文章编号:0253-2778(2019)01-0001-07

基于网格的无线传感器网络虫洞攻击抵御策略

吴一尘,章曙光

(安徽建筑大学电子与信息工程学院,安徽合肥 230022)

摘要:虫洞攻击破坏路由操作、影响节点定位,对整个无线传感器网络(WSNs)的安全性造成极大的威胁.针对这种情况,提出了基于网格的虫洞攻击抵御策略(DEAD).通过附加的网格属性,借助特定网格内节点的信息交换来检测网络中的虫洞攻击,包括具有伪造篡改能力的特殊虫洞攻击,从而大大减少了虫洞攻击造成的危害.仿真实验表明,该策略能够在网络受到攻击时,有效地检测出恶意节点.

关键词:无线传感器网络;虫洞攻击;基于网格的检测

中图分类号:TP391 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2019.01.001

引用格式:吴一尘,章曙光. 基于网格的无线传感器网络虫洞攻击抵御策略[J]. 中国科学技术大学学报,2019,49(1):1-7.

WU Yichen, ZHANG Shuguang. Defence mechanism against wormhole attacks based on grid[J]. Journal of University of Science and Technology of China, 2019,49(1):1-7.

Defence mechanism against wormhole attacks based on grid

WU Yichen, ZHANG Shuguang

(*School of Electronic and Information Engineering, Anhui Jianzhu University, Hefei* 230022, *China*)

Abstract: A wormhole attack destroys routing operations, affects the node positioning, and poses great threats to the security of the entire wireless sensor network (WSN). Aiming at resolving this issue, the grid based wormhole attack defense strategy was presented. Through additional grid properties, information was exchanged with nodes in specific grids to detect wormhole attacks, including attacks from special wormholes with the forgery and tampering ability in a network, thus greatly reducing damages brought by wormhole attacks. The simulated experiment proves that malicious nodes can be effectively detected in an attacked network if this strategy is used.

Key words: wireless sensor networks; wormhole attacks; detection based on gird

0 引言

近几年来,无线传感器网络取得了跨越式的发展,具有广阔的应用前景.由于无线传感器节点随机分布、资源有限,且通常部署在野外及无基础设施区域,所以容易受到各种各样的恶意攻击.虫洞攻击就是一种常见的恶意攻击,由至少两个相距较远的恶意节点合谋发起[1],通过私有信道互相发送信息,严重破坏路由的建立、更新与维护过程.现有的虫洞攻击检测机制一般都建立在一定的先决条件之上,这

收稿日期:2017-06-09;**修回日期**:2018-09-27

基金项目:安徽省教育厅自然科学研究项目(KJ2016A155)资助.

作者简介:吴一尘,男,1988年生,硕士/副教授,研究方向:无线传感器网络.E-mail:puffywyc@gmail.com

通讯作者:章曙光,男,1970年生,博士/教授.E-mail:20314852@qq.com

些条件大多忽略了虫洞攻击可能具有篡改能力.实际应用中,虫洞攻击很可能会对数据进行篡改,躲避检测,如跳数、距离和信号强度等.针对这种情况,本文提出了一种基于网格的虫洞攻击抵御策略,先将区域网格化,节点按网格划分,然后利用节点的网格属性以及与特定相邻网格内节点的信息交换来检测攻击.此种策略的优势在于能抵御住具有篡改能力的虫洞攻击,而且不需要额外的硬件.仿真实验表明,本文提出的虫洞攻击抵御策略能够有效抵御无线传感器网络中的虫洞攻击.

1 相关工作

现阶段很多研究人员提出了相关应对虫洞攻击的机制.如文献[2-3]提出基于跳数的防御机制,在源节点希望与目的节点进行数据传输时,进行路由发现,在此过程中记录下各路径所经过的跳数,统计和比较各跳数值;对于跳数值异常的,管理者可以判断网络正遭受虫洞攻击,但是常常受限于节点的资源和处理能力.文献[4]针对无线传感器网络中无需测距的定位技术,提出一种基于信誉模型的抵御虫洞攻击的分布式轻量级DV-Hop安全定位算法,但在网络连通度较差或节点密度较大时,性能会有所下降.文献[5]提出基于拓扑的被动式实时虫洞攻击检测方案,利用虫洞攻击大量吸引网络流量和显著缩短平均网络路径的特征,通过收集网络中部分路由信息来实时探测虫洞节点,但在网络中节点较多的情况下,检测时延较大.文献[6]在虫洞检测中利用了传输受限特性和数据分组唯一特性,在数据发送前引入了test过程,即广播test数据分组,然后监听test数据分组并根据上面两个特性来判断无线传感器网络是否遭受虫洞攻击的威胁,但此方法并没有考虑节点通信过程中的分组丢失问题.文献[7]提出利用信号强度指示器(RSSIs),通过比较信号强度和一系列的分析计算来检测虫洞攻击,但是检测效率往往受到无线信号物理特性的影响.文献[8]在文献[5-7]基础上进行了优化,在对比信号强度的同时,通过在发送消息中嵌入节点到初始基站的距离这一因子,进一步限制了邻居发现消息的传输距离,从而防御虫洞攻击,但是防御效果一定程度上取决于相关节点到基站的距离和时钟的同步精度.文献[9]提出了一种反向思维,有虫洞两端点A、B的邻居节点集合C_A、C_B因为虫洞的影响会互相认为互为邻居,形成新的伪邻居节点集合C_{AB},然后通过一定的准则阻断C_{AB}中某一个邻居连接,并观察邻居集C_{AB}是否分裂成若干子集,最终经过计算分析来检测防御虫洞攻击.此方法检测过程相对来说比较复杂,受限于节点的处理能力.文献[10]提出了一种在无线传感器网络数据融合过程中进行虫洞攻击检测的协议,此种方法需要一定的前提条件.文献[11]提出了一种相对于利用往返时间(RTT)检测虫洞方法的改进型,既利用单次时间(single trip)来更快速地发现攻击,并通过了标时标色的Petri网建立了模型,并验证了有效性.由于这是标时标色Petri网第一次用来验证虫洞攻击的检测模型,可靠性还有待观察.

综上所述,现有的虫洞攻击防御方法中,大多都建立在一定的假设和要求之上,或假设数据无丢失、或要求时间精确同步、或需要额外的硬件等,然而却很少考虑到位置、时间、跳数和信号强度等数据被恶意篡改的情况.实际应用中,如果遇到这一类型的虫洞攻击,则很难被检测出.

2 系统模型

2.1 网络模型

假定WSN中的节点随机部署在区域内,并在部署后划分好网格,节点相对固定,每个节点的通信范围相同,覆盖自身和周围共9个网格.文献[12-14]介绍了有关区域网格划分的办法,并保证网络连通率(每个节点至少要能与自身所处和周围的共9个网格内的节点建立连接).对于部分节点移动的情况,可以重新调用相关定位算法确认当前所在网格.本文是以正方形网格划分方式为基础构建相关抵御策略,每个网格以二维矩阵坐标为ID互相区分,如图1所示.每个节点知晓自身所处的网格ID(GID),在其所发出的信息中标识出,如果是转发其他节点的信息,则同时要标识出其他节点的GID.除了网格ID外,每个节点还有唯一的识别编号ID.数据包详细格式如图2所示.

2.2 攻击模型

(Ⅰ)等级一虫洞攻击

假定攻击者在发动攻击时对自身的GID和来自合谋节点的转发GID无改动地直接放入数据分组中,然后以一定的通信范围发送出去.

(Ⅱ)等级二虫洞攻击

假定攻击者为了躲避检测,在发动攻击时对自身的GID或来自合谋节点的转发GID进行篡改后

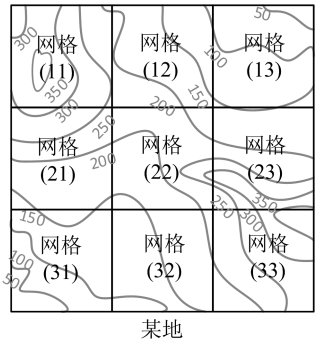

图 1　网格划分

Fig. 1　Grid division

图 2　GID 及数据包格式

Fig. 2　GID and data packet format

放入数据分组中，再以一定的通信范围发送出去. 通常把相关节点伪装成在自身的正常通信范围内，隐蔽性强.

3　基于网格的虫洞攻击抵御策略（DEAD）

本文提出的 DEAD 策略适用于节点不发生移动的 WSNs. 首先把全区域划分成网格，在节点部署后通过网格把无序的节点联系起来，再从网格的角度出发，把距离的概念赋予到网格的 GID 中，检测流程如图 3 所示.

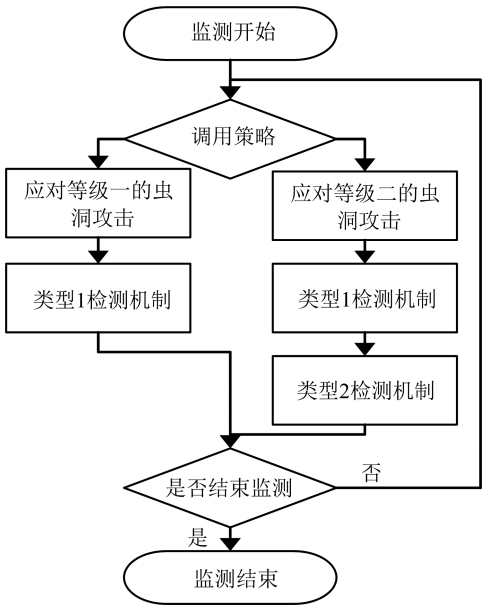

图 3　检测流程

Fig. 3　Detection process

针对等级一的虫洞攻击，采取类型 1 的检测机制，即通过判断数据分组中的网格属性来防御攻击；针对等级二的虫洞攻击，先调用类型 1 检测机制，再对通过检测的剩余数据分组调用类型 2 检测机制，即通过与辅助节点的合作来防御攻击. 实际应用中，对于状况较好，节点资源有限的网络，可以多采用针对等级一虫洞攻击的抵御策略，间歇性地调用针对等级二虫洞攻击地抵御策略；反之对于状况复杂，安全性低的网络，可以多采用针对等级二虫洞攻击的抵御策略. 通过适当地调用策略将两种防御方式相结合，适应实际需求，防御能力更强.

3.1　DEAD 的 3 类检测机制

（Ⅰ）常规检测

所有节点在每一次收到数据分组时，都要首先通过数据包中的自身 GID 判断数据的一跳前节点是否在自身正常通信范围内，如果不满足则说明一跳前节点通信范围异常，可能为恶意节点，丢弃该数据分组. 所有后续检测都是建立在常规检测的基础上. 相应伪代码如下：

if（$R_{GID} \notin S_{GID} \cup S_{GID+[0,1]} \cup S_{GID+[1,1]} \cup S_{GID+[1,0]} \cup S_{GID+[0,-1]} \cup S_{GID+[-1,-1]} \cup S_{GID+[-1,0]} \cup S_{GID+[1,-1]} \cup S_{GID+[-1,1]}$）

Node ndiscard R_{data}.

else go on.

其中，R_{GID} 是指数据接收节点的自身 GID，如图 4 中的节点 n；S_{GID} 是指数据发送节点的自身 GID，如节点 m，R_{data} 是节点 m 发送的数据.

（Ⅱ）类型 1 检测机制

等级一的虫洞攻击中，恶意节点没有篡改能力，所以对于每个通过常规检测的数据分组，接收节点都可以借助其中的转发 GID 得知其两跳前的节点（如遭受攻击，就是合谋节点的邻居节点）来自哪个网格，把那些不属于其一跳前节点（如遭受攻击，就是恶意节点）正常通信范围内的数据分组排除，达到抵御虫洞攻击的目的. 如图 4 所示，节点 m 通过私有信道把合谋节点转发的邻居节点 p_1、p_2 的数据给节点 n，以达到影响路由算法等相关攻击. 由于节点 m 并没有篡改节点 p_1、p_2 的 GID，所以节点 n 可以通过判断节点 p_1、p_2 的 GID（节点 m 发送给节点 n 的数据分组中的转发 GID）是否来自节点 m 的通信范围内进行过滤. 如果不是，则丢弃此次收到的数据分组. 相应伪代码如下：

if（$S_{FGID} \notin S_{GID} \cup S_{GID+[0,1]} \cup S_{GID+[1,1]} \cup S_{GID+[1,0]} \cup$

$S_{GID+[0,-1]} \cup S_{GID+[-1,-1]} \cup S_{GID+[-1,0]} \cup S_{GID+[1,-1]} \cup S_{GID+[-1,1]}$)

Node ndiscard R_{data}.

else go on.

其中,S_{FGID} 是指节点 m 发送数据中的转发 GID.

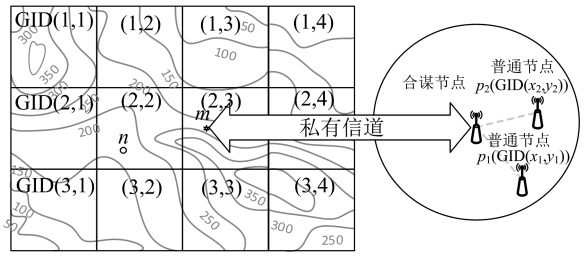

图 4 检测机制

Fig. 4 Detection mechanism

(Ⅲ)类型 2 检测机制

等级二的虫洞攻击中,由于恶意节点可以对数据中的转发 GID 进行篡改(如果篡改自身 GID 则是女巫攻击),隐蔽性更强. 图 4 中节点 m 在收到合谋节点的数据后,把其转发的邻居节点的 GID 篡改成在节点 m 的正常通信范围内,然后再放入自身的转发 GID 中. 本文中对通过类型 1 检测的数据分组调用类型 2 检测机制,以达到检测等级二虫洞攻击的目的. 根据节点 m 的攻击范围(通信范围),类型 2 检测机制采取不同的检测方法.

情况一:节点 m 以大于普通节点的通信范围对周围节点进行攻击.

如图 5 所示,假设此处节点 m 的攻击范围是一个以节点 m 所在网格为中心,5 个网格为边长的正方形. 节点 n 为受到节点 m 攻击的任意一节点(此处选择的节点 n 在节点 m 的自身及周围 9 个网格中.

这里节点 n 选择节点 m 正常通信范围外的网格内任意一个节点作为辅助判断节点,从效率的角度,采取就近原则,选取 mn 方向上向外的与节点 n 相邻的网格内的节点. 图 5 中选择与节点 n 所在网格相邻的网格 31 中的节点 n_2 作为辅助判断节点. 若网格 31 中没有节点,就从网格 21 和 41 中选择. 在节点分布十分稀疏的情况下,若网格 21、31、41 中都没有分布任何节点,则直接使用情况二的机制检测.

正常情况下,节点 n_2 是无法收到节点 m 发送的数据. 而在受到此种虫洞攻击的情况下,节点 n_2 可以收到节点 m 发送的数据,所以通过节点 n_2 的验证结果可以判断节点 n 是否遭受虫洞攻击. 相应伪代码如下:

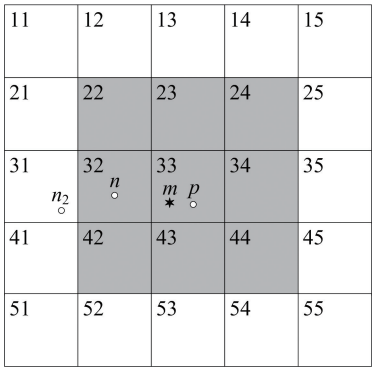

图 5 类型 2 的节点检测

Fig. 5 Node detection of type 2

if(aNode$_{[2n-m]}$ received R_{data})

Node ndiscard R_{data}.

else go on.

其中,aNode$_{[2n-m]}$ 是指网格[$2n_{GID}-m_{GID}$]中的任意节点.

情况二:节点 m 以普通节点的通信范围对周围节点进行攻击.

此时,虫洞攻击的攻击范围为节点 m 自身及周围共 9 个网格中(如图 5 中灰色部分).

如果节点 m 转发的篡改后的信息(来自节点 p_1 或 p_2,见图 4)中的 FGID 在图 5 中灰色部分与节点 n 正常通信范围重合部分中(如图 5 中的网格 22、23、32、33、42、43. 如果节点 n 在灰色部分中四角的网格内,如网格 42,则重合网格是 32、33、42、43),则节点 n 通过自身接收到的数据进行检测,无需辅助判断节点. 由于节点 p_1 宣称在节点 n 的直接通信范围内,所以节点 n 除了能够接收到由节点 m 转发的关于节点 p_1 的信息,还必然能够收到由节点 p_1 直接发送来的信息,但因为节点 p_1 的 GID 是被节点 m 篡改的,并不是实际存在的,所以节点 n 无法收到由节点 p_1 直接发送来的信息,所以节点 n 可以依据此种特性的验证结果来检测虫洞攻击. 相应伪代码如下:

if($Node_n$ received R_{data}

which R_{GID}==m

&&

$Node_n$ can not received R'_{data}

which R'_{GID}==R_{FGID})

Node n discard R_{data}.

else go on.

其中,$Node_n$ 是指的是节点 n.

如果节点 m 篡改的 F_{GID} 不在上述范围内,则选择在节点 m 所在的网格中任意另一节点作为辅助判断节点,如节点 p. 由于节点 p 和节点 m 在同

一网格内，正常情况下，节点 p 与节点 m 通信范围相同，所以节点 p 不仅能够接收到由节点 m 转发的来自节点 p_1 的信息，也能够接收到由节点 p_1 直接发送来的信息. 如果只能够接收到转发信息而无法接收到直接信息则可以判断当前无线传感器网络正遭受虫洞攻击. 相应伪代码与上面叙述的相同.

如果节点 m 所在的网格内只有其本身一个节点，那么则选择节点 n 通信范围内与伪节点 p_1 所在网格相邻的其他网格内的任意节点作为辅助判断节点，如图 5 所示. 假如伪节点 p_1 在网格 24 中，则选择网格 23 中的任意节点作为辅助判断节点. 此时如果节点 n 和伪节点 p 分别在对角线的两端网格中，那么节点 n 通信范围内与伪节点 p_1 所在网格仅有节点 m 所在一个网格，所以无法选择辅助判断节点，这可以通过选定中间节点来继续寻找辅助判断节点，如节点 n 可以选择网格 43 内的节点作为中间节点，再由中间节点选择网格 34 内的节点作为辅助判断节点，最终完成虫洞攻击的检测.

在节点分布十分稀疏的情况下，可能会存在节点的受攻击一侧（如图 5 中与节点 n 相邻的网格 23、33、43）或整个周围除了恶意节点（仅发生在节点捕获型恶意攻击时）外没有任何其他节点存在，从而导致无法选择辅助判断节点的情况. 经过分析虫洞攻击的原理和相关路由算法，可以发现在此种情况下，不论攻击是否存在，节点 n 往节点 m 方向的数据流通大部分只能通过节点 m，所以虫洞攻击对网络中的路由算法的影响得到明显降低，对此种防御策略的影响相对较小.

3.2　调用策略

针对网络管理者对网络中何时存在何种等级的虫洞攻击一无所知，且无线传感器网络具有资源有限的特点，本文提出的抵御策略并不要求所有节点在每次接收到数据时都进行两种类型检测机制同时调用. 通常情况下，恶意攻击具有很大的随机性，但是恶意攻击往往呈集群式出现，时间相对集中. 正常情况下，对于整个无线传感器网络使用应对等级一虫洞攻击的检测机制，以一定的时间间隔采取应对等级二虫洞攻击的检测机制；一旦检测发现受到等级二的虫洞攻击，则缩小时间间隔；如果没有发现攻击，则恢复初始时间间隔.

归纳出时间间隔公式如下：

$$T=\frac{T}{2\sum_{i=1}^{n}\triangle A'_i};$$

其中，T 为时间间隔，且

$$\triangle A=\begin{cases}1, \text{第 } i \text{ 次检测到虫洞攻击}\\ -1, \text{第 } i \text{ 次没有检测到虫洞攻击}\end{cases}.$$

当然也可以根据实际情况，相应地调整调用策略，提高防御效果. 一个合适的时间间隔策略对整个抵御策略的效率影响很大，然而实际使用中很难找到一个完美的时间间隔策略去适应任何可能发生的攻击.

4　仿真实验及分析

4.1　安全性分析

当随机选择的辅助判断节点恰巧为恶意节点时，可能会刻意隐瞒真实信息，直接影响最终的检测结果. 此种情况往往发生在恶意节点密度较大的情况下. 密度越大，检测准确度会一定程度的下降. 文献[14]介绍了有关恶意节点溯源定位的方法，可以隔离恶意节点，降低恶意节点在无线传感器网络中的密度，从而保证了虫洞攻击的检测率.

当正常节点在区域中分布十分稀疏或者十分不均时，可能会出现无法找到辅助判断节点的情况，对虫洞攻击的检测率会有一定影响，在此情况下，虫洞攻击带来的危害却相对降低. 在大多数用于检测采集信息的无线传感器网络中，为了保证一定的信息采集效果和网络连通度，较少会出现此种情况.

当攻击者刻意伪造出不存在的辅助判断节点时，会回复虚假信息，迷惑受攻击节点的判断，对检测准确度有较大影响，但是此种攻击已经超出了一般虫洞攻击的范畴，是一种女巫攻击和虫洞攻击结合的复杂恶意攻击. 结合文献[16-17]提出的女巫攻击的防御方法，本文提出的方法能有效检测到大部分的虫洞攻击.

4.2　支出分析

本文提出的基于网格的抵御策略所花费的开支是随着防御等级的提高而提高. 常规检测需要一次判断运算，等级一攻击检测是在常规检测的基础上再加一次判断运算，等级二攻击检测需要与邻近节点交换信息并判断. 同时，调用策略越合理，支出相对越少.

虽然此抵御策略在节点部署阶段划分网格时需要一定的支出，但是在具体检测阶段，与其他防御方式相比，如基于跳数的（需要记录跳数并比较分析）、信誉模型的（通过相关公式计算信誉度）、冲突集的（确定并交换自身冲突集并判断）等，算法相对简单. 综合以上分析，该策略总体支出并没有明显增长，甚至有些情况下，支出小于其他防御方式，而且既能保

证较高的检测率，又能检测出具有篡改能力的虫洞攻击.

4.3 仿真实验

本节以 Matlab 为仿真平台对本文所提出的虫洞检测机制进行性能分析. 仿真实验配置：节点个数 500 个，节点随机分布在范围为 3000 m×3000 m 的区域内，含 100 个网格，每个网格面积为 300 m×300 m，检测持续时间 10 到 20 秒.

仿真持续期间内，间隔随机时间在随机网格内生成可造成等级一或等级二虫洞攻击的恶意节点. 其中恶意节点的攻击范围，数据分组中的 GID 和等级二攻击中篡改后的 GID 都是随机生成的.

图 6 显示了在某次调用应对等级二攻击的检测机制后，所有节点的相关状态，标“·”节点为未受到攻击的节点，标“*”节点为检测到攻击的节点. 此次调用时区域内存在两个等级一的攻击节点，标“+”表示；一个等级二的攻击节点，标“.”表示，攻击范围都是以自身网格为中心，边长为 5 个网格的正方形区域. 在 3 个恶意节点通信范围内的普通节点共有 273 个，全部节点都检测到了虫洞攻击.

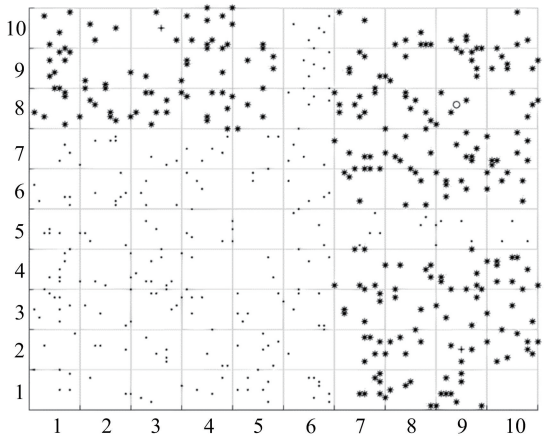

图 6 调用应对等级二攻击的检测机制后所有节点的相关状态

Fig. 6 Relevant status of all nodes after calling detection mechanisms for level 2 attacks

图 7 显示了调用此次检测机制后，区域内受到等级二攻击的节点的相关状态. 标“*”节点在等级二攻击节点的攻击范围内，但在正常通信范围外，共有 55 个节点通过类型 1 检测机制排除了攻击；标“*”节点在等级二攻击节点的攻击范围内并且在正常通信范围内，共有 54 个节点通过类型 2 检测机制排除了攻击. 两种检测机制相结合，大大降低了虫洞攻击的威胁.

图 8 显示了在某次持续 18 秒的仿真中检测率的变化. 其间以一定时间间隔对全区域内所有节点的攻击检测率进行了 10 次统计，抵御策略可以发现绝大多数的虫洞攻击.

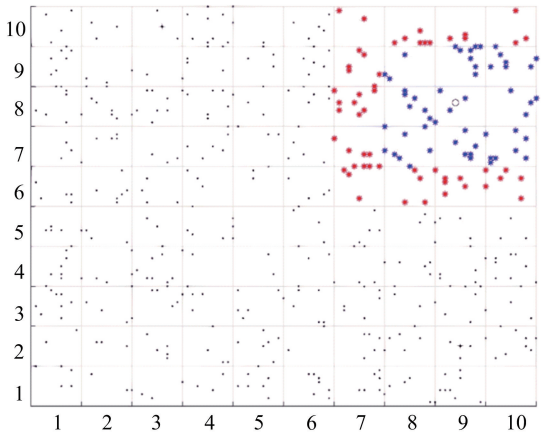

图 7 区域内受到等级二攻击的节点状态

Fig. 7 Nodes state under level 2 attack in an area

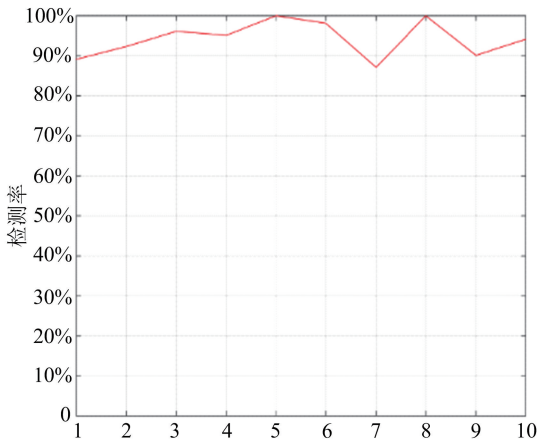

图 8 单次仿真结果

Fig. 8 Single simulation result

经过对多次仿真结果的讨论，可以得出以下结论：

(Ⅰ)本文提出的抵御策略能有效地检测出网络中存在的虫洞攻击，不论是否具有篡改能力，并且保持着较高的检测率.

(Ⅱ)检测率的高低主要取决于检测持续期间应对等级二攻击的检测机制的调用次数. 如图 9 所示，调用次数越多，检测率越高. 如果每个节点每次接收数据都调用等级二攻击的检测机制，检测率接近 100%. 由于等级二攻击的检测机制相比于等级一的更加复杂，这就意味着在追求高检测率的同时，调用的次数越多就带来更多的资源消耗，所以时间间隔策略的制定极其重要，直接影响检测效率.

5 结论

本文针对无线传感器网络中具有篡改能力的虫

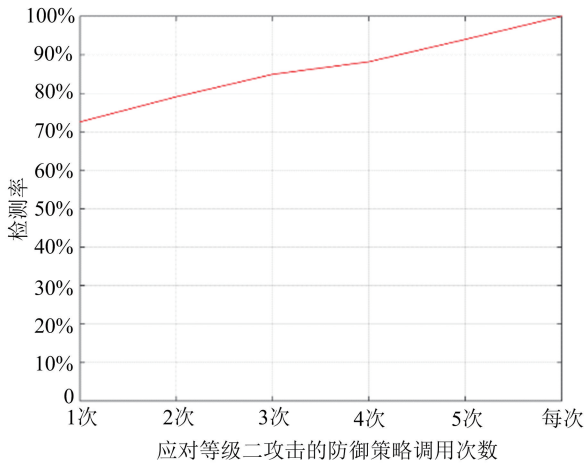

图 9　仿真结果分析

Fig. 9　Analysis of simulation results

洞攻击，提出了一种基于网格的抵御策略，该策略把网络中存在的虫洞攻击分为没有篡改能力的和具有一定篡改能力两种. 对于前者，该机制让接收节点通过判断相关网格属性的方式排除恶意节点发送来的信息；对于后者，该机制通过接收节点与辅助判断节点合作的方式排除恶意节点发送来的信息. 根据传感器所处的环境和安全需求的不同，可以将两种检测机制以不同方式相结合，采用不同的时间间隔策略. 最后，通过仿真实验验证了该方法的有效性.

本文提出的虫洞攻击抵御策略，并没有考虑无线传感器网络中节点大量动态移动和重新定位所带来的能耗问题，而且是建立在所有节点的通信范围都一样的假设基础上，同时在恶意节点密度过大或普通节点密度过低的情况下，检测率会有所下降. 今后的研究工作之一是解决节点动态移动情况下对虫洞攻击的检测问题，使之能够适用于不同密度情况下的传感器网络，同时允许不同节点具有不同通信范围.

参考文献(References)

[1] 易平. 无线网络攻防原理与实践[M]. 北京：清华大学出版社，2012.

[2] JHAVERI R H，PATEL A D，PARMAR J D，et al. MANET routing protocols and wormhole attack against AODV[J]. International Journal of Computer Science and Network Security，2010，10(4)：12-18.

[3] 吕兆辉，张红梅，郭远洋. 基于跳数的防御无线传感器网络中虫洞攻击方案[J]. 单片机与嵌入式系统应用，2013，13(4)：7-10.

[4] 陈立建，金洪波，毛科技，等. 抵御虫洞攻击的无线传感器网安全定位算法[J]. 传感技术学报，2016，29(12)：1882-1887.

[5] 鲁力，HUSSAIN M J，朱金奇. 无线传感器网络中虫洞攻击实时被动式探测[J]. 软件学报，2016，27(12)：3085-3103.

[6] 陈鸿龙，王志波，王智，等. 针对虫洞攻击的无线传感器网络安全定位方法[J]. 通信学报，2015，(3)：2015056(1-8).

[7] JAIN S，TA T，BARAS J. Wormhole detection using channel characteristics[C]// Proceedings of the IEEE International Conference on Communications. Ottawa，Canada：IEEE，2012：6699-6704.

[8] 胡蓉华，董晓梅，王大玲. SenLeash：一种无线传感器网络虫洞攻击约束防御机制[J]. 通信学报，2013，34(10)：65-75.

[9] BAN X M，SARKAR R，GAO J. Local connectivity tests to identify wormholes in wireless networks[C]// Proceedings of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Paris，France：ACM，2011：13-24.

[10] DUTTA K，KUMAR M. Detecting wormhole attack on data aggregation in hierarchical WSN [J]. International Journal of Information Security and Privacy，2017，11(1)：35-51.

[11] CHEN L S，LIU C Y，HUANG H J. Secure routing against wormhole attack and its formal verification based on timed colored Petri Net[C]// Proceedings of the 11th ACM Symposium on QoS & Security for Wireless & Mobile Networks. Cancun，Mexico：ACM，2015：157-164.

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

[13] AL-KARAKI J N，UL-MUSTAFA R，KAMAL A E. Data aggregation in wireless sensor networks-exact and approximate algorithms[C]//Proceedings of the IEEE Workshop on High Performance Switching and Routing. Phoenix，USA：IEEE Computer Society Press，2004：241-245.

[14] TILAK S，ABU-GHAZALEH N B，HEINZELMAN W. Infrastructure tradeoffs for sensor networks[C]// Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications. Atlanta，USA：ACM，2002：49-57.

[15] 章曙光，周学海，杨峰，等. 无线传感器网络中基于邻居节点信息的溯源追踪策略[J]. 小型微型计算机系统，2015，36(3)：483-487.

[16] GEETHA C，RAMAKRISHNAN M. Detection of SYBIL attack using neighbour nodes in static WSN[J]. International Journal on Recent and Innovation Trends in Computing and Communication，2015，3(4)：2428-2432.

[17] DONG W，LIU X J. Robust and secure time-synchronization against sybil attacks for sensor networks [J]. IEEE Transactions on Industrial Informatics，2015，11(6)：1482-1491.