文章编号:0253-2778(2020)01-0072-07

# 异构无线传感器网络中基于AOA的女巫攻击检测方案

章曙光[1,2],汪 乾[1],王 浩[2],钟 娟[1]

(1.安徽建筑大学电子与信息工程学院,安徽合肥 230061;2.安徽建筑大学信息网络中心,安徽合肥 230061)

**摘要**:无线传感器网络中,女巫攻击节点通过伪造多重身份发动攻击,若不同的女巫身份使用不同的发射功率发送消息,导致该女巫攻击行为难以检测.针对该问题,本文提出一种异构网络环境下基于信号到达角度(angle of arrival, AOA)的女巫攻击检测方案.该方案中异构节点检测周边节点的到达角度信号,利用角度信息建立可疑女巫节点列表,通过相邻异构节点之间的信息交互,相互协作定位女巫攻击节点.针对异构节点稀疏的特殊情形,提出了单异构节点的增强检测机制,以检测女巫节点.理论分析与仿真实验表明,该方案能快速准确地识别恶意节点,降低了节点能耗,延长了网络的生存期.

**关键词**:无线传感器网络;女巫攻击;信号到达角度;节点协作

**中图分类号**:TP393 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2020.01.009

**引用格式**:章曙光,汪乾,王浩,等.异构无线传感器网络中基于AOA的女巫攻击检测方案[J].中国科学技术大学学报,2020,50(1):72-78.

ZHANG Shuguang, WANG Qian, WANG Hao, et al. Sybil attack detection scheme based on AOA in heterogeneous wireless sensor networks[J]. Journal of University of Science and Technology of China, 2020,50(1):72-78.

# Sybil attack detection scheme based on AOA in heterogeneous wireless sensor networks

ZHANG Shuguang[1,2], WANG Qian[1], WANG Hao[2], ZHONG Juan[1]

(1. *School of Electronic and Information Engineering, Anhui Jianzhu University, Hefei* 230061, *China*;
2. *Information Network Center, Anhui Jianzhu University, Hefei* 230061, *China*)

**Abstract**: In the wireless sensor network, sybil attack nodes launch attacks by forging multiple identities. If different sybil identities send messages with different transmitting powers, the sybil attack behavior will be difficult to detect. To solve this problem, this paper proposes a sybil attack detection scheme based on the angle of arrival (AOA) in a heterogeneous network environment. In this scheme, heterogeneous nodes detect the angle of arrival from surrounding nodes, and use the angle information to establish a list of suspicious sybil nodes. Through the information interaction between neighboring heterogeneous nodes, the sybil attack node can be located cooperatively. For the special case of heterogeneous nodes, a single heterogeneous node enhanced detection mechanism is proposed to detect sybil nodes. Through theoretical analysis and simulation experiments, the scheme can quickly and accurately identify the malicious nodes,

**收稿日期**:2019-10-29;**修回日期**:2019-12-21

**基金项目**:赛尔网络下一代互联网技术创新项目(NGII20190602),安徽省教育厅自然科学重点项目(KJ2016A155),校博士启动基金(2015QD05),高等学校省级优秀青年人才基金重点项目(2013SQRL099ZD),赛尔网络下一代互联网技术创新项目(NGII20170117)资助.

**作者简介**:章曙光(通讯作者),男,1970年生,博士/教授.研究方向:无线传感器网络和网络安全.E-mail:zsg@ahjzu.edu.cn

reduce the energy consumption of the nodes, and extend network life.

**Key words**: wireless sensor network; sybil attacks; angle of arrival; node cooperation

## 0　引言

无线传感器网络通常部署在无人监管的恶劣环境中,由大量的传感器节点自组织构成. 节点间通过无线信道连接,无线信道的公开性使得网络易受到攻击,而女巫攻击[1]就是其中最为典型的攻击之一.

女巫攻击节点对网络中表现出多重身份,让网络中其他节点误以为周围区域存在多个传感器节点,破坏了网络中的路由机制、资源的公平分配、数据融合和分布式存储等机制,对网络的正常工作有较大的危害,因此高效的女巫攻击检测方案研究显得尤为重要.

女巫攻击节点可通过调整发射功率的形式,配合不同的女巫身份发动攻击,使得该女巫攻击行为难以检测. 针对该问题,本文提出了一种异构网络环境下基于信号到达角度的女巫攻击检测方案,即在网络中部署带有天线阵列[2]的异构节点,检测周边节点的信号到达角度(angle of arrival, AOA),将节点间 AOA 差值在设定阈值内的节点列入可疑女巫节点列表,通过异构节点间的协作,分析可疑女巫节点列表来检测女巫攻击节点. 针对异构节点稀疏的特殊情形,提出单异构节点的增强检测机制来检测女巫攻击节点.

## 1　相关工作

近年来,学者对女巫攻击的检测开展了相关的研究并取得了一定的研究成果.

文献[3]提出了基于规则网络异常检测系统. 该系统的核心是利用超带宽测距的检测算法,以分布式方式进行异常检测,但当女巫攻击节点窃取合法节点的身份时,该系统将无法检测出女巫攻击. 文献[4-5]提出了一种基于分簇协议的安全机制抵御女巫攻击,即当网络中簇头数目超过设定阈值时,启动基于 RSSI(received signal strength indication)的女巫攻击检测策略,该策略由 4 个检测节点比较某节点 RSSI 比值的大小来判断是否存在女巫攻击;该方法需要至少 4 个检测节点,检测效率不高. 文献[6]提出了一种增强 RSSI 机制来识别女巫攻击节点;该机制设定节点在不同时刻 RSSI 值的比率范围,以此判断女巫攻击是否存在;不足是该机制对网络内的检测节点密度要求高. 文献[7]提出了一种基于到达时间差(time difference of arrival, TDOA)的女巫攻击检测方案;该方案将节点身份与 TDOA 比率相联系,比较不同节点身份的 TDOA 比率是否相同来检测女巫攻击;但该方案同样要求检测的节点较多,能耗较大. 文献[8]提出了一种基于近似三角形内点测试法的女巫攻击检测方案;通过 APIT (approximate point-in-triangulation test)定位算法确定女巫节点的地理位置,即发现不同节点在同一位置检测为女巫攻击节点;该方案基于定位机制,能耗过大且对网络的连通性有较高的要求. 文献[9]提出了一种基于邻居节点信息的女巫攻击检测机制;该机制由认证节点收集邻居节点的信息,并分析得出一个临界集合,利用临界集合检测女巫攻击;但该方案要求认证节点的邻居列表中女巫节点的数目较多才能取得较好的效果. 文献[10]提出了一种基于单向密钥链的身份认证机制以降低攻击发生的概率,再利用椭圆曲线离散对数问题提出一种新的邻居认证协议,阻止女巫节点加入网络;但该方案中密钥管理过于复杂. 文献[11]提出了一种基于分层网络的女巫攻击检测方案;该方案先采用分层网格技术大致确定女巫攻击节点的位置,再通过网格内部节点间的密钥信息定位女巫攻击节点;但该方案无法处理恶意节点同一时刻表现多个不同身份的情况. 文献[12]提出了一种基于能量信任模型的女巫攻击检测方法;该方法使用基于身份与地理位置认证的多层检测机制,将信任算法应用到节点能量上,有效地防范了女巫攻击;但该方案要求网络节点拥有相同的处理和存储能力.

以上文献中的节点主要以相同的发射功率发送消息,当发动女巫攻击时,不同身份使用不同的发射功率发送消息,上述解决方案难以检测该攻击行为. 针对此问题,本文提出了一种异构无线传感器网络环境下基于信号到达角度的女巫攻击检测方法,利用异构节点的角度信息定位女巫攻击节点;并针对异构节点密度较低的情况,提出一种单异构节点增强机制检测女巫攻击.

## 2　基于 AOA 的女巫攻击检测方案

### 2.1　网络模型和相关假设

#### 2.1.1　网络模型

假设异构无线传感器网络[13]由大量的普通节

点和少量的异构节点组成，各节点间保持时钟同步，合法节点使用相同的功率发送消息. 网络内普通节点的邻居节点中至少存在一个异构节点. 网络中 Sink 节点能量充足且安全性高. 异构节点具有较高的能量，通信半径不小于普通节点的 2 倍，且该类节点带有智能天线阵列，能准确地检测出节点的信号到达角度[14]. 网络初始化阶段是安全的，部署完成后网络节点不再移动.

2.1.2 女巫攻击模型

女巫攻击节点以相同的功率发送消息时，基于 RSSI 定位技术的检测方案能确定其位置. 若恶意节点通过可调功率的方式发送消息，即当恶意节点使用女巫身份 $S_1$ 时，以功率 $P_1$ 发送消息，当恶意节点使用女巫身份 $S_2$ 时，以功率 $P_2$ 发送消息，这将导致接收消息的节点对同一物理节点会显示出不同的 RSSI 值，基于 RSSI 定位技术的检测方案会将女巫攻击节点定位在不同的位置.

女巫攻击模型如图 1 所示. 假设 $M$ 为恶意节点，$S_1$、$S_2$ 是恶意节点伪造的女巫节点，在恶意节点的最小通信半径内有两个异构节点 $O_i$ 和 $O_j$，其余节点 1～17 为普通合法节点. 女巫节点 $S_1$ 以功率 $P_1$ 发送消息，通信半径为 $r_{S_1}$，女巫节点 $S_2$ 以功率 $P_2$ 发送消息，通信半径为 $r_{S_2}$，合法节点均以功率 $P_0$ 发送消息，通信半径为 $r$.

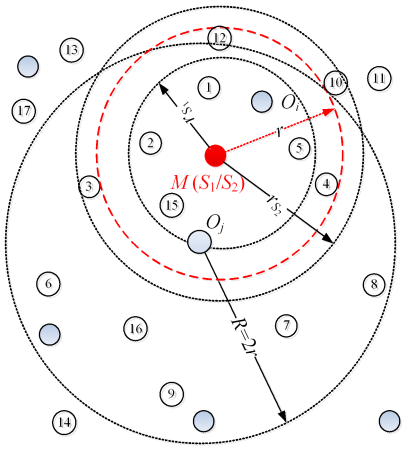



图 1 女巫攻击模型

Fig. 1 Sybil attack model

## 2.2 女巫攻击检测方案

2.2.1 基本检测原理

女巫攻击表现出的女巫身份均来源于同一个真实的物理节点，恶意节点使用任一女巫身份发送消息，异构节点检测到信号都将来源于同一个方向.

(Ⅰ)当恶意节点通信范围内有两个及其以上异构节点时，异构节点可测得恶意节点的信号到达角度，从而异构节点通过协作，利用信号到达角度信息定位恶意节点. 多异构节点检测原理如图 2 所示，设恶意节点为 $M$，坐标为 $(x,y)$，其伪造的女巫节点为 $S_1$ 和 $S_2$. 异构节点的集合为 $O=\{O_1,O_2\}$，位置坐标分别为 $(x_1,y_1)$ 和 $(x_2,y_2)$. 异构节点 $O_1$ 和 $O_2$ 都能感知到节点 $M$、$S_1$ 和 $S_2$. 异构节点 $O_1$ 和 $O_2$ 测得恶意节点的信号到达角度分别为 $\theta_1$ 和 $\theta_2$. 异构节点 $O_1$ 感知到节点 $M$、$S_1$ 和 $S_2$ 的位置如图 2 中 $M$、$S'_1$ 和 $S'_2$ 所示，异构节点 $O_2$ 感知到节点 $M$、$S_1$ 和 $S_2$ 的位置如图 2 中 $M$、$S''_1$ 和 $S''_2$ 所示.

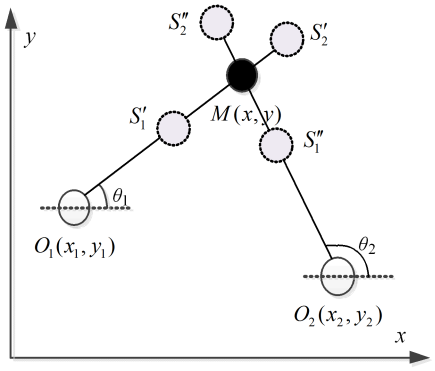



图 2 多异构节点检测原理图

Fig. 2 Schematic diagram of multi-heterogeneous node detection

异构节点 $O_1$ 感知到节点 $M$、$S_1$ 和 $S_2$ 位于同一角度 $\theta_1$，将其列入可疑女巫节点列表. 异构节点 $O_2$ 感知到节点 $M$、$S_1$ 和 $S_2$ 位于同一角度 $\theta_2$，同样将其列入可疑女巫节点列表. 对比分析两个女巫节点列表，公共的节点即为女巫攻击节点.

(Ⅱ)若网络中异构节点的密度较低，且单异构节点通过 AOA 信息检测到可疑女巫节点的存在，但其通信范围内无其他异构节点. 针对此情况，本文提出一种单异构节点的增强检测机制检测女巫攻击，单异构节点检测原理如图 3 所示. 假设图 3(a)中恶意节点为 $M$，坐标为 $(x,y)$，其伪造的女巫节点为 $S_1$ 和 $S_2$，异构节点为 $O$，位置坐标为 $(x_0,y_0)$.

异构节点 $O$ 向周边节点广播测量数据包，并记录广播时间 $T_1$，当节点 $M$ 接收到该数据包后，经过一段时间的处理，节点 $M$ 向异构节点 $O$ 发送确认数据包，其中包含测量数据包接收时间 $T_2$ 与确认数据包发送时间 $T_3$，节点 $M$ 接收该确认数据包并记录到达时间 $T_4$，如图 3(b)所示.

由于网络为静态网络，节点间的距离保持不变，无线电信号传输的速度为恒定值，可利用

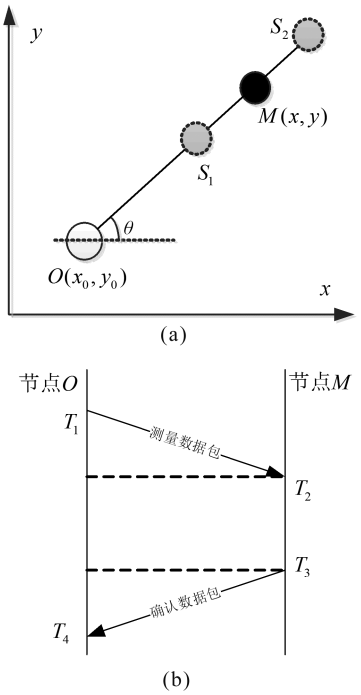



**图 3　单异构节点检测原理图**

**Fig. 3　Schematic diagram of single-heterogeneous node detection**

$$\frac{T_2-T_1}{T_4-T_3}\approx 1 \tag{1}$$

确保节点 $M$ 提供的时间是可信的. 若已知的 4 个时间值满足式(1),则认为节点 $M$ 提供的数据可信,可计算出两节点间信号传播时间(TOA)为

$$\mathrm{TOA}=\frac{(T_4-T_1)-(T_3-T_2)}{2} \tag{2}$$

从而计算出节点 $M$ 与异构节点 $O$ 之间的距离为

$$d=\mathrm{c}\times\mathrm{TOA}=\mathrm{c}\times\frac{(T_4-T_1)-(T_3-T_2)}{2} \tag{3}$$

式中,c 为无线电的传播速度.

利用公式(3)分别计算出节点 $M$、$S_1$ 和 $S_2$ 到异构节点 $O$ 的距离. 通过比较各节点到异构节点的距离可知,若不同节点到异构节点的距离相同,则发现其为女巫攻击节点. 算法思想伪代码如下:

**Algorithm pseudocode**

```
Input: Heterogeneous nodes and normal sensor nodes.
for Each sensor node do
  Broadcast 'Hello' message
  Build the received neighbor node list
end for
for Each heterogeneous node do
  Record the received neighbor node's AOA
  if Some node's AOA is same then
    Heterogeneous nodes build the list of suspicious
      sybil nodes
    The heterogeneous nodes exchange the lists with
    each other
  end if
end for
if Heterogeneous node is density
  for Heterogeneous node do
    Compare the list of suspicious sybil nodes with
      each other
      if Different lists overlap is more than 2then
        Nodes in the intersection section are sybil
        nodes
      end if
    end for
  end if
  if Heterogeneous node is sparse
  for Heterogeneous node do
Send the measurement packet and record the
      time T1, T2, T3, T4
      if (T2−T1)/(T4−T3)≈1 then
      Calculate the TOA and the distance(dSi)
        between heterogeneous node with the
        suspicious sybil node i
          if The distance dSi=dSj(i≠j) then
        the node i and j are sybil nodes
      end if
    end if
    This data is discarded
  end for
  end if
  out put: The list of sybil nodes
```

2.2.2　女巫攻击检测具体步骤

根据上述基本检测原理,女巫攻击检测步骤分为稠密图和稀疏图两种情形进行讨论.

(Ⅰ)稠密图的情形

当网络中异构节点密度较为稠密时,异构节点间的距离较近,公共邻居节点数目较多. 若存在女巫攻击,则利用多异构节点间的协作检测恶意节点,具体步骤如下:

(a)当网络中异构节点收到周围节点的数据包后,记录节点的 ID 与该节点的信号到达角度的值,建立邻节点信息列表.

以图 1 所示的女巫攻击模型为例,异构节点 $O_i$

和$O_j$能够检测到的传感器节点集合为{1,2,4,5,10,11,12,$M$,$S_1$,$S_2$},对应传感器节点的信号到达角度分别为{$\theta_1$,$\theta_2$,…,$\theta_{10}$},建立邻节点信息列表,如表 1 所示.

**表 1 节点 $O_i$ 的邻节点信息列表**

**Tab. 1 List of adjacent nodes of node $O_i$**

| 节点 ID | 1 | 2 | 4 | 5 | 10 | 11 | 12 | $M$ | $S_1$ | $S_2$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 信号到达角度 | $\theta_1$ | $\theta_2$ | $\theta_3$ | $\theta_4$ | $\theta_5$ | $\theta_6$ | $\theta_7$ | $\theta_8$ | $\theta_9$ | $\theta_{10}$ |

同样地,异构节点$O_j$能够得到邻节点信息列表,如表 2 所示.

**表 2 节点 $O_j$ 的邻节点信息列表**

**Tab. 2 List of adjacent nodes of node $O_j$**

| 节点 ID | 2 | 3 | 5 | 7 | 15 | 16 | $M$ | $S_1$ | $S_2$ |
|---|---|---|---|---|---|---|---|---|---|
| 信号到达角度 | $\theta'_1$ | $\theta'_2$ | $\theta'_3$ | $\theta'_4$ | $\theta'_5$ | $\theta'_6$ | $\theta'_7$ | $\theta'_8$ | $\theta'_9$ |

(b)异构节点计算各传感器节点 AOA 值的差值,若信号到达角度差小于阈值$\delta$(本文取$\delta=3°$),则认为传感器节点来自于同一个方向;若同一个方向上的节点数目超过阈值$\eta$(本文取$\eta=2$),则将节点定义为可疑女巫节点.异构节点$O_i$所测得的信号到达角度中$\theta_3$和$\theta_4$,$\theta_5$和$\theta_6$,$\theta_8$、$\theta_9$和$\theta_{10}$的差值均小于阈值$\delta$,将其定义为同方向上的可疑女巫节点.异构节点$O_i$得到可疑女巫节点列表,如表 3 所示.

**表 3 节点 $O_i$ 的可疑女巫节点列表**

**Tab. 3 List of suspected sybil nodes of node $O_i$**

| 可疑女巫节点 | 4、5 | 10、11 | $M$、$S_1$、$S_2$ |
|---|---|---|---|

同样地,异构节点$O_j$得到可疑女巫节点列表,如表 4 所示.

**表 4 节点 $O_j$ 的可疑女巫节点列表**

**Tab. 4 List of suspected sybil nodes of node $O_j$**

| 可疑女巫节点 | 2、15 | $M$、$S_1$、$S_2$ |
|---|---|---|

(c)异构节点$O_i$和$O_j$向周边异构节点发送可疑女巫节点列表.

(d)异构节点$O_i$和异构节点$O_j$对比分析表 3 和表 4,得到公共的可疑女巫节点信息$M$、$S_1$、$S_2$,由检测原理可知$M$、$S_1$、$S_2$为女巫节点,将其列入女巫节点黑名单 Black-List.

(Ⅱ)稀疏图的情形

当网络中异构节点密度较为稀疏时,如图 4 所示.恶意节点$M$仅被异构节点$O_j$检测到,此时无法利用多异构节点检测机制确认是否存在女巫攻击,可利用上述单异构节点检测机制进行识别,具体步骤如下:

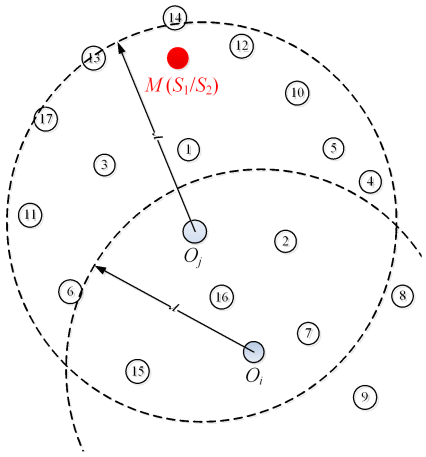



**图 4 异构节点稀疏图**

**Fig. 4 Sparse graph of heterogeneous nodes**

(a)异构节点$O_j$记录周围节点的 ID 与信号到达角度,建立邻节点信息列表.通过检测建立可疑女巫节点列表,如表 5 所示.

**表 5 节点 $O_j$ 的可疑女巫节点列表**

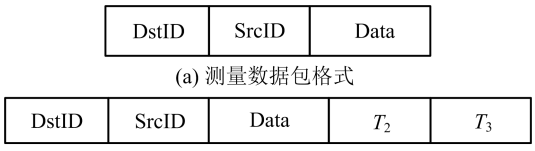
**Tab. 5 List of suspected sybil nodes of node $O_j$**

| 可疑女巫节点 | 1、14、$M$、$S_1$、$S_2$ |
|---|---|

(b)异构节点向可疑女巫节点发送测量数据包,数据包格式如图 5(a)所示.

(c)可疑女巫节点对接收到的测量数据包进行处理,并向异构节点发送确认数据包,数据包包括测量数据、测量数据包接收时间$T_2$和确认数据包发送时间$T_3$,数据包格式如图 5(b)所示.

(d)异构节点接收可疑女巫节点的确认数据包后,分析该数据包.




(a) 测量数据包格式




(b) 确认数据包格式

**图 5 数据包格式**

**Fig. 5 Data packet format**

首先利用公式(1)检测数据包内数据的可信度,若满足公式(1),则认为数据可信;然后利用公式(3)计算可疑女巫节点到自身的距离,若距离相同(如$M$、$S_1$、$S_2$),则发现其为女巫攻击节点,列入女巫节点黑名单 Black-List;若不满足公式(1),原因可能为发送此数据的节点伪造相关数据,该恶意节点的

行为本文不作讨论.

图 5 中,DstID 表示目标节点的标识符,SrcID 表示数据包生成节点的标识符,Data 表示相关数据,$T_2$ 为测量数据包的接收时间,$T_3$ 为确认数据包的发送时间.

## 3　仿真实验与分析

本文以 MATLAB 仿真平台对相关算法进行仿真分析. 在本文的攻击模型下,文献[6]中的检测算法能检测出女巫攻击,其他文献无法检测,故采用与文献[6]相同的仿真环境进行对比实验. 实验环境为:将 100 个普通节点(其中女巫攻击节点的数目为 $m$ 个)和 $n$ 个异构节点随机部署在 100 m×100 m 的方形区域内. 普通节点和异构节点的通信半径分别为 $r$ 和 $R$(本文取 $r$=30 m,$R$=60 m). 将 20 次的实验数据的平均值作为最终的实验结果.

图 6 为网络内存在不同女巫节点个数的情况下,本文算法和文献[6]算法的女巫节点检测率仿真示意图. 设异构节点数目 $n$=30. 横坐标表示网络中存在的女巫节点的数目,纵坐标表示女巫节点的检测率. 实验结果表明,两种算法检测率随女巫节点数目的增加波动都较小,算法的稳定性好,但本文算法比文献[6]算法检测的准确率约高出 5%.

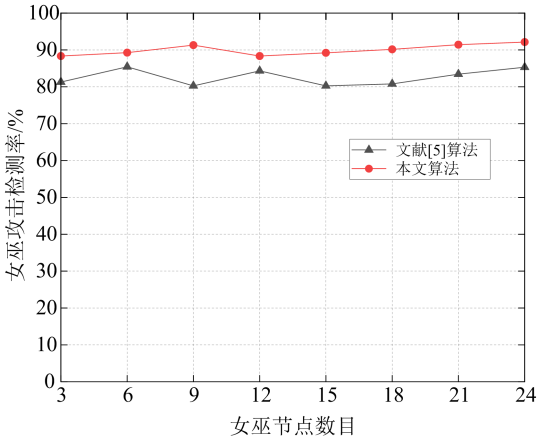



**图 6　两种算法女巫攻击检测率**

**Fig. 6　Two algorithms' sybil attack detection rate**

图 7 是网络中存在不同异构节点数目时的仿真检测结果,两种总算法的检测率(女巫节点数目为 10). 横坐标表示网络内异构节点的数目,纵坐标表示女巫节点的检测率. 由图 7 可知,随着网络内异构节点数目的增加,两种算法的检测率随之增加. 其原因是随着异构节点数目的增加,更多的女巫节点能够被周围的异构节点检测到. 在不同异构节点数目下,本文算法较文献[6]算法有更高的检测率;当异构节点数目少于 30 时,本文算法检测效果更显著. 当网络中异构节点数目达到 30 时,异构节点已基本覆盖部署区域,算法能检测出绝大多数女巫攻击节点. 同时从图 7 还可看出,当异构节点数目继续增加时,本文算法检测率趋于收敛,这表明在该网络环境下,部署 30 个异构节点性价比最高.

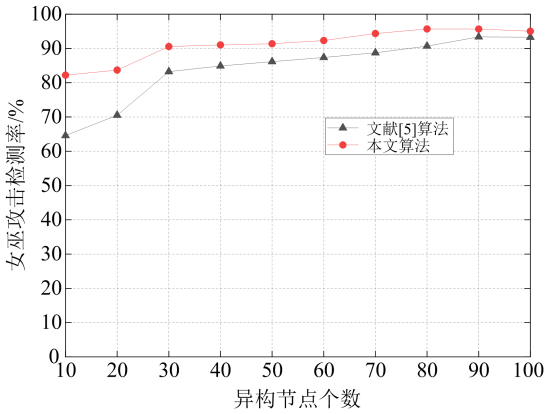



**图 7　不同异构节点数目下两种算法的女巫攻击检测率**

**Fig. 7　Two algorithms' sybil attack detection rate under different number of heterogeneous nodes**

多异构节点检测算法和多异构节点+单异构节点增强的混合算法仿真示意图如图 8 所示. 设女巫节点个数为 10,从图 8 可看出,在异构节点数目较少时,仅采用多异构节点检测方法,检测效率较低;而结合了单异构节点的增强检测算法后,虽需要增加额外的通信开销,但有效地提高了检测率,且增加的开销在可接受范围内;当异构节点数达到 30 时,本文算法主要以多异构节点检测方法为主.

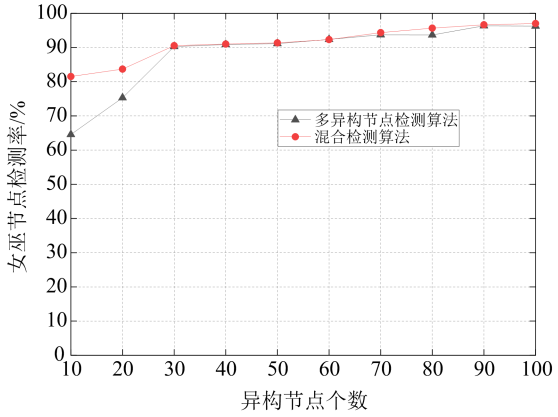



**图 8　多异构节点检测与混合检测算法对比图**

**Fig. 8　Diagram of comparison between multi-heterogeneous node detection and hybrid detection algorithms**

## 4 结论

本文利用带有天线阵列的异构节点检测信号到达角度(AOA),针对异构节点稠密的情形,采用多异构节点协作的方法识别女巫攻击节点,异构节点稀疏的情形,采用单异构节点的增强检测算法检测女巫攻击.与传统的基于定位机制的女巫攻击检测算法相比,本文算法不需要确定节点的具体坐标位置就可以检测女巫攻击节点,简化了计算过程,降低了节点的能耗与时延,检测效率高.

**参考文献(References)**


[1] AMOL Vasudeva, MANU Sood. Survey on sybil attack defense mechanisms in wireless Ad Hoc networks[J]. Journal of Network and Computer Applications, 2018, 120:78-118.

[2] 单志龙, 刘方伟. 天线阵列用于无线传感器网络的节点定位算法[J]. 小型微型计算机系统, 2014, 35(1): 85-88.
SHAN Zhilong, LIU Fangwei. Study for the localization algorithms based on the antenna array in wireless sensor networks[J]. Journal of Chinese Computer Systems, 2014, 35(1):85-88.

[3] SARIGIANNIDIS Panagiotis, KARAPISTOLI Eirni, ECONOMIDES Anastasios A. Detecting sybil attacks in wireless sensor networks using UWB ranging-based information[J]. Expert Systems with Applications, 2015, 42(21): 7560-7572.

[4] JAN Mian Ahmad, NANDA Priyadarsi, HE Xiangjian, et al. A sybil attack detection scheme for a centralized clustering-based hierarchical network[C]// Proceedings of 15th IEEE Trustcom/BigDataSE/ISPA. Helsinki, Finland: IEEE, 2015: 318-325.

[5] CHEN Shanshan, YANG Geng, CHEN Shengshou. A security routing mechanism against sybil attack for wireless sensor networks [C]// International Conference on Communications & Mobile Computing. Shenzhen, China: IEEE Computer Society, 2010: 142-146.

[6] MISRA Satyajayant, MYNENI Sowmya. On identifying power control performing sybil nodes in wireless sensor networks using RSSI [C]//Global Telecommunications Conference. Miami, USA: IEEE, 2010: 1-5.

[7] WEN Mi, LI Hui, ZHENG Yanfei, et al. TDOA-based sybil attack detection scheme for wireless sensor networks[J]. Journal of Shanghai University, 2008, 12(1): 66-70.

[8] YUAN Yali, HUO Liuwei, WANG Zhixiao, et al. Secure APIT localization scheme against sybil attacks in distributed wireless sensor networks[J]. IEEE Access, 2018, 6(99):27629-27636.

[9] SSU Kuo-Feng, WANG Wei-Tong, CHANG Wen-Chung. Detecting sybil attacks in wireless sensor networks using neighboring information[J]. Computer Networks, 2009, 53 (18): 3042-3056.

[10] 胡蓉华, 董晓梅, 王大玲. 无线传感器网络节点复制攻击和女巫攻击防御机制研究[J]. 电子学报, 2015, 43(4):743-752.
HU Ronghua, DONG Xiaomei, WANG Daling. Defense mechanism against node replication attacks and sybil attacks in wireless sensor networks[J]. Acta Electronica Sinica, 2015, 43(4):743-752.

[11] 任秀丽, 江超. 基于分层网格的 Sybil 攻击检测方案[J]. 计算机工程, 2010, 36(11):159-160,163.
REN Xiuli, JIANG Chao. Sybil attack detection scheme based on hierarchical grid[J]. Computer Engineering, 2010, 36(11):159-160,163.

[12] ALSAEDI N, HASHIM F, SALI A, et al. Detecting Sybil Attacks in Clustered Wireless Sensor Networks Based on Energy Trust System (ETS)[J]. Computer Communications, 2017, 110:75-82.

[13] 冀文娟, 石为人, 李明,等. 异构无线传感器网络中多目标优化节点部署策略[J]. 传感器与微系统, 2012, 31(3):29-31.
JI Wenjuan, SHI Weiren, LI Ming, et al. Node deployment strategy of multi-objective optimization for heterogeneous wireless sensor networks [J]. Transduces and Microsystem Technologies, 2012, 31(3):29-31.

[14] 于涛, 郭文强, 朱晓章. 一种 UWB 稀疏阵列天线虚拟中心阵元到达角估计方法[J]. 计算机科学, 2019, 49(Z1):321-324.
YU Tao, GUO Wenqiang, ZHU Xiaozhang. UWB sparse array antenna virtual center element arrival angle estimation method[J]. Computer Science, 2019, 49(Z1):321-324.