doi:10.11959/j.issn.1000-436x.2015056

针对虫洞攻击的无线传感器网络安全定位方法

陈鸿龙[1]，王志波[2]，王智[3]，许江铭[4]，李燕君[5]，刘丽萍[6]

（1. 中国石油大学（华东） 信息与控制工程学院，山东 青岛 266580；2. 武汉大学 计算机学院，湖北 武汉 430072；
3. 浙江大学 工业控制技术国家重点实验室，浙江 杭州 310027；4. 中国石油塔里木油田公司，新疆 库尔勒 841000；
5. 浙江工业大学 计算机科学与技术学院，浙江 杭州 310014；6. 天津大学 电气与自动化工程学院，天津 300072）

摘 要：节点定位技术是无线传感器网络的关键技术之一，是很多基于无线传感器网络的应用的基础。然而，无线传感器网络通常部署在无人值守的敌对环境中，攻击节点能够很容易地破坏网络中节点的定位过程。针对无线传感器网络中距离无关的定位技术，分析了虫洞攻击对 DV-Hop 定位过程的影响，提出了一种无线传感器网络中抵御虫洞攻击的 DV-Hop 安全定位方法。仿真结果表明，所提出的安全定位方法能够有效降低虫洞攻击对 DV-Hop 定位过程的影响，验证了该方法的有效性。

关键词：无线传感器网络；虫洞攻击；安全定位；DV-Hop 定位

中图分类号：TP393 **文献标识码**：A

Secure localization scheme against wormhole attack for wireless sensor networks

CHEN Hong-long[1], WANG Zhi-bo[2], WANG Zhi[3], XU Jiang-ming[4], LI Yan-jun[5], LIU Li-ping[6]

(1. College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China;
2. Computer School, Wuhan University, Wuhan 430072, China; 3. State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China; 4. China Petro Tarim Qilfield Company, Kurla 841000, China;
5. College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310014, China;
6. School of Electrical Engineering and Automation, Tianjin University, Tianjin 300072, China)

Abstract: As one of the key technologies in wireless sensor networks (WSN), localization is the basis of many WSN-based applications. However, WSNs are often deployed in the hostile environment, in which the attackers can easily disrupt the localization procedure of the nodes. The effects of wormhole attack on the DV-Hop localization procedure are analyzed firstly, after which a secure localization scheme against the wormhole attack is proposed. The simulation results illustrate that the proposed secure localization scheme can efficiently reduce the effects of the wormhole attack on the DV-Hop localization, which validates the effectiveness of the proposed scheme.

Key words: wireless sensor networks; wormhole attack; secure localization; DV-Hop localization

1 引言

近年来，微机电系统（MEMS, micro-electro-mechanical systems）以及无线通信等技术的迅猛发展，使无线传感器网络（WSN, wireless sensor networks）的研究[1]得到越来越多的研究机构和学者们的支持。目前，无线传感器网络有着极其广泛的应用，包括军事领域的目标定位和追踪，民用领域的森林火警监测、医疗监护和智能家居等。然而，许多无线传感器网络的应用是基于节点位置信息

收稿日期：2013-10-08；**修回日期**：2013-12-09

基金项目：国家自然科学基金资助项目(61309023，61273079, 61104208)；山东省自然科学基金资助项目(ZR2013FQ032)；中央高校基本科研业务费专项基金资助项目(13CX02100A)；浙江省可视媒体智能处理技术研究重点实验室开放课题基金资助项目(2012008)

Foundation Items: The National Natural Science Foundation of China (61309023, 61273079, 61104208); The Natural Science Foundation of Shandong Province (ZR2013FQ032); The Fundamental Research Funds for the Central Universities (13CX02100A) ; The Open Project of Zhejiang Provincial Key Lab of Intelligent Processing Research of Visual Media (2012008)

的，其监测的事件与节点的物理位置信息息息相关，没有位置信息的监测数据是毫无意义的。因此，作为无线传感器网络的关键技术之一，节点定位技术是无线传感器网络的理论发展和应用的基础，贯穿了整个无线传感器网络技术的研究和发展。

无线传感器网络中通常包括 2 种节点：信标节点（Beacon）和未知节点（Unknown）。其中，信标节点在网络部署之后就能够知道其自身位置信息（通过 GPS 设备或者人工部署的方式），而未知节点则不能提前获得自身位置，需要通过特定的定位方法来获取该信息。无线传感器网络中节点定位可分为基于距离的（range-based）和距离无关的（range-free）定位方法。基于距离的定位方法中，未知节点通过测量其与信标节点之间的距离信息或者角度信息，结合信标节点的坐标计算其自身坐标，包括基于 TDoA[2]，ToA，RSSI 以及 AoA 等；距离无关的定位方法则是利用网络特性，如节点间跳数或者节点中心等，常见的方法有 DV-Hop[3]、APIT[4]、Fingerprinting[5]等。

然而，由于无线传感器网络经常部署在无人值守的环境中，攻击节点能够很轻易地入侵到网络中，破坏网络的正常功能。同时，无线通信过程的开放特性决定了攻击节点能够监听网络中数据分组或者伪造数据分组并广播到网络中。因此，安全问题已经成为无线传感器网络研究过程中的一个重大挑战。攻击节点通过发起特定的攻击手段，如虫洞攻击，就能够对网络中的节点定位过程产生严重的影响。本文首先分析虫洞攻击对 DV-Hop 定位过程的影响，提出一种抵御虫洞攻击的安全定位方法，并通过仿真验证所提出的安全定位方法的有效性。

2　相关工作

近几年，传感器网络安全定位技术成为了研究热点之一，引起了广大学者们的充分重视，并取得了大量成果。文献[6]概述了现有的传感器网络中的安全定位方法，其中大部分的安全定位方法采用的是加密解密[7,8]、检测节点异常[9~11]或者验证节点位置信息[12,13]等方法。DRBTS[7]采用了网络级的组群秘钥来对数据分组进行加密，通过基于信誉值的方法剔除位置信息有误的 Beacon 节点，同时 Sensor 节点基于投票选举的方法选出可信认的 Beacon 节点。SLAT[8]通过信息认证的方式有效抑制节点伪造位置信息，同时通过特定的位置报告算法来确保被攻击的Beacon节点对定位的影响不会太大。文献[9]提出了基于一致性检测的方法来检测并剔除异常的距离信息，使攻击节点对未知节点的定位过程的影响大大降低。SLA[10]提出了一种利用信标节点在不同功率等级下的传输随机数(nonce)来相互验证数据有效性的安全定位算法。文献[11]提出了一种基于隐藏移动基站的位置校验机制，该机制能够为无线传感器网络中的许多定位方法提供安全保障。Capkun 等人提出了 SPINE[12]，即一种基于可验证多边形的基于距离的安全定位方法，该方法通过约束未知节点到邻居参考节点的距离上限值来抵御位置和距离哄骗攻击。Rope[13]提出了一种分布式的定位方法，在此基础上提供一种位置验证机制以验证节点所声称的位置是否受到攻击的影响。

虫洞攻击可以由 2 个合作的攻击节点共同发起，其对安全定位过程的影响不可忽视。目前，学者们已经提出了许多针对虫洞攻击的检测方法[14]。SeRLoc[15]提出了一种基于扇区唯一特性和通信距离违背特性的虫洞攻击检测方法，并通过对受攻击的信标节点的识别与剔除实现了抵御虫洞攻击的安全定位。HiRLoc[16]在 SeRLoc 基础上进一步考虑了天线的可旋转特性以及多个无线发射功率等级，有效地提高了定位精度。文献[17]提出了一种基于标签的抵御虫洞攻击的 DV-Hop 定位方法，该方法通过将虫洞链路两端的节点进行标注，分配不同的标签，未知节点通过相应的区分算法对邻居节点进行过滤，剔除受到虫洞攻击的节点，进而实现安全定位。然而，SeRLoc 和 HiRLoc 方法均需要特殊硬件（方向性天线），而文献[17]方法比较复杂，对于计算资源有限的节点来说实现起来比较困难。本文针对 DV-Hop 定位过程，提出了一种简单有效的抵御虫洞攻击的安全定位方法。

3　问题描述

3.1　网络部署

假设无线传感器网络中有 3 种节点：Beacon、Sensor 和 Attacker。其中，Beacon 节点是位置信息已知的节点（可通过 GPS 设备或者提前部署获得），可以为网络中其他节点提供定位服务，Sensor 节点是位置未知的节点，在网络中执行特定的检测任务，同时可以在网络中 Beacon 节点的帮助下进行自身定位，以获得位置信息；Attacker 节点成对出现，通过合作的方式共同发起攻击，干扰网络中

Sensor 节点的定位过程。网络中的所有节点通信半径均为 R，且假设任意两节点在通信半径范围之内进行数据分组交换不存在分组丢失。Beacon 节点在网络中满足泊松分布，即当 Beacon 节点密度为 ρ_B 时，假设 N_B 为面积为 πR^2 的区域内的 Beacon 节点个数，则满足 $\Pr(N_B=k)=\frac{(\pi R^2\rho_B)^k}{k!}\mathrm{e}^{-\pi R^2\rho_B}$。

3.2 DV-Hop 定位过程

DV-Hop[3]定位过程主要包括 3 个阶段：首先，网络中的所有 Beacon 节点各自发起泛洪，之后网络中的其他节点便能够得到其到达每个 Beacon 节点的最小跳数；其次，每个 Beacon 节点在得到其到达网络中其他 Beacon 节点的最小跳数后，即可估计出平均每跳距离。例如，假设 Beacon 节点 B_i 得到到达其他 Beacon 节点的最小跳数后，即可估计平均每跳距离为 $H_i=\frac{\sum_{i\neq j}\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{\sum_{i\neq j}h_{ij}}$，其中，$x_i$ 表示 Beacon 节点 B_i 的坐标，h_{ij} 表示 Beacon 节点 B_i 和 B_j 之间的最小跳数。Beacon 节点估计得到平均每跳距离后，将该信息广播给其邻居 Sensor 节点；最后，Sensor 节点根据其到达每个 Beacon 节点的最小跳数以及其邻居 Beacon 节点估计得到的平均每跳距离，可以估计出其与每个 Beacon 节点之间的距离，即可利用三边法或者极大似然估计法计算出其自身位置坐标。

3.3 攻击模型

无线传感器网络网络中的攻击节点可以分为外部攻击节点和内部攻击节点，其中外部攻击节点无需获得系统的认证即可对网络功能进行干扰和破坏，而内部攻击节点需要得到系统认证并获得相关的秘钥信息。本文主要考虑的是一种外部攻击节点——虫洞攻击（wormhole attack）对 DV-Hop 定位过程的影响。虫洞攻击通常是由 2 个攻击节点合谋共同发起的，其中一个攻击节点部署在网络中的一端，监听周围节点的数据分组，通过虫洞链路（wormhole link）发送给位于网络另一端的另一个攻击节点，并由该攻击节点广播给其周围节点。假设虫洞链路双向对称的，即数据分组可以从任何一个攻击节点转发到另一个攻击节点。因此，如果虫洞链路的长度小于 R，则由攻击节点广播的数据分组会被另一个攻击节点接收到，并再由通过虫洞链路发送回去，形成环路自激。由于虫洞攻击链路越长，对定位过程的影响越大，本文假设虫洞链路长度大于 $2R$，因此不存在上述自激问题。

虫洞攻击过程简单，但是会对定位过程带来非常恶劣的影响。如图 1 所示，网络中存在一对虫洞攻击节点 A_1 和 A_2。在 DV-Hop 定位过程中，Beacon 节点 B_1 首先发起泛洪，各个未知节点即可得到 B_1 的最小跳数。在没有虫洞攻击的条件下，Sensor 节点 S_6 得到的距离 B_1 的最小跳数应该为 5（$B_1\rightarrow S_2\rightarrow S_3\rightarrow S_4\rightarrow S_5\rightarrow S_6$），而在受到虫洞攻击之后，Sensor 节点 S_6 得到的距离 B_1 的最小跳数变为 3（$B_1\rightarrow S_1\rightarrow A_1\rightarrow A_2\rightarrow S_7\rightarrow S_6$），其中，由于虫洞攻击节点是无条件转发，$S_1\rightarrow A_1\rightarrow A_2\rightarrow S_7$ 被认为是 1 跳。因此，由于虫洞攻击的存在，S_6 得到的距离 B_1 的最小跳数比实际要小得多，因此其将得到一个到达 B_1 距离的错误估计值，使最终的定位结果被严重干扰。所以，虫洞攻击能够对 DV-Hop 定位过程产生严重的影响。本文将针对 DV-Hop 定位过程，提出一种简单有效的抵御虫洞攻击的安全定位方法。

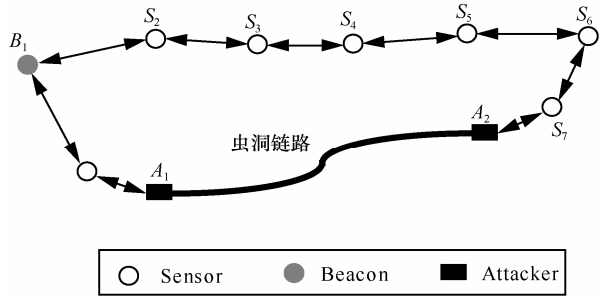


图 1 虫洞攻击对 DV-Hop 定位过程的影响

4 安全定位方法

针对虫洞攻击对 DV-Hop 定位过程的影响，我们提出了有效的安全定位方法，包括虫洞攻击检测，异常节点剔除和 DV-Hop 定位 3 个过程。

为了更清楚地阐述本文所提出的安全定位方法，首先定义几个本文常用的术语：$N_B(u)$，$N_S(u)$ 和 $N(u)$ 分别表示节点 u 的邻居 Beacon 节点，邻居 Sensor 节点和邻居节点，很明显，在本文中，$N_B(u)+N_S(u)=N(u)$；$D_R(u)$ 表示以 u 为圆心，R 为半径的圆盘。

4.1 虫洞攻击检测

当无线传感器网络中的 DV-Hop 定位过程受到虫洞攻击时，网络中的 Beacon 节点可以采用以下 2 个特性来检测虫洞攻击。

传输距离受限特性：任何一个节点不能与其通信范围之外的节点通信。

基于传输距离受限特性的检测方法：在正常情况下，传输距离受限特性是不会被违背的，但是，当节点受到虫洞攻击时，就可能会有异常出现。如图 2 所示，Beacon 节点 B_3 和 B_4 在 B_1 的传输距离之外，即 $B_3, B_4 \notin D_R(B_1)$，因此正常情况下 B_3 和 B_4 无法接收到 B_1 的数据分组。但是当网络中存在虫洞攻击时，B_1 发送的数据分组能够被攻击节点 A_1 接收到，并且通过虫洞链路转发给 A_2，再由 A_2 广播给其邻节点，包括 B_3 和 B_4，因此，B_3 和 B_4 能够接收到 B_1 的数据分组。另外，由于 B_1，B_3 和 B_4 都是 Beacon 节点，其自身坐标是已知的，因此，B_3 和 B_4 在接收到来自 B_1 的数据分组后可以通过计算其与 B_1 之间的距离来判断是否违背上述特性。因此，在 DV-Hop 定位之前，Beacon 节点首先广播一个 test 数据分组，并将自己的 ID 以及坐标等信息存在广播数据分组中。当 B_3 和 B_4 接收到 B_1 的 test 数据分组时，会提取出 B_1 的位置信息，并计算它们到达 B_1 的距离，若距离大于 R，则可以判断当前受到虫洞攻击。

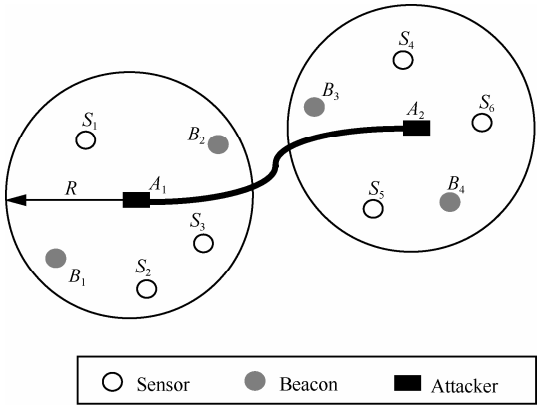


图 2　无线传感器网络中的虫洞攻击

数据分组唯一特性：在一次通信过程中，每个节点只能接收一次来自其邻节点的广播数据分组。

基于数据分组唯一特性的检测方法：同样地，正常情况下网络中的节点通信不会违背数据分组唯一特性。但是当网络中存在虫洞攻击时，如图 2 所示，节点 B_3 在 B_2 的通信距离内，即 $B_3 \in D_R(B_2)$，因此，在 DV-Hop 定位之前，B_2 首先广播 test 数据分组，test 数据分组首先会直接被 B_3 接收到。同时，由于 B_2 在 A_1 的通信半径之内，B_2 广播的数据分组也会被 A_1 监听到，并且转发给 A_2，再由 A_2 广播给其邻节点，最终，B_3 能够从 A_2 接收到来自 B_2 的数据分组。因此，B_3 能够接收到 2 次来自 B_2 的数据分组，违背了上述特性。所以，当 DV-Hop 定位过程中受到虫洞攻击时，Beacon 节点即可采用上述方法检测时候违背数据分组唯一特性，若违背，则可以判断当前受到虫洞攻击。

因此，当无线传感器网络中的 DV-Hop 过程受到虫洞攻击影响时，网络中的 Beacon 节点可以采用上述方法来检测虫洞攻击。并且，上述虫洞攻击检测方法满足。

定理 1　当节点 DV-Hop 定位过程受到虫洞攻击时，若 2 个攻击节点的通信范围内分别至少存在一个 Beacon 节点，则虫洞攻击能够被检测出来。

证明　不失一般性，假设 2 个虫洞攻击节点的通信范围内各存在一个 Beacon 节点 B_i 和 B_j。若 B_i 和 B_j 之间的距离大于 R，则 2 个节点之间的通信会违背传输距离受限特性；若 B_i 和 B_j 之间的距离小于或等于 R，则它们之间的通信会违背数据分组唯一特性。因此，虫洞攻击均能够被检测出来。

当虫洞攻击节点的通信范围内存在的 Beacon 节点个数不止 1 个时，上述证明过程亦然有效。因此，定理 1 得证。

定理 2　当 DV-Hop 定位过程中受到虫洞攻击影响时，传感器网络能够成功检测出虫洞攻击的概率为

$$\Pr(s) = (1 - \mathrm{e}^{-\rho_B \pi R^2})^2$$

证明　由定理 1 可知，传感器网络能够成功检测出虫洞攻击的条件是虫洞攻击节点的通信范围内个存在至少一个 Beacon 节点。令事件 A 为虫洞攻击节点 A_1 通信范围内不存在 Beacon 节点，事件 B 为虫洞攻击节点 A_2 通信范围内不存在 Beacon 节点。由于网络中 Beacon 节点在单位面积内的个数满足泊松分布，可得 $P(\mathrm{A}) = P(\mathrm{B}) = \mathrm{e}^{-\rho_B \pi R_2}$。因此，事件 $\overline{\mathrm{A}}\overline{\mathrm{B}}$ 表示能够成功检测出虫洞攻击，且 $P(\overline{\mathrm{A}}) = P(\overline{\mathrm{B}}) = 1 - \mathrm{e}^{-\rho_B \pi R_2}$。由于两个虫洞攻击节点通信范围内的 Beacon 节点的分布是相互独立的，可得

$$\Pr(s) = P(\overline{\mathrm{A}}\overline{\mathrm{B}}) = P(\overline{\mathrm{A}})P(\overline{\mathrm{B}}) = (1 - \mathrm{e}^{-\rho_B \pi R^2})^2$$

其中，ρ_B 表示网络中 Beacon 节点的密度，R 表示节点的通信半径。因此，定理 2 得证。

4.2　异常节点剔除

当网络中的 DV-Hop 定位过程受到虫洞攻击时，Beacon 节点检测出虫洞攻击的存在之后，还必须进一

步把受到虫洞攻击影响的节点（包括 Beacon 节点和 Sensor 节点）识别出来，并且从网络中剔除掉，使 DV-Hop 定位不受虫洞攻击的影响，实现安全定位。

只要节点位于虫洞攻击节点的通信范围之内，就有可能通过虫洞链路与位于另一个虫洞攻击节点通信范围内的其他节点进行信息交互，而这类信息交互会直接影响到 DV-Hop 定位过程。因此，最直接的办法是将虫洞链路两端的节点区分开来，人为地将两端的节点之间的通信链路切断。然而，这种方法相对比较复杂。本文采用的方法是将虫洞攻击节点通信范围内的所有节点全部识别出来，并且令它们在 DV-Hop 定位过程中直接进入休眠状态，不参与 DV-Hop 定位，这样一来可以简单有效地把虫洞攻击的影响抵消掉，其代价是牺牲了网络中的一部分节点。

为了使虫洞攻击节点通信范围内的所有节点进入休眠状态，一种简单的实现方法是：当 Beacon 节点检测到虫洞攻击时，即可广播一个 Sleep 数据分组，而接收到 Sleep 数据分组的节点则进入休眠状态。如图 2 所示，当 Beacon 节点 B_1 基于传输距离受限特性检测到虫洞攻击时，即可广播一个 Sleep 数据分组。由于 S_2 在 B_1 的通信范围内，S_2 可以接收到 Sleep 数据分组并且进入休眠状态。同时，B_1 的 Sleep 数据分组可以通过攻击节点 A_1 经由虫洞链路转发给 A_2，并由 A_2 广播给其邻节点，包括 B_3，B_4，S_4，S_5 和 S_6，因此这些节点均会进入休眠状态。同样地，B_4 也会检测出虫洞攻击，并且广播 Sleep 数据分组，S_5 和 S_6 会直接收到 B_4 的 Sleep 数据分组并进入休眠状态。而 B_4 的 Sleep 数据分组也会经过虫洞链路转发给 B_1，B_2，S_1，S_2 和 S_3，因此这些节点也会进入休眠状态。这样一来，可以使 A_1 和 A_2 通信范围内的所有节点都进入休眠状态。但是，该方法的缺陷是，Beacon 节点广播的 Sleep 数据分组不仅会经虫洞链路转发到另一端的节点，也会被其邻节点接收到。如果 Beacon 节点刚好位于攻击节点的通信范围边缘，则可能会有一些节点位于该 Beacon 节点的通信范围内，但又在攻击节点的通信范围外，这些节点接收到该 Beacon 节点的 Sleep 数据分组后同样会进入休眠状态。因此，这种方法会产生很严重的副作用，尤其是当虫洞攻击节点通信范围内的 Beacon 节点数据较多时，会使很多本不受到虫洞攻击影响的节点进入休眠状态，影响 DV-Hop 的定位精度。因此，本文提出了一种基于节点冲突集的异常节点剔除方法，可以有效减低上述影响。

4.2.1 冲突集

为了阐述所提出的基于节点冲突集的异常节点剔除方法，首先引入冲突集这一概念。

定义 1 冲突集：在受到虫洞攻击下，每个 Beacon 节点把其他与其之间的通信违背距离传输受限特性和数据分组唯一特性的 Beacon 节点的集合作为冲突集。

如图 2 所示，B_3，B_4 与 B_1 之间的通信违背了距离传输受限特性，因此 B_1 的冲突集为 B_3 和 B_4。令 $C(B_i)$ 为 Beacon 节点 B_i 的冲突集，因此在图 2 中，$C(B_1)=C(B_2)=\{B_3,B_4\}$，$C(B_3)=C(B_4)=\{B_1,B_2\}$。

定理 3 某一个虫洞攻击节点的通信范围内的 Beacon 节点，其冲突集是虫洞链路另一端的攻击节点通信范围内的所有 Beacon 节点。

证明 由冲突集的定义即可得出上述结论。

如图 2 所示，当 Beacon 节点 B_1，B_2，B_3 和 B_4 广播 test 数据分组后，即可得到 $C(B_1)=C(B_2)=\{B_3,B_4\}$，$C(B_3)=C(B_4)=\{B_1,B_2\}$。

引理 1 同一个虫洞攻击节点通信范围内的 Beacon 节点的冲突集是一致的。

证明 由定理 3 可知，一个虫洞攻击节点通信范围的 Beacon 节点的冲突集是另一个虫洞攻击节点通信范围内的所有 Beacon 节点的集合。因此，同一个虫洞攻击节点通信范围内的 Beacon 节点的冲突集是一致的。引理 1 得证。

4.2.2 异常节点剔除方法

在 DV-Hop 定位之前，所有的 Beacon 节点广播一个 test 数据分组，每个 Beacon 节点即可根据接收其邻居 Beacon 节点的 test 数据分组的过程中是否违背上述 2 个特性，建立其冲突集。由引理 1 可知，虫洞攻击节点通信范围内的所有 Beacon 节点的冲突集是一致的，因此可以从冲突集中挑选出一个唯一的 Beacon 节点，让这个 Beacon 节点来广播 Sleep 数据分组，让其周围的节点进入休眠状态，即可有效降低本章前面介绍的方法所带来的副作用。

具体的异常节点剔除方法如下：Beacon 节点广播 test 数据分组，并接收到其邻居 Beacon 节点的 test 数据分组，在这一过程中，每一个 Beacon 节点建立其自身的冲突集（若 Beacon 节点不在虫洞攻击节点的通信范围内，则冲突集为空）。之后，Beacon 节点将自真的冲突集广播给其邻居 Beacon

节点。Beacon 节点在接收到邻居节点广播的冲突集数据分组后，首先判断自己是否在该冲突集中，如果是，进一步判断其 ID 是否是冲突集中的所有节点中最小的，若是，则 Beacon 节点广播一个 Sleep 数据分组，若不是，则 Beacon 节点继续监听网络中的数据分组。每个 Sensor 节点接收到 Sleep 数据分组后，立即进入休眠状态。而 Beacon 节点接收到 Sleep 数据分组后，首先判断该数据分组的发送者是否在其冲突集中，若是，则进入休眠状态，若不是，则继续监听。算法 1 为异常节点剔除算法的伪代码。

如图 2 所示，当 B_1、B_2、B_3 和 B_4 广播 test 数据分组后，即可建立各自的冲突集。之后，每个 Beacon 节点各自广播自己的冲突集，即 B_1 和 B_2 广播 $\{B_3, B_4\}$，而 B_3 和 B_4 广播 $\{B_1, B_2\}$。B_3 接收到 B_1 和 B_2 广播的冲突集后，判断自己在冲突集中，且其 ID 最小，因此，B_3 广播一个 Sleep 数据分组。Sensor 节点接收到 B_3 广播的 Sleep 数据分组后，即可进入休眠状态。例如，S_1、S_2、S_3 和 S_4 均能够接收到 B_3 的 Sleep 数据分组，因此进入休眠状态。而 Beacon 节点接收到 B_3 的 Sleep 数据分组后，首先判断 B_3 是否在其冲突集中。例如，B_1 和 B_2 接收到 B_3 的 Sleep 数据分组后，由于 B_3 均在其冲突集中，因此 B_1 和 B_2 进入休眠状态。另外，B_4 也能够接收到 B_1 和 B_2 广播的冲突集，但由于 B_4 不是该冲突集中 ID 最小的，因此，B_4 继续监听。类似的，B_1 和 B_2 也能接收到 B_3 和 B_4 广播的冲突集，且 B_1 是冲突集中 ID 最小的，因此，B_1 也广播一个 Sleep 数据分组。Sensor 节点 S_2，S_4，S_5 和 S_6 接收到 B_1 的 Sleep 数据分组后即可进入休眠状态。B_3 和 B_4 接收到 B_1 的 Sleep 数据分组后，判断 B_1 在它们的冲突集中，因此，也进入休眠状态。

算法 1　异常节点剔除算法

1) Beacon 节点广播 test 数据分组，并且监听其邻居 Beacon 节点的 test 数据分组，建立其冲突集；

2) Beacon 节点广播其冲突集；

3) Beacon 节点 B_i 接收到冲突集 $C(B_j)$ 后，如果 $B_i \in C(B_j)$ 并且 B_i 是 $C(B_j)$ 中 ID 最小的，则广播 Sleep 数据分组，否则，继续监听；

4) Sensor 节点接收到 Sleep 数据分组后，进入休眠；

5) Beacon 节点 B_i 接收到 B_j 的 Sleep 数据分组后，如果 $B_j \in C(B_i)$，则进入休眠，否则，继续监听。

因此，如图 2 所示，利用上述方法之后，$D_R(A_1) \cup D_R(A_2)$ 中的所有节点以及 $D_R(B_1) \cup D_R(B_3)$ 中的所有 Sensor 节点都会进入休眠状态。而如果利用本章开头介绍的方法，则 $D_R(A_1) \cup D_R(A_2) \cup D_R(B_1) \cup D_R(B_2) \cup D_R(B_3) \cup D_R(B_4)$ 中的所有节点都会进入休眠状态。所希望的是只有 $D_R(A_1) \cup D_R(A_2)$ 中的节点进入休眠状态。因此，采用所提出的异常节点剔除方法之后，可以有效地降低额外牺牲的节点个数。

4.3　DV-Hop 定位

经过异常节点剔除算法之后，所有虫洞攻击节点通信范围之内的节点都进入休眠状态，不参与定位过程。此时，网络中的其他节点即可进行 DV-Hop 定位。由于受到虫洞攻击影响的节点不参与定位，DV-Hop 定位过程不再受到虫洞攻击的影响，因此，可以实现安全定位。

5　仿真结果与分析

本节中，首先通过仿真来分析虫洞攻击对 DV-Hop 定位过程的影响，说明安全特性在 DV-Hop 定位过程中的重要性；接着将通过仿真来验证上述针对虫洞攻击检测概率的理论结果以及所提出的安全定位方法的有效性。

仿真过程中默认的参数配置如下：传感器网络部署在 800 m×800 m 的正方形区域，包括 100 个节点，其中信标节点 20 个和未知节点 80 个，以及一对虫洞攻击节点，节点的通信半径 R=150 m，虫洞链路长度为 $4R$。图 3 是仿真过程中的一个节点分布示例，其中，圆圈表示 Sensor 节点，三角形表示 Beacon 节点，正方形表示攻击节点。

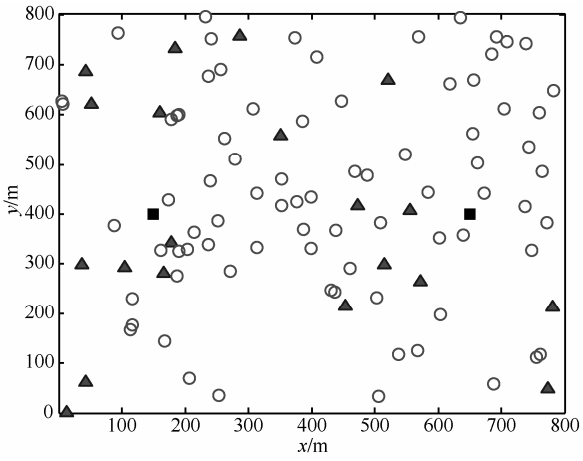


图 3　存在虫洞攻击的传感器网络节点分布

图4说明了虫洞链路长度对DV-Hop定位精度的影响。从图中曲线可以看出，虫洞攻击对DV-Hop定位过程的影响比较严重，其定位平均误差基本上大于 R（R=150 m）。并且虫洞链路越长，DV-Hop定位的平均误差越大，虫洞攻击对DV-Hop定位过程的影响越严重。所以，本文所提出的抵御虫洞攻击的DV-Hop安全定位方法是非常有必要的。

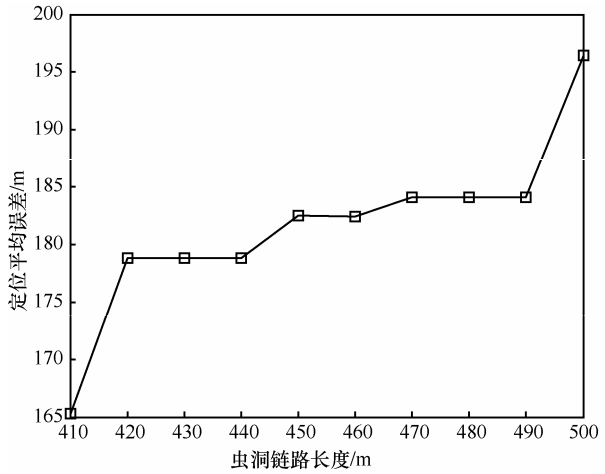


图4 虫洞链路长度对DV-Hop定位精度的影响

图5对所提出的虫洞攻击检测方法的实际检测概率和理论概率进行了比较，其中，理论概率为定理2所得到的结果。从图5中曲线可以看出，当信标节点个数增加，即网络中信标节点密度增大时，虫洞攻击检测概率增大，且当信标节点比例达到30%时，虫洞攻击检测概率即可超过90%，说明了所提出的检测方法的有效性。同时，曲线也表明了实际检测概率与理论概率十分吻合，最大误差不超过3%，验证了定理2中的理论结果的正确性。

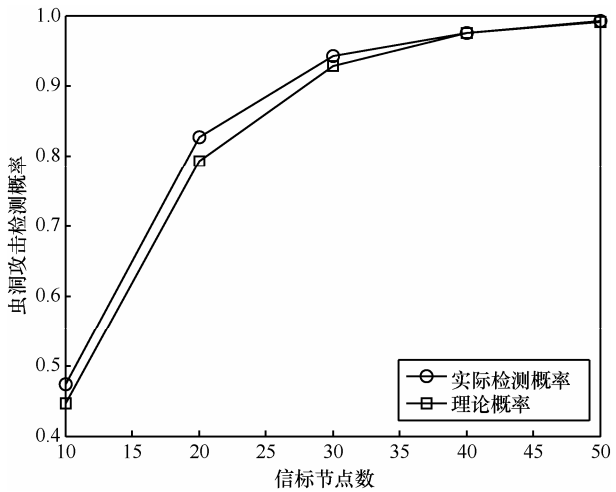


图5 实际虫洞攻击检测概率与理论概率的对比

图6对3种不同情况下的DV-Hop定位方法的相对定位误差进行比较，包括无虫洞攻击下的DV-Hop 定位、虫洞攻击下但没有抵御措施的DV-Hop 定位以及抵御虫洞攻击的 DV-Hop 定位。很明显，在虫洞攻击下，没有抵御措施的 DV-Hop定位的相对误差比较大（大于 R），进一步说明了安全定位的重要性。由图6中曲线可以看出，本文所提出的抵御虫洞攻击的DV-Hop定位方法的相对误差已经十分接近没有虫洞攻击下的DV-Hop定位过程，尤其在信标节点个数大于或等于 30 时，两者已无明显差别，充分说明了本文所提出的安全定位方法的有效性。

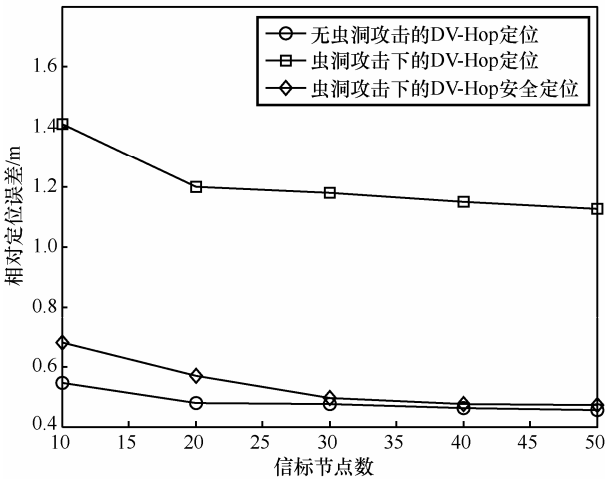


图6 相对定位误差比较

6 结束语

本文针对无线传感器网络中距离无关的定位技术，分析了虫洞攻击对DV-Hop定位过程的影响，说明了传感器网络中DV-Hop定位过程安全的重要性。接着本文提出了一种无线传感器网络中抵御虫洞攻击的安全定位方法，包括虫洞攻击检测、异常节点剔除以及DV-Hop定位。仿真结果验证了本文相关理论的正确性，表明所提出的安全定位方法能够有效降低虫洞攻击对DV-Hop定位过程的影响，验证了该方法的有效性。

本文所提出的针对抵御虫洞攻击的安全定位方法中，并不考虑节点通信过程中的分组丢失问题，且假设所有节点的通信半径都是一样的，因此，今后的研究工作之一是解决分组丢失存在条件下的针对虫洞攻击的节点安全定位问题，并且使之能够适用于不同类型节点具有不同通信半径这一条件下。

参考文献：

[1] AKYILDIZ I, SU W, SANKARASUBRAMANIAM Y, *et al*. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.

[2] 陈鸿龙, 李鸿斌, 王智. 基于 TDoA 测距的传感器网络安全定位研究[J]. 通信学报, 2008, 29(8):11-21.
CHEN H, LI H, WANG Z. Research on TDoA-based secure localization for wireless sensor networks[J]. Journal on Communications, 2008, 29(8):11-21.

[3] SIT T, LIU Z, ANG M, SEAH W. Multi-robot mobility enhanced hop-count based localization in ad-hoc networks[J]. Robotics and Autonomous Systems, 2007, 55(3):244-252.

[4] HE T, HUANG C, BLUM B, *et al*. Range-free localization and its impact on large scale sensor networks[J]. ACM Transactions on Embedded Computing Systems, 2005, 4(4): 877-906.

[5] BSHARA M, ORGUNER U, GUSTAFSSON F, BIESEN L. Fingerprinting localization in wireless sensor networks based on received-signal-strength measurements: a case study on WiMAX Networks[J]. IEEE Transactions on Vehicular Technology, 2010, 59(1): 283-294.

[6] BOUKERCHE A, OLIVERIA H A, NAKAMURA E F, *et al*. Secure localization algorithms for wireless sensor networks[J]. IEEE Communications Magazine, 2008, 46(4):96-101.

[7] SRINIVASAN A, TEITELBAUM J, WU J. DRBTS: distributed reputation-based beacon trust system[A]. Proceedings of the IEEE International Symposium on Dependable, Autonomic and Secure Computing[C]. 2006.277-283.

[8] PIRRETTI M, VIJAYKRISHNAN N, MCMANIEL P, MADAN B. SLAT: Secure Localization with Attack Tolerance[R]. Technical report 2006.

[9] LIU D, NING P, DU W. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks[A]. Proceedings of the IEEE ICDCS[C]. 2005.609-619.

[10] ANJUM F, PANDEY S, AGRAWAL P. Secure localization in sensor networks using transmission range variation[A]. Proceedings of the IEEE MASS[C]. 2005. 195-203.

[11] CAPKUN S, RASMUSSEN K B, CAGALJ M, *et al*. Secure location verification with hidden and mobile base stations[J]. IEEE Transactions on Mobile Computing, 2008, 7(4):470-483.

[12] CAPKUN S, HUBAUX J P. Secure positioning in wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 221-232.

[13] LAZOS L, POOVENDRAN R, CAPKUN S. ROPE: robust position estimation in wireless sensor networks[A]. Proceedings of the IEEE IPSN[C]. 2005. 324-331.

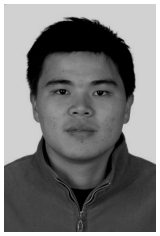
[14] DONG D, LI M, LIU Y, *et al*. Topological detection on wormholes in wireless ad hoc and sensor networks[J]. IEEE /ACM Transactions on Networking, 2011, 19(6):1787-1796.

[15] LAZOS L, POOVENDRAN R. SeRLoc: robust localization for wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2005, 1(1): 73-100.

[16] LAZOS L, POOVENDRAN R. HiRLoc: high-resolution robust localization for wireless sensor networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2):233-246.

[17] WU J, CHEN H, LOU W, *et al*. Label-based DV-Hop localization against wormhole attacks in wireless sensor networks[A]. Proceedings of IEEE NAS[C]. 2010.79-88.

作者简介：

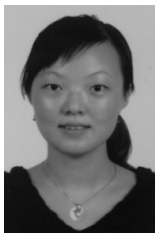


陈鸿龙（1984-），男，福建泉州人，中国石油大学（华东）副教授，主要研究方向为无线传感网络、容迟网络和移动自组织网络。

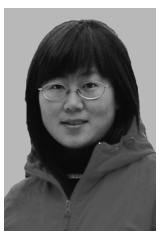
王志波（1984-），男，山东潍坊人，博士，武汉大学副教授，主要研究方向为无线传感器网络与移动感知网络。

王智（1969-），男，辽宁锦州人，博士，浙江大学副研究员、博士生导师，主要研究方向为无线传感网络、实时与工业通信、网络控制、多移动机器人以及分布式估计与监测。

许江铭（1991-），男，浙江东阳人，2013 年毕业于中国石油大学（华东），现任职于塔里木油田公司。



李燕君（1982-），女，江苏南通人，浙江工业大学副教授，主要研究方向为无线网络的协议与算法。



刘丽萍（1979-），女，河北保定人，天津大学副教授，主要研究方向为无线传感器网络。

doi:10.11959/j.issn.1000-436x.2015057

联合网络编码和中继选择的协作传输方案及其性能分析

冀保峰[1,2]，宋康[2]，王毅[2]，黄永明[2]，杨绿溪[2]
（1. 河南科技大学 信息工程学院，河南 洛阳 471023；2. 东南大学 毫米波国家重点实验室，江苏 南京 210096）

摘 要：研究了 Nakagami 信道中联合网络编码和双向协作中继选择的中断与平均误码率的性能，基于 3 个时隙的网络编码方案提出了一种最小化较差用户误码率的协作中继选择策略。在 Nakagami 信道下，从双向通信的角度，通过理论分析得出其中断概率和平均误码率的解析式和渐近式，同时推导了无协作中继选择时网络编码的中断概率和平均误码率解析式。通过理论分析发现，当 Nakagami 信道衰落参数降低时，联合网络编码的协作中继选择方案相对于无协作中继选择时的性能增益将逐渐升高。数值仿真实验结果表明，所提策略的平均误码率性能要显著高于无协作中继选择时的网络编码性能。

关键词：网络编码；中继选择；中断概率；平均误码率
中图分类号：TN925 **文献标识码**：A

Cooperative transmission scheme of relay selection combined with network coding and its performance analysis

JI Bao-feng[1,2], SONG Kang[2], WANG Yi[2], HUANG Yong-ming[2], YANG Lv-xi[2]
(1. Information Engineering College, Henan University of Science and Technology, Luoyang 471023, China;
2. School of Information Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: The outage probability and average BER (bit error ratio) of two-way relay system with network coding using relay selection were analyzed over Nakagami channels. The cooperative relay selection criterion of minimizing the worse user's BER was proposed based on three time slots network coding. The closed-form expressions of outage probability and average BER were derived through theoretical analysis from the point of two-way communication; meanwhile, the analytical expressions of outage probability and average BER of two-way relay system using network coding without cooperative relay selection were also obtained rigorously. By the analysis of two-way relay system without cooperative relay selection, it was found that the performance gains of the proposed scheme would increase gradually with the Nakagami channel fading parameters decreasing. Simulation results verified the correctness of theoretical analysis and illustrated that the performance of the proposed scheme can be improved significantly relative to the network coding without cooperative relay selection.

Key words: network coding; relay selection; outage probability; average bit error ratio

1 引言

由于无线通信系统受到多径衰落和多普勒效应的影响，导致无线通信网络性能的严重恶化，而协作分集的提出可以有效地对抗信道衰落。协作中继传输是无线通信网络中协作分集技术的重要实

收稿日期：2013-10-13；**修回日期**：2014-02-15
基金项目：国家自然科学基金资助项目(61201172, 61271018, 61372101, 61201176, U1404615)；毫米波国家重点实验室开放课题基金资助项目(K201504)；国家科技重大专项基金资助项目(2013ZX03003006-002, 2012ZX03004005-003)；教育部博士点基金资助项目(20100092110010)；河南省自然科学基金资助项目(142300410343)
Foundation Items: The National Natural Science Foundation of China (61201172, 61271018, 61372101, 61201176, U1404615); Open Funds of State Key Laboratory of Millimeter Waves (K201504); The National Science and Technology Major Project of China (2013ZX03003006-002, 2012ZX03004005-003); The Doctoral Program of Ministry of Education (20100092110010); The Natural Science Foundation of Henan Province (142300410343)