿真 CA 算法的分簇效果，实验中场景大小是半径为 100 单位长度的圆，节点通信半径为 30 单位长度，节点随机部署。

4.1 拓扑分析

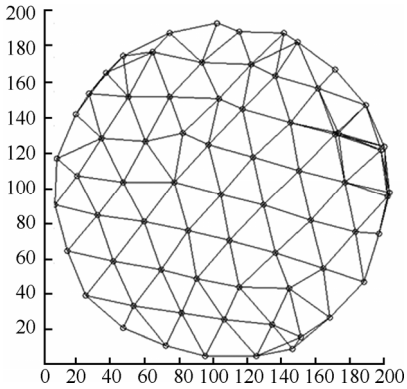
分别在节点总数分别为 200 个、500 个和 2 500 个的情况下，使用 CA 算法进行分簇，得到分簇后的拓扑如图 3 所示。



(a) 200 节点



(b) 500 节点



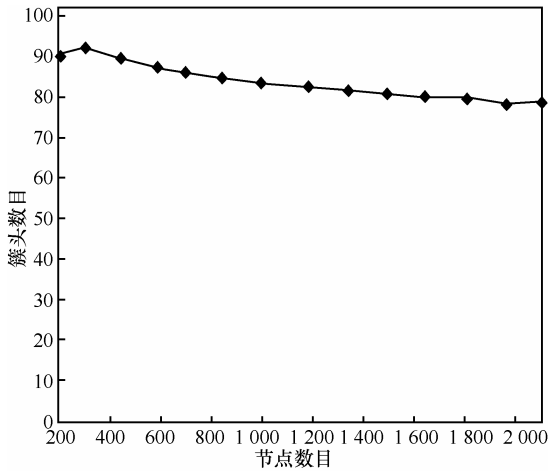
(c) 2 500 节点

图 3　节点拓扑

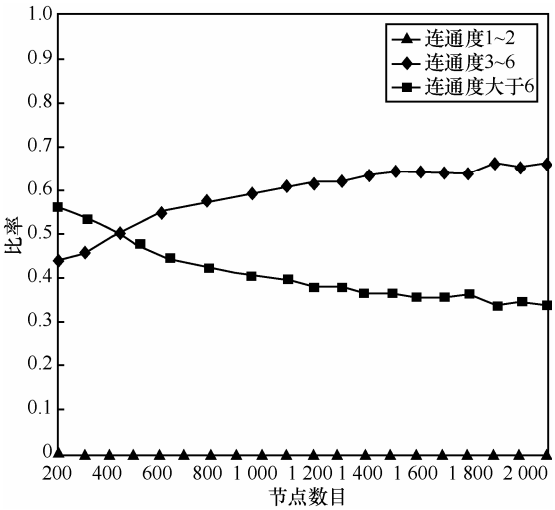
从图 3 可以看出，当节点密度越大，通过 CA 算法得到的簇头节点，越近似于三角形网格图，可见 CA 算法是收敛的。该拓扑保证了单个簇头节点在网络中的连通度，从而可以提高 Sink 节点的收集效率。

4.2　连通性分析

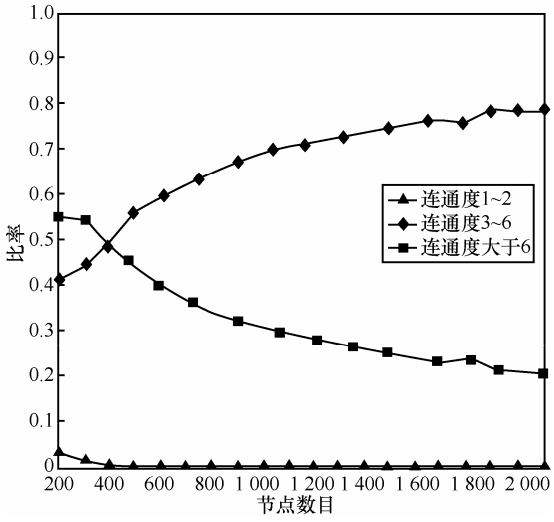
通过改变部署区域内节点数目，从 200 到 2 100，以 100 为间隔进行了仿真实验，分别对成簇后的簇头数目、簇头连通度和普通节点最大通信范围内簇头节点数目进行了统计。仿真结果如图 4 所示，所有仿真结果均取 500 次实验的平均值。



(a) 簇头数目



(b) 簇头连通度



(c) 普通节点连通度

图 4　节点数目对网络节点影响

从图 4(a)可以看到，簇头节点数目随着节点数目增加而减少，主要原因在于随着节点密度增大，分簇形成的三角形面积更大，更加逼近与以通信半

径为边长的等边三角形。而在 200 时较 300 低，但是簇头节点占总节点比例高。从图 4(b)可以看出，随着节点数目增加，簇头连通度在 3 到 6 之间的比例越大，最后趋于稳定。从图 4(c)可以看出，随着节点数目增加，普通节点连通度大于 6 的节点数逐渐增加。从实验结果可见，网络具有较高的连通度。

5 基于分布式密钥共享的安全分簇算法

由于 Sink 节点的不定期到访，使攻击者可以在 Sink 节点未到访时，冒充 Sink 节点进行数据的收集，本文提出一种安全 CA 算法(DKS-CS)，使用分布式密钥共享的方案来改进分簇算法，使 UWSN 网络可以对 MS 节点的身份进行认证。为保证认证的执行，对第 3 节所述的算法做如下改进。在所有的簇头形成后，广播的成簇消息包含自身公钥，而收到该消息的节点，保存其公钥，以保证整个网络中，节点具有一跳范围内簇头节点的公钥。系统在部署前，将从密钥池(由无线节点公钥和 MS 节点公钥组成)中随机地选取部分公钥存储。

移动节点的认证共分为 4 个阶段，并且对于广播消息均需要收到 2 条，节点才会对其处理并转发。协议发起由 MS 节点广播 AuthMessage 消息，使其周边可互相通信的 3 个簇头节点发起协议，进入密钥搜索阶段。当网络中发现密钥，则根据来时路径返回密钥，此时进入应答阶段。当协议发起簇头节点验证签名并在数量上满足初始设定的门限值时，广播 KACK 消息，协议进入确认阶段。而在整个认证协议执行过程中，如若发现异常情况，则立即进入协议终止阶段，防止敌手的攻击。在算法的描述过程中使用到的符号如表 2 所示。

表 2　　密钥管理方案符号

符号	定义
Sk_i	节点 i 的私钥
PK_i	节点 i 的公钥
C_i	节点中存储的公钥列表
R	消息传递的路由
$\{m\}_{SK}$	对消息 m 使用 SK 的签名
$Enc_{PK}\{m\}$	对消息 m 用公钥 PK 加密
$currKREQNum_Q$	关于 Q 的 KREQ 消息数量
SSN	协议发起簇头节点
S	请求节点
Q	请求公钥的 ID 号

5.1 密钥搜索阶段

MS 节点到达部署区域后，广播请求身份认证的消息 AuthMessage，其中包括自身 ID，以及对 ID 的签名。接受到该消息的簇头节点取出 ID 后，生成 KREQ 消息，并对其签名，广播出去，此时该簇头节点为 SSN 节点。KREQ 消息形式如下

$$KREQ=\{S,Q,R,\{S,Q,R\}_{SK_d}\} \tag{14}$$

式(14)中 S 为该 KREQ 消息的发起者 ID，Q 为搜索的目标节点 ID，R 为该消息的传输路径，最后为当前传输节点对该消息的签名。

对于接受到 KREQ 消息的簇头节点，如果所寻找公钥对应的 ID 存在于其 LN 列表中，进入协议终止阶段，否则验证来源签名，并保存下来。当接受到 2 条不同来源的 KREQ 消息后，如果所寻找的公钥存在于节点中，同时广播 KREQ 给其余簇头，否则广播 KREQ 给所有节点，并且节点进入应答阶段。对于接受到 KREQ 消息的普通节点，查看是否存在所需公钥，如果存在，验证 KREQ 的签名后，按照下一节所述方法产生 KREP 消息，并用 KREQ 消息来源的簇头节点的公钥加密后单播给簇头节点，如果不存在，则不做消息应答。

上述步骤可以用算法 2 进行形式化描述。

算法 2　KREQ 消息处理算法

1) Node i receives a KREQ message
2) $d \leftarrow$ last node ID in R and $R \leftarrow \{R; i\}$
3) if $Q \in LN(i)$ then
4) Node i radios KESC to all Cluster Heads Nodes
5) exit
6) end if
7) $currKREQNum_Q \leftarrow currKREQNum_Q + 1$
8) if $currKREQNum_Q > 1$ then
9) if $Q \in C_i$ then
10) Node i sends $Enc_{PKd}\{KREP\}$ to node d
11) Node i radios KREQ to all Cluster Heads Nodes
12) else
13) Node i radios KREQ to all nodes
14) end if
15) end if

5.2　应答阶段

节点在应答阶段中，如果公钥存在于节点中，则将其放入 KREP 消息中，并将存储的 KREQ 消息中 R 较短的路由存入 KREP 消息中，并用上一节点公钥加密后，传递给上一节点。KREP 消息形式如下

$$KREP=\{S,Q,PK_Q,R,\{S,Q,PK_Q,R\}_{SK_d}\} \quad (15)$$

其中，S、Q 和 R 来自于所应答的 KREQ，PK_Q 为搜索到的公钥信息。

对于接收到 KREP 消息的簇头节点，对其解密并验证签名后，根据其路由 R 逆序传递。在传输时，对数据使用上一节点的公钥加密。

5.3　确认阶段

SSN 节点接受到 KREP 消息后，验证 KREP 的签名，然后验证 AuthMessage 的签名。当公钥数达到门限值后，对 KACK 消息签名后广播。KACK 消息形式如下

$$KACK=\{S,Q,PK_Q,\{S,Q,PK_Q\}_{SK_d}\} \quad (16)$$

其中，S 和 Q 来自于所应答的 KREQ，PK_Q 为搜索到的公钥信息，其中 S 和 Q 主要用于路由功能。

对于通信范围内存在 SSN 节点的簇头节点，则必须收到可通信的 SSN 节点的 KACK 消息，并且需要满足收到 2 条 KACK 消息，才对 KACK 消息签名转发。对于通信范围内没有 SSN 节点的簇头节点，收到 2 条 KACK 消息即进行 KACK 消息的签名转发。同时对于存在可通信 SSN 节点的簇头节点，当收到多个非 SSN 节点的 KACK 消息时，可将其报告给 SSN 节点，若此时 SSN 节点没有发送 KACK 消息，则会发送 KESC 消息，进入协议终止阶段。

5.4　中止阶段

收到 KESC 消息的簇头节点，验证来源签名，并收到 3 条 KESC 消息后终止协议，不再处理关于此 ID 节点的任何消息，并同时签名广播 KESC 消息。KESC 消息形式如下

$$KESC=\{Q,\{Q\}_{SK_d}\} \quad (17)$$

其中，Q 来自于 KREQ 消息。

6　仿真实验与分析

本节将从密钥搜索概率和变节攻击 2 个方面来进行实验分析。

6.1　密钥搜索概率

在上一节所述协议中，确认阶段要求公钥数目达到阈值，则协议执行成功的关键在于单个节点搜索到的公钥数目。假设节点路由为最短路径路由算法。此时，3 个 SSN 节点的管辖范围划分为 3 个 120° 夹角的空间。为计算方便，假设部署区域为圆形，MS 节点距离部署中心距离为 d，管理范围分界线与 MS 节点—部署中心连线的夹角为 θ，则 3 块管理范围如图 5 所示。

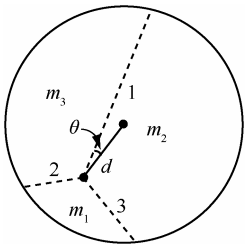


图 5　簇头节点划分范围示意

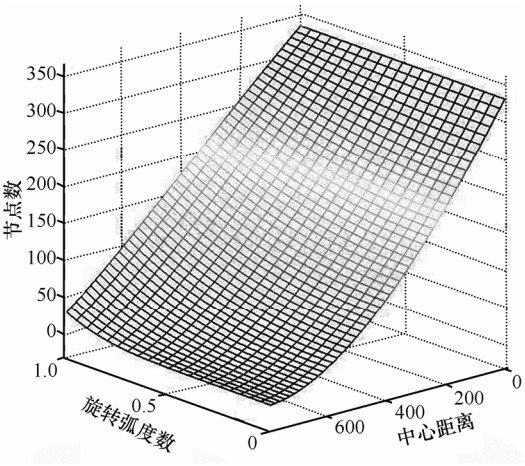
假设部署区域的节点密度均匀，在半径为 800 单位长度的圆内部署 1 000 个节点，根据数学方法分别对 3 块区域进行面积的积分，继而可以估算出 3 块区域内分别包含多少节点。实验结果如图 6 所示。

在图 6 中，可以看出 m_1 中节点数目与中心距离关系密切；m_2 中节点数目一直保持较高数目，其数量与中心距离成反比，与角度成正比；m_3 中节点数目与中心距离成反比，与角度成正比，且角度对节点数目的影响随着中心距离的增加而增加。

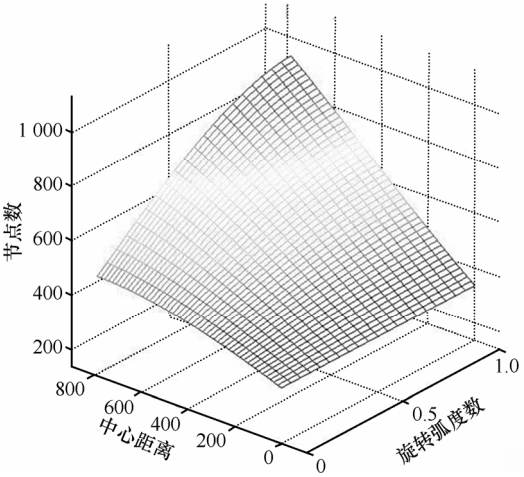
同时由实验可得到：当 MS 节点与部署中心距离在 400 单位长度以内时，任何角度下的普通节点数量均在 100 以上，即 SSN 节点等同搜索网络中 10% 的节点是否存在公钥信息。普通节点数为 1 000，MS 节点数为 50，组成密钥池大小为 1 050 的密钥池中随机选取公钥存入节点，当 SSN 节点与部署中心距离在 400 单位长度以内时，任何角度均有较大的几率至少搜到一个公钥信息。

6.2　变节节点下的攻击分析

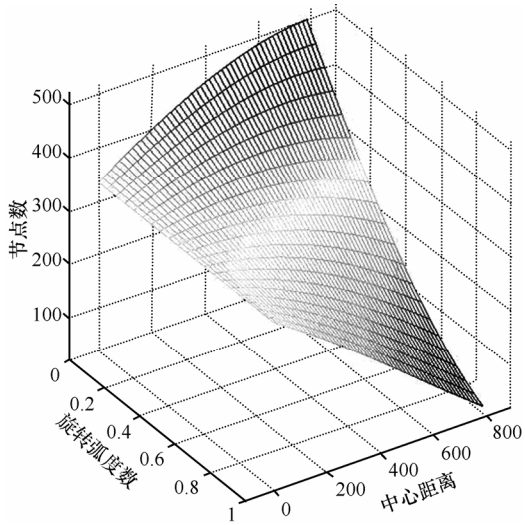
不管攻击者是否知道密钥池信息，其想要通过 MS 节点的认证，则必须知道一个 Sink 节点的 ID，并且知道该 ID 对应的私钥信息，否则无法通过 MS 节点的认证。由于密钥对与 ID 无直接关系，且在攻击中，攻击者至多知道公钥信息，而由公钥计算私钥是不可能的，故保证攻击者无法通过公钥来获得私钥，从而保证了攻击者无法伪造特定 ID 号的节点进行通信。



(a) 区块 m_1 中节点数目



(b) 区块 m_2 中节点数目



(c) 区块 m_3 中节点数目

图 6 均匀分布下三块区域节点数

但是由于攻击者可以通过修改变节节点数据，来添加新的 Sink 节点 *ID* 以及公钥信息。故本文通过仿真来对安全分簇算法抵御变节节点的攻击效果进行测试，实验参数与 4.2 节一致，其中公钥门限值设定由网络节点数目与簇头节点数目决定，变节节点随机选取，攻击者位于部署中心，对变节节点比例从 1%~80%进行测试，每一组进行 100 次测试，得到的测试结果如图 7 所示。

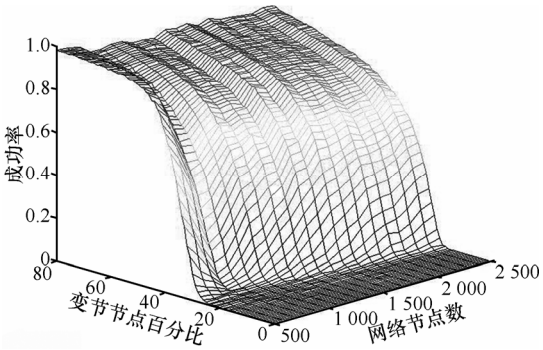


图 7 攻击成功率

从图 7 可知，攻击的成功率随变节节点百分比增多而提高，但是网络节点的增多对攻击成功率影响并不多，其主要原因是簇头节点数目变化不大，而门限值根据簇头节点和网络节点数目设定。在变节节点比例低于 20%时，攻击者成功率接近零，当变节节点比例超过 20%时，成功率急剧增加，变节节点比例 60%时接近 100%，而后攻击成功率基本均为 100%。

7 结束语

本文针对 UWSN 中数据收集效率和基站离线而引发的安全问题，提出了一种新颖的安全分簇方案，利用三角形的性质，提高了网络连通度，折中了能耗和收集效率；利用分布式密钥管理的技术，解决了 UWSN 中节点对移动节点的认证问题。通过实验分析，本文提出的安全分簇方案的拓扑简洁且连通性好，在密度较高时，趋近于三角形网格，验证了算法的收敛性；此外，实验表明该安全算法可以一定程度上抵御变节攻击——当 20%节点变节时，敌手仅有 5%的几率攻击成功。然而，当 40%节点变节时，在部分情况下敌手有 50%几率攻击成功，下一步研究将继续提高算法容忍攻击的能力。

参考文献：

[1] YAVUZ A A, NING P. Hash-based sequential aggregate and forward secure signature for unattended wireless sensor networks[A].Mobile and Ubiquitous Systems: Networking & Services[C].2009.1-10.

[2] RUAN Z, SUN X, LIANG W, *et al*. CADS: co-operative anti-fraud data storage scheme for unattended wireless sensor networks[J]. In-

formation Technology Journal, 2010, 9(7): 1361-1368.

[3] DI P R, MANCINI L V, SORIENTE C, *et al.* Catch me (if you can): data survival in unattended sensor networks[A]. Proc IEEE Sixth Ann Int'l Conf Pervasive Computing and Comm[C]. 2008. 185-194.

[4] DI P R, MA D, SORIENTE C, *et al*. Posh: proactive co-operative self-healing in unattended wireless sensor networks[A]. Reliable Distributed Systems[C]. 2008. 185-194.

[5] LIU Z, MA J, PARK Y, *et al*. Data security in unattended wireless sensor networks with mobile sinks[J]. Wireless Communications and Mobile Computing, 2012, 12(13): 1131-1146.

[6] BOYINBODE O, LE H, MBOGHO A, *et al*. A survey on clustering algorithms for wireless sensor networks[A]. 2010 13th International Conference on Network-Based Information Systems (NBiS)[C]. 2010. 358-364.

[7] LI J, MOHAPATRA P. Analytical modeling and mitigation techniques for the energy hole problem in sensor networks[J]. Pervasive and Mobile Computing, 2007, 3(3): 233-254.

[8] 韩志杰, 黄刘生, 王汝传等. 一种基于自适应半径调整的无线传感器网络覆盖控制算法[J]. 计算机研究与发展, 2010, 47(z2):69-72.
HAN Z J, HUANG L S, WANG R C, *et al*. A coverage control algorithm for wireless sensor network based on adaptive adjustment of sensing radius[J]. Journal of Computer Research and Development, 2010, 47(z2): 69-72.

[9] HEINZELMAN W R, CHANDRAKASAN A, BALAKRISHNAN H. Energy-efficient communication protocol for wireless microsensor networks[A]. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000[C]. 2000.

[10] YOUNIS O, FAHMY S. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks[J]. IEEE Transactions on Mobile Computing, 2004, 3(4): 366-379.

[11] WANG J, YANG X, MA T, *et al*. An energy-efficient competitive clustering algorithm for wireless sensor networks using mobile sink[J]. International Journal of Grid & Distributed Computing, 2012, 5(4): 79-92.

[12] EL-SAADAWY M, SHAABAN E. Enhancing S-LEACH security for wireless sensor networks[A]. 2012 IEEE International Conference on Electro/Information Technology(EIT)[C]. 2012. 1-6.

[13] LI Y, DU L, ZHAO G, *et al*. A lightweight identity-based authentication protocol[A]. 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC)[C]. 2013.1-4.

[14] PENG S. An ID-based multiple authentication scheme against attacks in wireless sensor networks[A]. 2012 IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS)[C]. 2012. 1042-1045.

[15] XUE K, MA C, HONG P, *et al*. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks[J]. Journal of Network and Computer Applications, 2013, 36(1): 316-323.

[16] DELGADO-MOHATAR O, FÚSTER-SABATER A, SIERRA J M. A light-weight authentication scheme for wireless sensor networks[J]. Ad Hoc Networks, 2011, 9(5): 727-735.

[17] 王良民, 姜顺荣, 郭渊博. 物联网中移动 Sensor 节点漫游的组合安全认证协议[J]. 中国科学: 信息科学, 2012, 42(7): 815-830.
WANG L M, JIANG S R, GUO Y B. Composable-secure authentication protocol for mobile Sensor roaming in the Internet of Things[J]. Scientia Sinica(Informationis), 2012, 42(7): 815-830.

[18] SAVOLA R M. Node level security management and authentication in mobile ad hoc networks[A]. Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, MDM '09[C]. 2009. 449-458.

[19] MA D, SORIENTE C, TSUDIK G. New adversary and new threats: security in unattended sensor networks[J]. Network, IEEE, 2009, 23(2): 43-48.

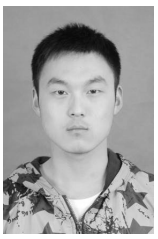
[20] WANDER A S, GURA N, EBERLE H, *et al*. Energy analysis of public-key cryptography for wireless sensor networks[A]. Pervasive Computing and Communications, PerCom 2005, Third IEEE International Conference on[C]. 2005. 324-328

[21] 裴庆祺, 沈玉龙, 马建峰. 无线传感器网络安全技术综述[J]. 通信学报, 2007, 28(8): 113-122.
PEI Q Q, SHEN Y L, MA J F. Survey of wireless sensor network security techniques[J]. Journal on Communications, 2007, 28(8): 113-122.

[22] KONG Y, DEND J, TATE S R. A distributed public key caching scheme in large wireless networks[A]. Global Telecommunications Conference (GLOBECOM 2010)[C]. 2010.1-5.

作者简介：

仲红（1965-），女，安徽固镇人，安徽大学教授、博士生导师，主要研究方向为无线传感网、安全多方计算、私有信息保护。



张庆阳（1992-），男，安徽庐江人，安徽大学硕士生，主要研究方向为传感网安全。

田立超（1986-），男，山东威海人，安徽大学硕士生，主要研究方向为无线传感网和安全多方计算。

王良民（1977-），男，安徽潜山人，安徽省皖江学者特聘教授、博士生导师，主要研究方向为传感网安全、车联网安全及大数据安全等。