doi:10.3969/j.issn.1000-436x.2013.10.008

SenLeash：一种无线传感器网络虫洞攻击约束防御机制

胡蓉华，董晓梅，王大玲
(东北大学 信息科学与工程学院，辽宁 沈阳 110819)

摘 要：针对邻居发现或路由发现阶段可能受到虫洞攻击的问题，提出了一种约束防御机制 SenLeash，通过限制消息传输的距离来防御虫洞攻击。SenLeash 依赖 2 个因子：每个节点到初始基站的距离和一个精选的接收距离阈值。基于接收信号强度 RSSI，提出了一种 nRSSI 测量方法，在网络初始化阶段用来测量每个节点到初始基站的距离。基于每个节点的接收概率和 MAC 层的最大重传次数，对接收距离阈值的选择方法进行了研究。实验结果表明，SenLeash 可有效减少由虫洞攻击导致的虚假邻居节点个数和无效回复消息个数。
关键词：无线传感器网络；虫洞攻击；邻居发现；路由发现；RSSI；接收概率
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)10-0065-11

SenLeash: a restricted defense mechanism against wormhole attacks in wireless sensor network

HU Rong-hua, DONG Xiao-mei, WANG Da-ling
(College of Information Science and Engineering, Northeastern University, Shenyang 110819, China)

Abstract: The problem of wormhole attacks during neighbor discovery and route discovery phase was studied and a restricted mechanism, SenLeash, was presented to restrict the transmission range of messages and hence prevent wormhole attacks in WSN. The SenLeash depends on two factors: the distance of each node to an initial sink node and a chosen receiving distance. To obtain the distance of each node an initial sink node, a RSSI-based measure method nRSSI was proposed. Considering the receiving probability of each node and the maximum retransmission times of the MAC layer, the method of choosing an appropriate receiving distance was discussed. The simulation results demonstrate that the SenLeash can effectively decrease the number of invalidy neighbor nodes and invalidly reply messages caused by wormhole attacks in WSN.
Key words: wireless sensor network; wormhole attack; neighbor discovery; route discovery; RSSI; receiving probability

1 引言

无线传感器网络(WSN)是由大量集成了传感器模块、处理模块、通信模块和能量模块的节点组成的自组织网络，用于感知和收集各种感兴趣的物理或环境量。在军事和民用领域，WSN 都具有广泛的应用前景[1~3]。与传统网络和移动自组织网络相比，WSN 具有几个典型的特征。首先，节点资源受限。其次，通常部署在无基础设施区域，网络拓扑具有随机性。最后，网络节点个数可成百上千。由于存在这些特征，WSN 安全问题面临严峻挑战[4,5]。

虫洞攻击是 WSN 面临的最具挑战性的攻击之一。在这种攻击里，一个攻击节点 *A* 通过监听无线信道，记录其邻近节点发送的信息，然后通过一条高质量链路将记录的消息隧道传送给另一个离其很远的攻击节点 *B*；攻击节点 *B* 接收到来自攻击节点 *A* 发送的消息后在其本地重放[6]。这种攻击通过建立虚假的邻居节点或链路，可对 WSN 造成严重威胁。尽管有很多研究人员提出了许多应对虫洞攻击的机制[6~16]，但是大多数机制属于检测机制，要

收稿日期：2012-10-13；修回日期：2013-07-01
基金项目：国家自然科学基金资助项目(60873199)
Foundation Item: The National Natural Science Foundation of China (60873199)

么依赖精确的同步时钟，要么假设节点坐标位置信息或邻居节点信息已知。目前还没有针对网络初始化阶段进行防御的机制。

本文针对在网络初始化阶段，所有节点在未知自己位置信息和邻居节点信息的特殊条件下，提出了一种虫洞攻击约束防御机制 SenLeash，用于防御虫洞攻击和减轻虫洞攻击对网络造成的威胁。SenLeash 依赖 2 个因子：每个节点到初始基站的距离和一个精选的接收距离阈值。SenLeash 的主要思想是限制邻居发现消息 HELLO_MSG 的传输距离。在网络初始化阶段，每个接收节点通过将预选的接收距离与自己和发送节点到初始基站的距离差的绝对值比较，判断是否回复加入到发送节点邻居表的信息。为了测量每个节点到初始基站的距离，本文提出了一种基于 RSSI 的测距方法 nRSSI，可将距离误差精确到可接受的范围内。为了选择合适的接收距离阈值，通过结合节点的接收概率和 MAC 层的最大重传次数，对接收距离阈值的选择进行了研究。

本文的主要贡献包括 3 个方面。首先，本文提出并实现了一种在网络初始化阶段防御虫洞攻击的方法 SenLeash，不需要额外的硬件设备。在网络初始化阶段，所有节点对自己位置信息和邻居节点信息未知，有别于许多已有的检测机制。其次，基于对数正态 shadowing 路径损失模型通过仿真实验验证了 SenLeash 的可行性。SenLeash 可有效减少建立虚假邻居节点个数和对虚假重播消息回复的消息个数。而且适用于多基站环境和能耗较少，每个节点仅需要额外消耗接收 200 个左右信元分组的能量，用来估计到初始基站的距离。最后，本文研究了如何选择接收距离，减少无意义的回复，可为其他提高网络性能的协议提供参考，特别是对位置信息已知的环境。

2 相关工作

已有应对虫洞攻击的解决机制大多数属于检测机制，没有从防御视角进行考虑。文献[17]对目前 WSN 中虫洞攻击应对机制作了分类介绍。

文献[6]提出了一种称为 packet leash 的一般机制，用于检测和防御移动自组织无线网络中的虫洞攻击。一个 leash 是加入到分组中的任何信息，用于限制分组的最大允许传输距离[6]。文献[6]提出了 2 种类型的 leash：地理 leash 和时间 leash。对于地理 leash，需要每个节点提前知道自己的位置坐标信息，而在 WSN 很多场景里，由于存在各种攻击，每个节点的位置信息很难正确获得[7]，文献[6]也没有讨论如何获得位置信息的具体方法。对于时间 leash，不适用于 WSN，需要所有节点同步时钟达到几十纳秒的精度。例如，如果通信距离为 30 m，传输时间仅需要 100 ns。如果同步时钟精度超过 50 ns，有可能将不在通信范围内的节点认为是邻居节点，将在通信范围内的节点认为是非邻居节点。为了防御虫洞攻击，同步时钟精度必须小于 50 ns，传感器节点很难达到这一要求。与文献[6]类似，有许多基于消息传输时间信息来检测虫洞攻击的方案，比如 TTM[8]、SECTOR[9]以及 DelPHI[10]。

文献[11]提出了一种基于多维缩放可视化虫洞(MDS-VOW)检测机制，该方案存在 2 个主要问题。首先，MDS-VOW 需要每个节点依据 RSS 测量到所有邻居节点的距离，通信代价可能会很大，而且是否可行有待研究。文献[11]没有给出具体如何依据 RSS 测量以及 RSS 测量误差，仅假设存在一个测量误差范围，在什么条件下才能达到假设的误差范围没有研究讨论。其次，文献[11]给出的网络引导方法不能防御虫洞攻击，达到基站获得所有节点的邻居表的目的。如图 1 所示，假如恶意节点 A 记录节点 A 的路由发现分组后，通过一条高质量链路传输给恶意节点 B；恶意节点 B 向其周围节点重放接收的路由发现分组，例如节点 M、N、V、W、U 和 T。这样，依据文献[11]提供的方法，恶意节点 B 周围的节点将更新它们到基站的路径长度为 1 跳，将节点 A 作为它们下一跳节点。这些虚假的 1 跳节点将重放它们接收的路由发现分组，进而网络将被这些虚假 1 跳节点划分，影响 MDS-VOS 对虫洞攻击的检测。

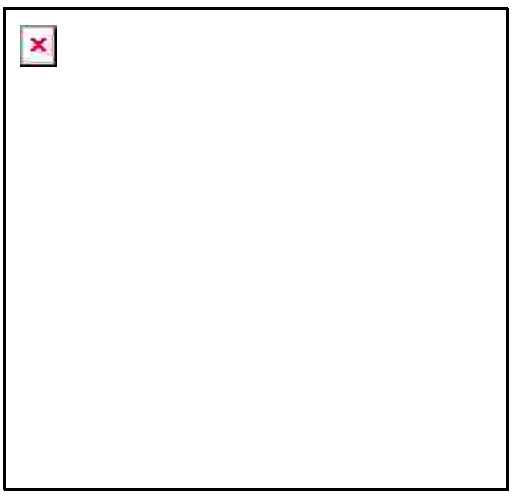

图 1 虫洞攻击一般模型

文献[12]提出了一种基于时间和信任的检测(TTD)机制，用于检测被捕获节点发送修改的虚假包的虫洞攻击。基于时间模块需要每个节点获得自己的邻居节点信息。然而，安全邻居发现是非常困难的[18,19]，在邻居发现和路由发现过程中文献[12]没有给出任何防御机制。文献[13]提出了一种基于信任的模式，用于识别隔离虫洞攻击。与文献[12]类似，节点监视邻居节点的投递行为，测量邻居节点的信任情况。

文献[14]提出了一种安全邻居发现和本地监视机制 LiteWorp，用于检测虫洞攻击。然而，LiteWorp 依赖对密钥建立 2 跳邻居表，仍然可受到虫洞攻击。即使节点存储空间足够，在网络部署时所有节点对存在共享对密钥，攻击者通过重放邻居发现分组，可建立虚假邻居节点。如果通过密钥管理协议建立邻居节点间的对密钥，在对密钥建立的过程中就有可能受到虫洞攻击。文献[15]提出了一种基于本地监视和安全中心结合的机制 MOBIWORP，用于减轻虫洞攻击对移动多跳无线网络的危害。文献[7]提出了一种基于一致性检验的安全邻居证实(SNV)协议。然而，文献[7]假设邻居节点已知，没有考虑在邻居发现阶段可能受到虫洞攻击的威胁，同时每个节点需要拥有 2 个网络接口。

文献[16]提出了一种无线指纹的机制，可用于防御虫洞攻击，然而还未实现节点直接识别指纹。其中有很多问题有待进一步研究，比如更好的指纹形成方法，噪声和移动对指纹识别过程的影响等。

3　系统模型

3.1　网络模型

假定一个静态 WSN 由一个基站和 N 个传感器节点组成。基站是一个功能强大的节点，拥有更多资源，同时是安全的。假定传感器节点有多个发射(Tx)功率等级，例如，CC2420 有 8 个不同的 Tx 等级。假定基站以某一特定 Tx 等级发射消息时，其通信范围可覆盖整个部署区域。所有节点共享一个全局密钥，用于安全初始化，同时每个节点拥有唯一的识别编号 ID。

3.2　攻击模型

本文主要考虑在网络初始化阶段，可能受到的外部虫洞攻击。与许多机制一样，假定在网络初始化阶段，没有网络节点被攻击者捕获。不同的是，本文没有假定在此阶段网络中也不存在外部虫洞攻击。因为发起虫洞攻击，攻击者不需要获得网络的秘密信息。假定攻击的目的是在节点间建立虚假链路，扰乱邻居发现和路由发现，进而影响路由和网络性能。假定虫洞攻击者拥有自己的安全机制，比如密钥管理协议，每对虫洞节点间可以安全通信。针对邻居发现或路由发现，一个攻击节点 A 首先封装已记录的分组，然后通过一条高质量或者外部信道链路发送至其合作攻击节点 B。攻击节点 B 解封装对应分组后，以一定 Tx 等级广播解封装的分组。

4　SenLeash：虫洞攻击约束防御机制

SenLeash 通过约束限制邻居发现消息的传输距离来防御虫洞攻击，有别于许多已提出来的检测机制。

4.1　SenLeash 防御虫洞攻击

SenLeash 机制包括 2 个方面：在发送消息中嵌入额外的约束信息；检查消息的有效性。其依赖 2 个因子：每个节点到初始基站的距离和一个精选的接收距离阈值。假定每个节点 i 到初始基站的距离记为 vd_i，测量 vd_i 的方法将在 4.2 节介绍。

在网络初始化阶段，当节点 i 发送一个 HELLO 消息时，将 Tx 功率 P_t 和距离信息 vd_i 加入到分组中，如图 2 所示，并使用全局密钥加密。当节点 j 接收到来自节点 i 发送的 HELLO 消息后，首先比较 P_t 和接收信号强度指示(RSSI)读数值 P_r，检查式(1)是否成立

$$P_r > P_t \tag{1}$$

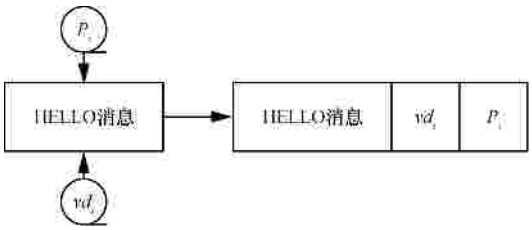

图 2　发送一个 HELLO 消息

RSSI 提供了信号在接收器前端的强度信息，对每个成功接收的消息，其值可从 radio 模块获得，比如 CC2420 radio。如果式(1)为真，则认为接收的 HELLO 消息为异常分组，丢弃。由于无线通信存在路径损失，如果式(1)为真，可认为接收的消息来自一个高 Tx 功率的恶意节点。如果式(1)为假，则计算 vd_i 和 vd_j 差的绝对值 $?_{vd}(ij)$，检查式(2)是否成立，其中 R_{Tx} 为精选的接收距离阈值

$$?_{vd}(ij) > R_{Tx} \tag{2}$$

如果式(2)为真，则认为接收的分组为异常分组，可能是由虫洞节点重放。接收 HELLO 消息的处理过程如图 3 所示。

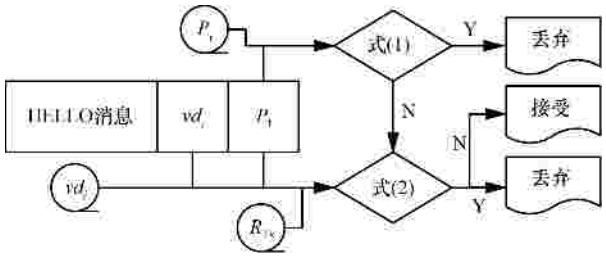

图 3 接收一个 HELLO 消息

SenLeash 可从 2 个方面约束防御虫洞攻击。如图 4 所示，假设节点 A 以某一低 Tx 功率发送 HELLO 消息发现其邻居节点，通信半径为 R_1。节点 A 到初始基站的距离记为 vd_A。在邻居发现阶段，所有传感器节点以相同的低 Tx 功率发送消息。

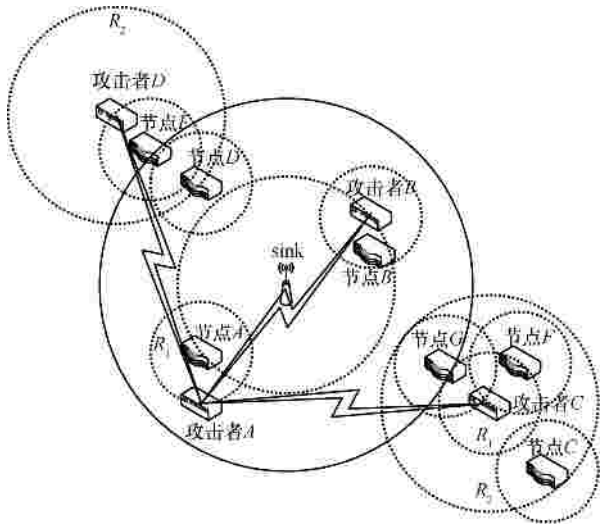

图 4 SenLeash 约束防御虫洞攻击

SenLeash 可以约束虫洞节点对的部署位置，给攻击节点对的部署带来难度。在没有 SenLeash 机制时，攻击者 A 可以将 HELLO 消息隧道传输到位于网络任何位置的恶意节点，例如攻击节点 B、C、D，然后这些恶意节点可以以低或者高 Tx 功率重放接收的 HELLO 消息分组。然而，如果使用 SenLeash，攻击节点 A 为了给节点 A 建立尽可能多的虚假邻居节点，仅能将 HELLO 消息分组隧道传输到以初始基站为圆心，以 vd_A 为半径的圆上，例如攻击节点 B。如果攻击节点 A 将 HELLO 消息隧道传输给攻击节点 C 或者节点 D，传感器节点接收到来自攻击节点 C 或者节点 D 重放的 HELLO 消息后，通过检查式(1)和式(2)成立与否，大量传感器节点可以过滤掉重放的 HELLO 消息分组。因此，SenLeash 可以减轻虫洞节点对(A,C)和(A,D)对节点 A 的威胁。SenLeash 可减轻以高 Tx 功率重放 HELLO 消息造成的威胁，减少回复虫洞节点重放消息的节点个数和由虫洞攻击建立的虚假邻居节点个数。如果攻击节点 C 以高 Tx 功率重放 HELLO 消息，通信半径为 R_2，可影响更多的传感器节点，例如节点 C、节点 F、节点 G 都会受到影响。当没有 SenLeash 时，节点 C、节点 F、节点 G 将回复接收到 HELLO 消息分组。假设攻击节点 C 在节点 C 通信范围之外，则仅可以接收到节点 F 和节点 G 回复的加入消息。如果网络中存在很多类似节点 C 的节点，这些节点回复 HELLO 消息会产生严重碰撞，形成一个 Flooding 攻击。然而，如果使用 SenLeash，节点 C、节点 F 和节点 G 首先检查式(1)和式(2)成立与否。如果对于节点 C 和节点 F 式(2)为真，仅节点 G 将回复重放的 HELLO 消息。因此，在这种情况下，SenLeash 可以减少由虫洞攻击引起的欺骗回复，减少建立虚假邻居节点的概率以及产生 Flooding 攻击的概率。

如果攻击节点 C 以某一低 Tx 功率重放 HELLO 消息，当没有 SenLeash 时，节点 F 和节点 G 首先检查式(1)和式(2)成立与否。如果对于节点 F 式(2)为真，仅节点 G 将回复重放的 HELLO 消息。因此，在这种情况下，SenLeash 也可以减少由虫洞攻击引起的虚假回复和建立虚假邻居节点的概率。

4.2 nRSSI 估计到初始基站距离 *vd*

为了减少节点成本，假定节点没有额外的定位设备，本文提出了一种基于 RSSI 的测量距离方法。由于基于 RSSI 的测距方法有一个缺点：估计误差相对较大，在网络初始化阶段不适用于邻居节点对间的距离测量。因此本文利用 RSSI 和基站相对强大的功能，在网络初始化阶段仅测量每个节点到初始基站的距离，以减少能量开销和初始化时间。

按照普遍应用于 WSN 的无线传输模型，对数正态 shadowing 路径损耗模型，可以估算发送节点和接收节点间的距离。对数正态 shadowing 模型可由式(3)表示。其中 $PL(d)$表示距离为 d 的路径损失；$PL(d_0)$为参考距离为 d_0 的路径损失；$?$ 为路径损失指数；X_s 为均值为 0，标准差为 s 的高斯随机变量。

$$PL(d) = PL(d_0) + 10h\lg(d/d_0) + X_s \qquad (3)$$

由于 $PL(d)$为 Tx 功率 P_t 和接收信号的 RSSI 值

P_r 之差，当 d_0=1 m，可以由式(4)计算距离 d

$$d = 10^{(P_t - P_r - PL(d_0) - X_s)/(10h)} \tag{4}$$

由于 X_s 是随机变量，仅依靠单一 RSSI 采样不能计算出精确的距离 d。然而 X_s 是一个均值为 0 的随机变量，可以通过采样一定数量的 RSSI，以平均距离 d_a 作为距离 d 的近似值，本文称之为 nRSSI 测量方法。平均距离 d_a 可由式(5)计算

$$d = 10^{(PL(d)_a - PL(d_0))/(10h)} \tag{5}$$

其中，$PL(d)_a$ 为 n 个采样的平均路径损失值 $\sum_{i=1}^{n} (P_t - P_{ri}) / n$。平均距离将作为节点到初始基站的近似距离，记为 vd。

nRSSI 测量方法很容易实现。在网络初始化阶段，初始基站以某一特定高 Tx 功率向全网发射 n 个广播信元分组，记为 Initail-Pkt。Initail-Pkt 包含 Tx 功率值 P_t-$high$ 和一个序列号 sn，使用全网共享的密钥加密。序列号 sn 用于标记 Initail-Pkt，防止恶意节点重放 Initail-Pkt，影响传感器节点测量距离。由于假设在网络初始化阶段没有节点被捕获，因此攻击节点不能恶意修改 Initail-Pkt 包含的内容。

传感器节点获得初始基站距离的处理过程如图 5 所示。当传感器节点 i 接收到序列为 sn_j 的 Initail-Pkt，首先通过比较 sn_j 与记录最近接收分组的序列号的计数器 cnt，检查接收的 Initail-Pkt 是否为新鲜分组。如果 Initail-Pkt 为新鲜分组，节点 i 记录相应的 RSSI 值 P_{rj} 并更新 cnt=sn_j。当基站发送完 n 个 Initail-Pkt 后，节点 i 按照式(5)计算到初始基站的距离。

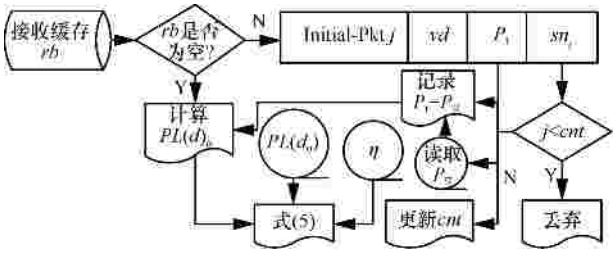

图 5　计算距离 vd 的处理过程

4.3　接收距离阈值 R_{Tx} 的选择

对一定的 Tx 功率，选择恰当的接收距离阈值可提高网络的性能。如果选择的接收距离阈值过小或过大，真实的邻居节点可能被认为虚假的邻居节点或者虚假的邻居节点认为是合法的邻居节点。由于使用 nRSSI 或者其他方法测量距离 vd 存在误差 d_{error}，假设最大的测量距离误差为 maxd_{er}。

按照对数正态 shadowing 路径损失模型，X_s 服从 $N(0,s^2)$分布，则 $PL(d)$也为高斯随机变量且服从 $N(PL(d_0)+10h\lg(d/d_0), s^2)$。对于一定的 Tx 功率 P_t，RSSI 值 P_r 也为高斯随机变量且服从 $N(P_t - PL(d_0) - 10h\lg(d/d_0), s^2)$。

由于 radio 模块存在接收敏感值 P_0，例如 CC2420 的 P_0=- 95dBm，当 P_r>P_0 时 radio 模块才能成功接收相应的信号。当发送节点和接收节点距离 d 时，可以按照式(6)计算接收节点的接收概率 $Prob_d$，其中，Q 为式(7)定义的函数。

$$\begin{aligned} prob_d(P_r > P_0) &= prob_d((P_r - P_t + PL(d_0) + 10h \cdot \lg(d/d_0))/d > (P_0 - P_t + PL(d_0) + 10h\lg(d/d_0))/d) \\ &= Q((P_0 - P_t + PL(d_0) + 10h\lg(d/d_0))/d) \end{aligned} \tag{6}$$

$$Q(z) = \frac{1}{\sqrt{2\pi}} \int_z^{+\infty} \exp(-\frac{x^2}{2}) \mathrm{d}x \tag{7}$$

由式(6)和式(7)，通过查找 Q 函数值表可得到 $Prob_d$。由式(6)可知，接收节点与发送节点距离越大，接收概率越小，因此每个节点应选择接收概率大的邻近节点作为邻居节点。从而，选择一个恰当的接收距离阈值需要选择一个恰当的接收概率阈值 P_{MAC}。

在网络协议栈中，仅 MAC 层的最大重传次数 maxTx 可影响到节点在路由层的接收概率。如图 6 所示，假设 maxTx=m，在网络层接收概率需要达到 P_{net}，则可通过式(8)和式(9)计算 P_{MAC}。

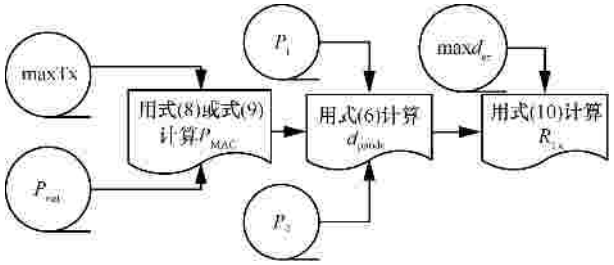

图 6　计算接收距离阈值 R_{Tx}

$$1 - \left[(1 - P_{MAC})(1 + P_{MAC})\right]^m > P_{net} \tag{8}$$

$$1 - (1 - P_{MAC})^m > P_{net} \tag{9}$$

对于式(8)，仅当 MAC 层确认包成功接收后，一次传输才认为成功完成。而对于式(9)，无需 MAC 层确认分组。为了确保通信的有效性和及时性，通

常 maxTx=2，而且需要 MAC 层确认分组，例如 SMAC[20]、TMAC[21]、IEEE 802.15.4[22]等已知的MAC 协议。如果 P_{net}=0.963 7，依照式(8)可得 P_{MAC}=0.9。

当接收概率阈值 P_{MAC} 确定后，对于某一特定的 Tx 功率 P_t 和 radio 接收敏感值 P_0，可依据式(6)计算接收概率距离 d_{pnode}，如图 6 所示。当发送节点和接收节点间的距离 $d_{sr}<d_{pnode}$ 时，对一次发射，分组被成功接收的概率大于 P_{MAC}。由于 radio 模块的 Tx 功率等级个数有限，例如 CC2420，因此在网络部署前，可以将 d_{pnode} 预载到节点中。

假设最大测量距离误差为 $\max d_{er}$，因此节点间的最大距离误差为 $2\max d_{er}$。为了使距离发送节点小于 d_{pnode} 的所有高接收概率节点都作为候选邻居节点，由 d_{pnode} 和 $\max d_{er}$ 可依据式(10)计算接收距离阈值 R_{Tx}，如图 6 所示。

$$R_{Tx} = d_{pnode} + 2\max d_{er} \tag{10}$$

由式(10)可知，如果 $\max d_{er}$ 过大，低接收概率节点甚至完全接收不到的节点将被包括在候选邻居节点中。对于前者，可能建立链路质量较差的邻居节点；对于后者，则给虫洞攻击提供了攻击机会，使得 SenLeash 防御性能较低。为了评估 R_{Tx}，本文引入评估概率 P_{evalu} 对其进行评估。P_{evalu} 为 R_{Tx} 对应的接收概率，可由式(6)计算得到。P_{evalu} 反映了候选邻居节点接收概率达到的等级。当 P_{evalu} 越小，允许回复 HELLO 消息分组的区域就越大，对虫洞攻击的防御性能相对就越弱。

4.4 多基站扩展

当网络监测区域大于单个基站最大通信范围 bs_{cell} 时，需要向监测区域部署多个基站，如图 7 所示。对于多基站情况，由于基站节点功能强大，基站节点间的虫洞攻击防御可由文献[6]中的 leash 机制防御，例如图 7 中的基站节点 A、B、C。因此对于多基站情形，仅需要额外考虑位于不同基站通信范围内普通节点受虫洞攻击的问题，如图 7 所示，即受到攻击节点 a、b、c 合作攻击的问题。

为了防御如图 7 中受到攻击节点 a、b、c 合作攻击问题，可将基站和普通节点分组部署。假设网络检测区域可逻辑划分成 n_{ex} 个大小为 bs_{cell} 区域，将基站和普通节点分成 n_{ex} 组，每组中有一个基站和 m_{ex} 个普通节点。每组中的所有节点共享一个唯一的全局组密钥，用于安全初始化。在部署时，将同组节点部署于相同划分区域，不同组节点部署于不同划分区域，且基站部署于划分区域中心位置区域。

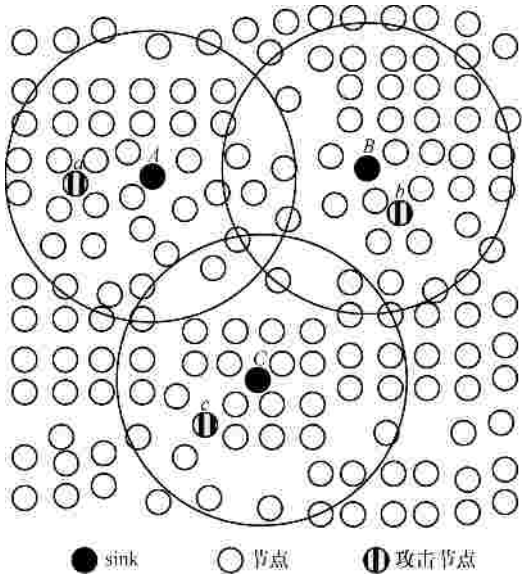

图 7 多基站体系结构

在网络初始化使用 nRSSI 计算到对应基站距离时，由于每组中的基站与对应组的普通节点相关联，具有共同的组密钥，因此，普通节点只接受与其对应的基站节点的广播信元分组，即可防御如图 7 中受到攻击节点 a、b、c 合作攻击影响测距的问题。在网络初始化节点发送 HELLO 消息时，可在发送的消息中额外嵌入对应的基站信息，比如基站 ID 信息，并使用组密钥加密，从而实现防御如图 7 中受到攻击节点 a、b、c 合作攻击影响邻居发现的问题。因此对于多基站情况，通过分组部署方式可转换为多个独立的单基站情形，SenLeash 可较容易地扩展到多基站的应用。

4.5 与已有应对机制比较

SenLeash 与其他一些重要的应对虫洞攻击机制的比较如表 1 所示。

由表 1 可知，已有方案大多数属于检测机制，依赖的假设条件是在网络初始化安全完成之后对虫洞的检测，需要节点的位置坐标信息或邻居节点信息。如果不能保证网络安全初始化，这些检测机制性能会受到影响，甚至失效。本文方案是在文献[6]中的地理 leash 基础上结合 WSN 的特点，针对网络初始化阶段节点坐标位置等信息未知的情况下，实现的一种有效防御机制 SenLeash。

表 1　已有应对虫洞方案与本文工作比较

研究工作	机制	方法	同步时钟	位置信息或邻居节点信息	额外硬件设备
Hu 等[6]	防御方法	地理和时间 leash	精确的同步时钟；不适合于 WSN	对地理 leash，每个节点需要知道自己的位置坐标；没有讨论如何获取位置坐标	GPS
Shokri 等[7]	检测方法	使用一致性检测进行安全邻居证实	微妙级的精确同步时钟	假设每个节点已知各自邻居节点信息及对密钥信息	2 个网络接口
Wang 等[11]	检测方法	基于 MDS 可视化	无	基于 RSS；需要基站获得每个节点的邻居表信息；设计的网络引导方法不能实现免疫虫洞攻击	无
Ozdemir 等[12]	检测方法	基于时间和信任	N/A	需要安全邻居发现机制	无
Khalil 等[14]	检测方法	安全邻居发现和本地监视	无	需要预分配对密钥管理协议；未考虑在预分配对密钥阶段可能受到的虫洞攻击	无
Rasmussen 等[16]	检测和防御方法	radio 指纹识别	无	无	指纹设备
本文机制	防御方法	SenLeash	无	基于 nRSSI 方法获得节点到初始基站距离	无

5　实验评估

本文所有实验在基于 OMNeT++[23]平台的无线传感器网络模拟器 Castalia [24]里完成。

5.1　节点接收概率

节点接收概率主要用于：验证到发送节点距离不同的节点，接收概率不同；验证本文基于 Castalia 实现的对数正态 shadowing 模型的时变参数文件的有效性。

虽然 Castalia 已实现了一个对数正态 shadowing 模型，但是仅用于模拟平均路径损失。将该模型的对应参数设置后，如果没有相应的时变模型，在一次模拟过程中，对于一条特定的链路其路径损失是不变的。目前，Castalia 仅为个人区域网(BAN)提供了一个时变参数文件，不适用于 WSN。因此需要为 WSN 提供一个类似的时变参数文件，以模拟更真实的对数正态 shadowing 模型。

为了兼容 Castalia 的无线信道模型，本文参照 Castalia 定义的时变参数文件格式[25]，创建了一个名 WSNtest 的参数文件。WSNtest 包括 2 层概率密度函数(pdf)，第一层有 1 001 个值，第二层有 10 个值。每个值为一个 double 类型的实数或者为 1 个字母，其中前者由高斯分布 $N(0,16)$产生，用于模拟式(3)中的 X_s，均值为 0，s=4；后者用于指向下一层 pdf。一个 pdf 定义了选取每个值的概率，例如，假设一个 pdf 里有 10 个不同取值，则取每一个值的概率为 0.1。

为了验证 WSNtest 可行性，本文将下面的实验结果与通过式(6)计算的结果进行了比较。500 个传感器节点随机均匀分布在 100 m×100 m 的区域，基站位于部署区域中心。$PL(d_0$=1 m)=47 dBm，γ=2.4。radio 模块为 CC24020，Tx 功率 P_t=- 25 dBm。基站节点共发送 9 999 个信元分组，其他节点统计接收到的分组个数，估计接收概率，结果如表 2 所示。

表 2　不同距离 *vd* 的接收概率

到 sink 的距离	估计概率	计算概率
1.897 8	0.999 9	0.999 9
5.731 2	0.884 188	0.884 9
10.136 4	0.384 738	0.385 9
15.194	0.089 609	0.090 1
17.570 9	0.044 104 4	0.047 2

由表 2 可知，距离基站越远，节点的接收概率越小，而且估计的接收概率非常接近理论计算的接收概率，这表明实现的时变参数文件 WSNtest 是可行的，可反映出对数正态 shadowing 模型的时变特性。

5.2　nRSSI 测量距离误差统计

考虑到 Castalia 所有节点都具有相同的资源，没有提供类似基站功能相对强大的节点，因此对相应参数进行如下设置：Tx 功率设置为最大 P_t=0 dBm；部署区域设置为 50 m×50 m，以便所有节点可以较高概率接收到初始基站发送的 Initial-Pkt；传感器节点

个数为 1 000；其他参数同 5.1 节。

实验结果如表 3 所示，其中 n 表示初始基站发送的 Initial-Pkt 总个数；c_1，c_2 和 c_3 分别表示测量距离误差落在区间 $[0,1)$，$[1,2)$ 和 $[2,3)$；c_4 表示测量距离误差大于 3 m；*max* 表示最大的测量误差；*mean* 和 *variance* 分别表示测量误差的均值和方差。

由表 3 可知，采样次数越大，测量误差越小；大多数距离误差小于 3 m。由于 X_s 是一个均值为 0 的高斯随机变量，采样次数越多，均值越接近于 0，因此使用式(5)估计的距离越接近真实的距离。当 $n > 200$ 时，几乎没有距离误差超过 3 m。为了减少部署代价，本文假定传感器节点没有安装额外的定位设备。因此，为了让传感器节点可以获得它们到初始基站的距离，由初始基站发送一定数量的 Initial-Pkt，以实现在网络初始化阶段防御虫洞攻击，这种策略的成本和能量开销很小。

表 3 不同采样次数 n 距离误差统计

n	c_1	c_2	c_3	c_4	*max*	*mean*	*variance*
49	686	234	67	13	4.1	0.8	0.5
99	823	156	20	1	3.5	0.6	0.3
149	874	122	3	1	3.2	0.5	0.2
199	909	87	4	0	2.4	0.4	0.15

5.3 防御效果对比实验

为了验证 SenLeash 的防御效果，本节将本文方法与文献[7]中的地理 leash(gLeash)和时间 leash(tLeash)、文献[7]的 SNV、文献[11]的 MDS、文献[12]的 TTD 和文献[14]的 LiteWorp 进行了对比实验。对于 gLeash，依据文献[6]，假设通过某种方式每个节点已获取自己的位置坐标信息；任意两节点距离的最大相对误差为 3 m。对于 tLeash，分别考虑了节点间的最大同步时钟误差 $?_{syn}$ 为 100 ns、50 ns 和 10 ns 的情况。当 $?_{syn}$=10 ns 时，在约束分组传输最大距离上 tLeash 和 gLeash 是等价的，都为(R_{comm}+3) m，因此在这种情况下两者的防御效果也是等价的，其中 R_{comm} 为节点的通信半径。对于 R_{comm} 取值考虑了 2 种情况：$R_{comm}=R$ 时表示采用单位圆通信模型使用的通信半径；$R_{comm}=r$ 时表示采用本文计算的接收概率距离 d_{pnode}。在后文中对 gLeash 的对比由 tLeash $?_{syn}$=10 ns 时的情况表示。

实验参数设置如下：100 个传感器节点随机均匀分布在 50 m×50 m 的区域；9 个固定坐标节点，如表 4 所示，其中 ID=0 的节点为基站；ID=7，8 的节点发送邻居发现分组；ID 节点对(1,2)、(3,4)和(5,6)分别表示 3 对不同情况的虫洞攻击节点；接收概率阈值 P_{MAC}=0.9，默认的 Tx 功率 P_t=- 25 dBm，因此依据式(6)，d_{pnode}=5.54 m；依据 5.2 节，maxd_{er}=3 m，因此接收距离阈值 R_{Tx}=11.54 m；其他参数同 5.1 节。按照式(6)可计算出 P_{evalu}=0.27。

对每一次实验包括 2 个阶段：第一阶段，初始基站节点广播 200 个信元分组，其中 Tx 功率 P_t=0 dBm，其他节点使用 nRSSI 计算到初始基站的距离；第二阶段，节点 7 和节点 8 发送邻居发现分组，记为 HELLO_ MSG，其中默认 Tx 功率 P_t=- 25 dBm。

当虫洞节点 1 接收到来自节点 7 发送的 HELLO_MSG，隧道发送给它的合作节点 2。节点 2 随后重播接收到的 HELLO_MSG，其中 Tx 功率 P_t=- 25 dBm。在这种情况下，节点 2 和节点 7 距离初始基站的距离相同，SenLeash 不能过滤掉重放的 HELLO_MSG。

表 4 固定坐标的节点

ID	*X*	*Y*
0	25	25
1	11	11
2	40	40
3	24	24
4	40	25
5	25	26
6	25	10
7	10	10
8	24	25

当虫洞节点 3 接收到来自节点 8 发送的 HELLO_MSG，隧道发送给它的合作节点 4。节点 4 随后重播接收到的 HELLO_MSG，其中 Tx 功率 P_t=- 25 dBm。在这种情况下，节点 4 和节点 8 到初始基站的距离分别是 15 m 和 1 m，因此一些节点使用 SenLeash 能过滤掉重放的 HELLO_MSG，具体依赖受影响节点的位置。

当虫洞节点 5 接收到来自节点 8 发送的 HELLO_MSG，隧道发送给它的合作节点 6。节点 6 随后重播接收到的 HELLO_MSG，其中 Tx 功率 P_t=- 15 dBm，比默认的 Tx 功率大。与第二种情形类似，节点 6 和节点 8 距离初始基站的距离分别是 15 m 和 1 m。在这种情形下如果没有防御策略，与以默认 Tx 功率重播 HELLO_MSG 相比，由于距离

越大接收概率越小，攻击者虽然不能建立起明显多的虚假邻居节点，但可以引起更广区域的节点回复 HELLO_MSG，可能引起 Flooding 攻击，进而使得网络初始化失败。

图 8 和图 9 为实验结果，其中所有结果是对 5000 次实验取平均值得到，节点 7 和节点 8 为没有受到虫洞攻击影响的结果，它们受虫洞攻击影响的结果由相应虫洞节点对应的结果表示。

图 8 显示了每个节点建立的邻居节点个数。由图 8 中节点 7 和节点 8 的结果可知，网络在没有受到虫洞攻击的情况下，除位于部署区域边缘节点外，节点的邻居个数为 8。由于 SNV、MDS、TTD 和 LiteWorp 属于事后检测机制，因此在邻居发现阶段它们建立的邻居节点个数和未使用防御策略的结果一样。当节点与邻居发现节点距离越远时，tLeash 防御效果越好，如节点 4 和节点 2 结果所示。当节点与基站距离和邻居发现节点与基站距离相差越大时，SenLeash 防御效果越好，如节点 2 和节点 4 结果所示。由节点 2 结果可知，当节点与基站距离和邻居发现节点与基站距离相差小于接收距离阈值 R_{Tx} 时，SenLeash 不能过滤掉节点 2 重播的 HELLO_MSG。由节点 4 和节点 6 结果可知，当节点与基站距离和邻居发现节点与基站距离相差大于接收距离阈值 R_{Tx} 时，SenLeash 防御效果优于 $?_{syn}$=100 ns 和 50 ns 的 tLeash 情况。这是由于当 $?_{syn}$>50 ns 时 tLeash 允许分组传输的通信距离更远。当 $?_{syn}$=10 ns 时，tLeash 的防御效果要优于 SenLeash。

图 9 显示了每个节点影响的回复节点个数。由图 9 可知，由于 SNV、MDS、TTD 和 LiteWorp 属于事后检测机制，因此在邻居发现阶段它们影响的回复节点个数和未使用防御策略的结果一样。在第二种和第三种情形下，当节点与基站距离和邻居发

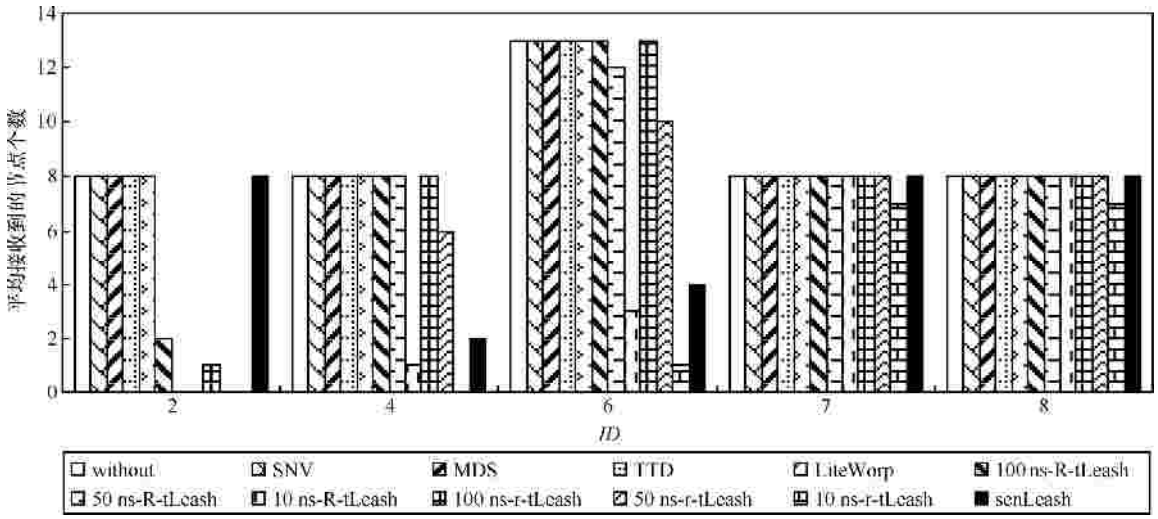

图 8　节点建立的邻居节点个数

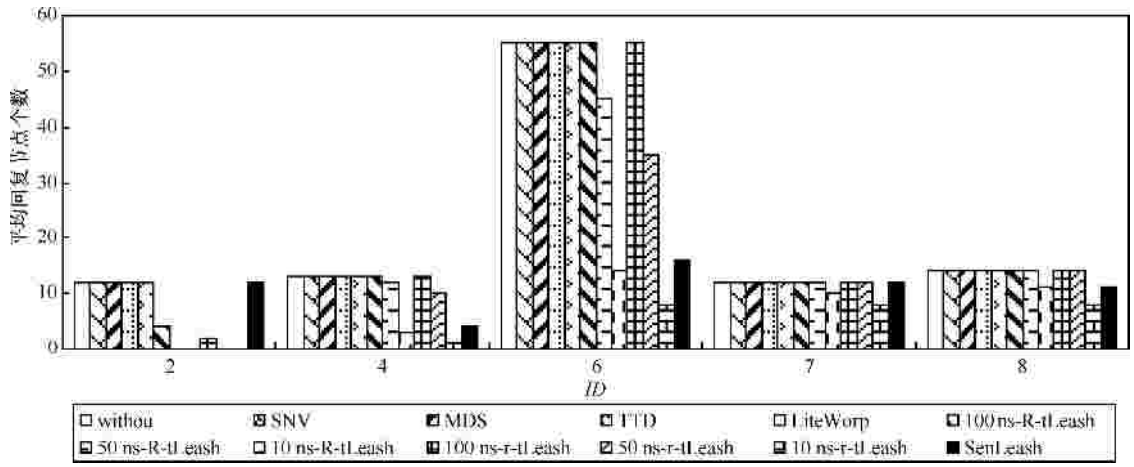

图 9　节点影响的回复节点个数

现节点与基站距离相差大于接收距离阈值 R_{Tx} 时，SenLeash 防御效果优于 $?_{syn}$=100 ns 和 50 ns 的 tLeash 情况，有更多受影响的节点不用发送回复分组，尤其对第三种情形。当 $?_{syn}$=10 ns 时，tLeash 的防御效果要优于 SenLeash。由图 8 和图 9 中的节点 8 结果可知，在不考虑虫洞攻击影响下，由于 P_{evalu}=0.27，SenLeash 可以让一些接收概率小于 0.27 的节点避免回复 HELLO_MSG，避免建立链路质量差的邻居节点，同时不影响建立的正常邻居节点个数，这有利于提高网络的性能。

由以上结果可知，在邻居发现阶段，SenLeash 防御效果优于 SNV、MDS、TTD 和 LiteWorp。当节点与基站距离和邻居发现节点与基站距离相差大于接收距离阈值 R_{Tx} 时，SenLeash 防御效果优于 tLeash。虽然当 $?_{syn}$=10 ns 时，tLeash 的防御效果要优于 SenLeash，但是目前传感器节点的同步时钟往往只能达到微妙级的精度，要达到 10 ns 级的精度是很难实现的。当节点与基站距离和邻居发现节点与基站距离相差小于接收距离阈值 R_{Tx} 时，虽然 SenLeash 不能防御虫洞节点重播的 HELLO_MSG，但是这也需要虫洞节点与基站距离和邻居发现节点与基站距离相等或接近时，这些节点才会或可能会受到影响，而这无疑给虫洞节点对的部署带来了困难。同时虽然 gLeash 的防御效果要优于 SenLeash，但是这需要额外的硬件设备支持和其他安全精确定位协议的支持，这将增加网络的部署难度和代价。因此，当综合考虑网络的部署难度、代价、所需设备和防御效果时，与已有检测和防御方法相比，SenLeash 具有一定的优势。

6 结束语

本文提出了一种约束防御策略 SenLeash，以防御在 WSN 初始化阶段可能受到的外部虫洞攻击。基于对数正态 shadowing 模型，通过组合节点接收概率，RSSI 和 MAC 层的最大重传次数，研究了如何实现 SenLeash 和如何得到及设置相应参数，包括一种测量相对距离的方法 nRSSI 和选择恰当的接收距离阈值。在能耗方面，每个节点仅需要额外接收 200 个左右的信元分组用来估计到初始基站的距离，因此能耗开销很小。实验结果表明了 nRSSI 和 SenLeash 的可行性。同时当综合考虑网络的部署难度、代价、所需设备和防御效果时，与已有检测和防御方法相比，SenLeash 具有一定的优势。

参考文献：

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

[2] ARAMPATZIS T, LYGEROS J, MANESIS S. A survey of applications of wireless sensors and wireless sensor networks[A]. Proceedings of the 13th Mediterranean Conference on Control and Automation[C]. Limassol, Cyprus, 2005. 719-724.

[3] GARCIA-HERNANDEZ C F, IBARGUENGOYTIA-GONZALEZ P H, GARCIA-HERNANDEZ J, *et al.* Wireless sensor networks and applications: a survey[J]. International Journal of Computer Science and Network Security (IJCSNS), 2007, 7(3): 264-273.

[4] ZHOU Y, FANG Y G, ZHANG Y C. Securing wireless sensor networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2008, 10(3): 6-28.

[5] CHEN X Q, MAKKI K, YEN K, PISSINOU N. Sensor network security: a survey[J]. IEEE Communications Surveys & Tutorials, 2009, 11(2): 52-73.

[6] HU Y C, PERRIG A, JOHNSON D B. Packet leashes: a defense against wormhole attacks in wireless networks[A]. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM)[C]. San Francisco, USA, 2003. 1976-1986.

[7] SHOKRI R, POTURALSKI M, RAVOT G, *et al.* A practical secure neighbor verification protocol for wireless sensor networks[A]. Proceedings of the Second ACM Conference on Wireless Network Security[C]. Zurich, Switzerland, 2009. 193-200.

[8] PHUONG T V, CANH N T, LEE Y K, *et al.* Transmission time-based mechanism to detect wormhole attacks[A]. The 2nd IEEE Asia-Pacific Services Computing Conference[C]. Tsukuba Science City, Japan, 2007.172-178.

[9] CAPKUN S, BUTTYÁN L, HUBAUX J P. SECTOR: secure tracking of node encounters in multi-hop wireless networks[A]. Proceedings of the 1st ACM Workshop on Security of Ad-hoc and Sensor Networks (SASN 03)[C]. Fairfax, USA, 2003. 21-32.

[10] CHIU H S, LUI K S. DelPHI: wormhole detection mechanism for ad-hoc wireless networks[A]. The 1st International Symposium on Wireless Pervasive Computing[C]. Phuket, Thailand, 2006. 1-6.

[11] WANG W C, BHARGAVA B. Visualization of wormholes in sensor networks[A]. Proceedings of the 2004 ACM Workshop on Wireless security[C]. Philadelphia, USA, 2004. 51-60.

[12] ÖZDEMIR S, MEGHDADI M, GÜLER I. A time and trust based wormhole detection algorithm for wireless sensor networks[A]. The 3rd Information Security and Cryptology Conference (ISC'08)[C]. Ankara, Turkey, 2008. 139-144.

[13] PIRZADA A A, MCDONALD C. Circumventing sinkholes and wormholes in wireless sensor networks[A]. Proceedings of International Workshop on Wireless Ad-hoc Networks[C]. London, UK, 2005. 1-6.

[14] KHALIL I, BAGCHI S, SHROFF N B. LITEWORP: a lightweight countermeasure for the wormhole attack in multi-hop wireless net-

works[A]. Proceedings of the International Conference on Dependable Systems and Networks[C]. Yokohama, Japan, 2005. 612-621.

[15] KHALIL I, BAGCHI S, SHROFF N B. MOBIWORP: mitigation o the wormhole attack in mobile multihop wireless networks[J]. Elsevier Ad Hoc Networks, 2008, 6(3): 344-362.

[16] RASMUSSEN K B, CAPKUN S. Implications of radio fingerprinting on the security of sensor networks[A]. Proceedings of Third International Conference on Security and Privacy in Communi ion Networks, SecureComm[C]. Nice, Frane, 2007. 331-340.

[17] MEGHDADI M, OZDEMIR S, GULER I. A survey of wormhole-based attacks and their countermeasures in wireless sensor networks[J]. The Institution of Electronics and Telecommu ication Engineers Technical Review, 2011, 28(2): 89-102.

[18] PAPADIMITRATOS P, POTURALSKI M, SCHALLER P, *et al*. Secure neighborhood discovery: a fundamental element for mobile ad-hoc networking[J]. IEEE Communications Magazine, 2008, 46(2):132-139.

[19] POTURALSKI M, PAPADIMITRATOS P, HUBAUX J P. Secure neighbor discovery in wireless networks: formal investigation of possibility[A]. Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security[C]. Tokyo, Japan, 2008. 189-200.

[20] WEI Y, HEIDEMANN J, ESTRIN D. An energy-efficient MAC protocol for wireless sensor networks[A]. Proceedings of IEEE Information Communication Conference(INFOCOM2002)[C]. Piscataway, USA, 2002. 1567-1576.

[21] VAN D T, LANGENDOEN K. An adaptive energy-efficient MAC protocol for wireless sensor networks[A]. SenSys'03: Proceedings of the 1st International Conference on Embedded Networked Sensor Systems[C]. Los Angeles, USA, 2003. 171-180.

[22] The IEEE 802.15.4 standard (ver. 2006)[EB/OL]. http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf, 2006.

[23] OMNeT++Community.OMNeT++[EB/OL].http://www. omnetpp. Org, 2013.

[24] Castalia Home: Castalia[EB/OL]. http://castalia. research.nicta.com.au/index.php/en/,2013.

[25] BOULIS A. Castalia user's manual[EB/OL]. http://castalia.research.nicta.com.au/index.php/en/documemtation.

作者简介：

胡蓉华（1985-），男，湖北荆州人，东北大学博士生，主要研究方向为无线传感器网络安全、信息隐藏。

董晓梅（1970-），女，河南开封人，博士，东北大学副教授，主要研究方向为网络与信息安全、信息隐藏、计算机取证等。

王大玲（1962-），女，辽宁新民人，博士，东北大学教授、博士生导师，主要研究方向为数据挖掘、机器学习、信息检索等。