



# ACO 结合 P2P 信任模型的无线传感器网络 Sinkhole 攻击检测

合尼古力·吾买尔

(新疆交通职业技术学院, 新疆 乌鲁木齐 831401)

**摘要:**针对无线传感器网络中的 Sinkhole 攻击问题,提出了一种基于蚁群优化(ACO)结合 P2P 信任模型的 Sinkhole 攻击检测(P-ACO)算法。首先,使用蚁群优化算法检测路由中是否存在 Sinkhole 攻击,并生成传感器节点的警报信息;然后,利用布尔表达式进化标记生成算法为群组警报节点分发密钥,并使用密钥标记可疑节点;最后,计算可疑节点列表中各节点的信任值,将信任值低于预设阈值的节点视为攻击节点。分析表明,相比二分查找算法与基于规则匹配的神经网络(RMNN)算法,该算法在匹配过程中需要更少的匹配搜索次数,提高了算法执行效率。实验结果显示,相比 RMNN 算法,该算法可以更加准确地检测 Sinkhole 攻击。

**关键词:**无线传感器网络; Sinkhole 攻击; 二分查找算法; 蚁群优化; P2P 信任模型

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016089

## Sinkhole attack detection based on fusion of ACO and P2P trust model in WSN

HENIGULI Wumaier

Xinjiang Vocational & Technical College of Communications, Urumqi 831401, China

**Abstract:** For the Sinkhole attack problem of wireless sensor network (WSN), a detection algorithm based on fusion of ant colony optimization(ACO) and P2P trust model was proposed. Firstly, ant colony optimization algorithm was used to detect the existence of a Sinkhole attack in route and generate the alarm information of sensor nodes. Then, Boolean expression evolve sign generation algorithm was used to distributed keys for group alarm nodes, and it was used to mark suspicious nodes. Finally, P2P trust model was used to compute trust value of each suspicious node, and the node with trust value was lower than the preset threshold as invasion of node. The analysis shows that the proposed algorithm need less matching search times in matching process than binary search algorithm and the rules matching based neural network(RMNN) algorithm, which indicates that it has improved the efficiency of the algorithm. Experimental results show that the proposed algorithm has higher detection accuracy on Sinkhole attack than RMNN algorithm.

**Key words:** wireless sensor network, Sinkhole attack, binary search algorithm, ant colony optimization, P2P trust model

## 1 引言

目前,无线传感器网络(wireless sensor network, WSN)<sup>[1]</sup>已在许多领域得到广泛应用。若不具备数据机密性和完整性,则 WSN 的应用都毫无意义<sup>[2]</sup>,例如, Sinkhole 攻击<sup>[3]</sup>给 WSN 应用带来了较大的挑战。参考文献[4]提出了一种基于规则匹配的神经网络(rules matching-based neural network, RMNN)算法,可有效检测 Sinkhole 攻击,然而,该算法中每个警报节点存储的密钥数量依赖于网络中警报节点的数量,因此增加了通信成本和内存开销。

本文提出了一种结合蚁群优化(ant colony optimization, ACO)和 P2P 信任模型的攻击检测(P-ACO)算法,用来检测 WSN 中的 Sinkhole 攻击,并确定攻击节点。使用基于蚁群优化的攻击检测算法生成传感器节点的警报信息,在规则库中定义链路质量,传感器节点可根据规则库生成基于节点 ID 的警报信息,构建可疑节点列表,同时利用 P2P 信任模型计算可疑节点的信任度,从而确定攻击节点。实验结果验证了本文算法的有效性及其可靠性。

## 2 系统架构

根据 Sinkhole 攻击检测规则<sup>[5]</sup>,每个传感器节点的本地检测引擎都存在一个规则库,规则库存储了相邻节点的 ID 和每个节点的链路质量,链路质量通过本地数据分组监听模块监听相邻节点间的通信获得。图 1 显示了攻击检测系统模型,用来检测 Sinkhole 攻击。

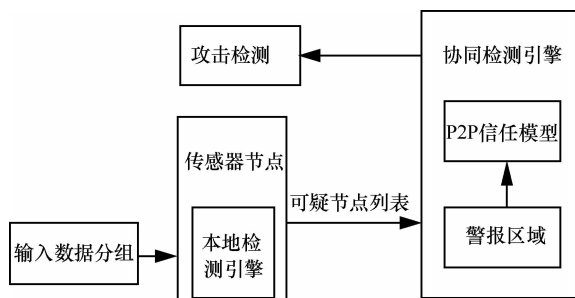


图1 攻击检测系统

从图1可以看出,利用协同检测引擎警报节点,并通过节点相互通信来交换可疑节点名单的ID,随后使用ID检测攻击者。利用具有最小布尔表达式的ACO算法给警报节点分配密钥,用来标记可疑列表。然后执行P2P信任模型计算可疑节点的信任值,将信任值低于阈值的节点作为攻击节点,并将该传感器节点从网络中移除。

本文提出的P-ACO算法主要分为3步:检测攻击,通过ACO算法检测路由中的Sinkhole攻击;标记可疑节点,如存在攻击,利用布尔表达式进化标记生成算法为群组警报节点分发密钥,并使用密钥标记可疑节点,获得可疑节点列表;识别攻击节点,通过P2P信任模型计算可疑节点信任值,从而确定攻击节点。

## 3 利用ACO检测Sinkhole攻击

ACO检测系统模型如图2所示,通过系统中的蚁群协同合作来获取最优解,蚁群中的蚂蚁移动时会留下信息素,用来和其他蚂蚁进行信息交换。蚁群智能代理有正位置和负位置之分,正值初始化为0,负值初始化为节点ID数加1。正位置和负位置表示规则库搜索的位置范围。蚁群智能代理使用从正位置和负位置选择的随机数存储信息素。蚁群智能代理表示节点ID在规则库中的位置,该位置用于与路由更新数据分组发送端进行比较。

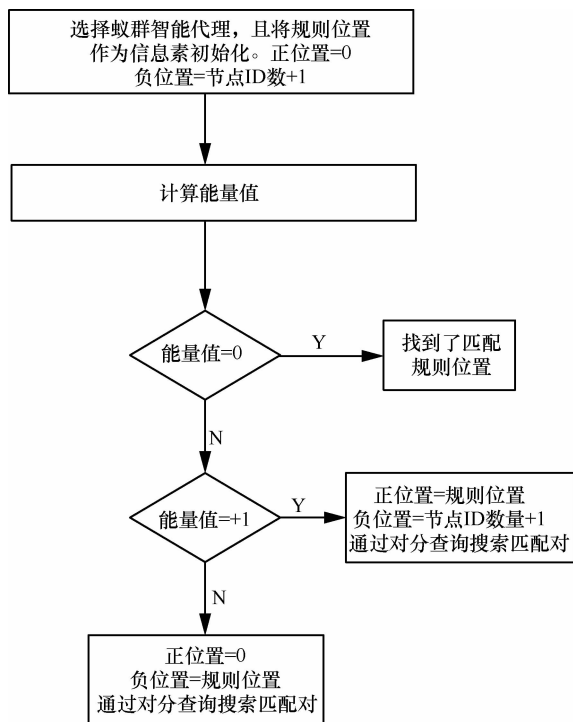


图2 蚁群系统模型

为了确定路由更新数据分组发送端的节点ID是否与规则库中的节点ID匹配,计算每个蚁群智能代理的能量。蚁群智能代理通过比较规则库中的节点ID(该节点ID用信息素表示)和路由更新数据分组发送端节点ID来计算能量值。



若两者的 ID 匹配,则能量值为 0 且停止该过程。若路由更新数据分组节点 ID 小于规则库中的节点 ID,则能量值为 1 且负位置的值被信息素代替,随后针对正位置和负位置的存储值,用二分查找<sup>[6]</sup>匹配路由更新数据分组节点 ID 和规则库中的节点 ID。如果输入数据分组节点 ID 大于用信息素表示的节点 ID,则能量值为+1 且正位置的值被信息素代替,随后针对正位置和负位置的存储值,用二分查找匹配路由更新数据分组节点 ID 和规则库中的节点 ID。如果路由更新数据分组发送端节点 ID 与规则库中的节点 ID 不匹配,则存在 Sinkhole 攻击,同时节点生成警报。如果两者 ID 匹配,则对应的链路质量可信。算法 1 和算法 2 分别显示了二分查找算法和 ACO 算法的伪代码。

设  $A_i$  表示蚁群智能代理,  $S(N_i)$  为第  $i$  个智能代理规则库中第  $j$  个位置的节点 ID, 该节点用于后续比较,  $i=1,2,\dots$ , 代理总数,  $j=1,2,\dots$ , 规则集中的规则总数。  $S(P)$  表示更新数据分组发送端的节点 ID。根据式(1)计算能量值:

$$\begin{aligned} (A_i) &= +1, S(P) > S(N_i) \\ (A_i) &= 0, S(P) = S(N_i) \\ (A_i) &= -1, S(P) < S(N_i) \end{aligned} \quad (1)$$

#### 算法 1 二分查找算法

binarySearch(a, value, left, right)

while left  $\leq$  right

mID := floor((right-left)/2)+left

if a[mID] = value

return mID

if value < a[mID]

right := mID-1

else

left := mID+1

return not found

#### 算法 2 ACO 算法

ACO()

分别初始化正位置和负位置值为 0 以及节点 ID 为+1;

选择用信息素表示规则位置的蚁群智能代理

根据能量函数计算蚁群智能代理  $A_i$  的能量

$$(A_i) = +1, S(P) > S(N_i)$$

$$(A_i) = 0, S(P) = S(N_i)$$

$$(A_i) = -1, S(P) < S(N_i)$$

if (能量=0) then

return(j);

exit( );

else if (能量=+1) then

正位置=j;

负位置=节点 ID+1;

else if (能量=-1) then

正位置=0;

负位置=j;

end if;

binarySearch(S(N), S(P), 正位置, 负位置);

end ACO

## 4 标记可疑节点

### 4.1 警报节点表示

使用二叉树表示警报节点且通过节点标识符识别节点。属于群组的警报节点表示为  $\{N_1, N_2, N_3, \dots, N_{N_1}\}$ , 其中,  $N_1=2^n$ ,  $N_1$  表示群组大小,  $n$  表示群组中每个警报节点的二进制节点标识符 ( $N_{ID}$ ) 的长度。每个警报节点  $N$  的  $N_{ID}$  用二进制形式表示,  $n$  个比特位 ID  $N_{ID}(N)=K_n K_{n-1} K_{n-2} \dots K_1$ , 其中,  $K_i$  要么为 0 要么为 1。  $N_{ID}$  的布尔隶属度函数  $m(\cdot)$  用于确定群组警报节点的存在。如果  $N(K_n K_{n-1} K_{n-2} \dots K_1)=1$ , 则字符为  $N_{ID}(K_n K_{n-1} K_{n-2} \dots K_1)$  的节点为群组警报节点; 如果  $N(K_n K_{n-1} K_{n-2} \dots K_1)=0$ , 则字符为  $N_{ID}(K_n K_{n-1} K_{n-2} \dots K_1)$  的节点不为群组警报节点。

群组的每个警报节点都有群组密钥  $SK$  和辅助密钥集  $k_1, k_2, \dots, k_n$ , 其中, 如果  $K_i=1$ ,  $k_i$  取  $k_i$  值; 如果  $K_i=0$ ,  $k_i$  取  $k_i^j$  值。辅助密钥对应于  $N_{ID}$  中的二进制位。图 3 显示了大小为 4 的群组中警报节点的密钥分布。群组中警报节点以真值表的形式表示, 并使用最小布尔表达式寻找最小数量密钥来加密群组警报节点的群组密钥。表 1 显示了群组的真值, 可以看出, 警报节点  $N_1, N_2, N_3$  在群组中存在。

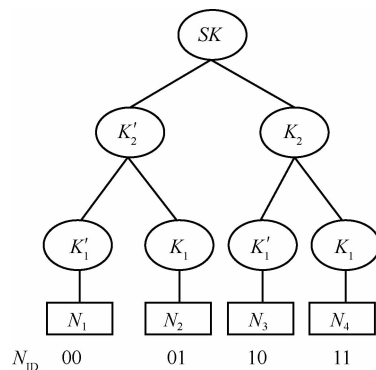


图 3 群组警报节点的密钥分布

表 1 群组警报节点的真值

| 警报节点  | 输入( $K_2K_1$ ) | 输出 |
|-------|----------------|----|
| $N_1$ | 00             | 1  |
| $N_2$ | 01             | 1  |
| $N_3$ | 10             | 1  |
| $N_4$ | 11             | 0  |

4.2 标记可疑节点的密钥分布

利用蚁群优化布尔表达式进化标记生成 (ant colony optimization Boolean expression evolve sign generation, ABXES)算法<sup>[7]</sup>为群组警报节点分发密钥。群组警报节点通过真值表表示。警报节点标识符( $N_{id}$ )为输入,输出值为 1 表示群组中存在警报节点,输出值为 0 表示群组中不存在警报节点。

通过蚁群智能代理协作获取最优解决方案,每个蚁群智能代理通过信息素获取最优解。每个布尔表达式作为蚁群智能代理,该智能代理由“或(OR)”操作联合各自位置的信息素组成<sup>[8,9]</sup>。图 4 描述了在两个变量情况下智能代理的表示方法。例如,在两个变量情况下,拥有信息素{1,4}的蚁群智能代理表示在位置 1 和 4,使用 OR 操作联合对应位置表达式  $K_1$  和表达式  $K_2'$ 。因此,信息素{1,4}表示布尔表达式  $K_1+K_2'$ 。

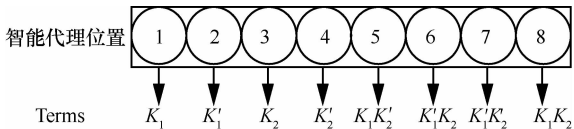


图 4 2 个变量情况下蚁群智能代理的表示方法

对有  $n$  个变量的函数,智能代理表达式的最大数量为  $3^n-1$ 。一般情况下,对有  $n$  个变量的表达式,表达式的数量和针对一个蚁群智能代理的位置数量定义如下:

$$n_{c_1} \cdot 2^1 + n_{c_2} \cdot 2^2 + \dots + n_{c_n} \cdot 2^n = \sum_{i=1}^n (n_{c_i}) 2^i = 3^n - 1 \tag{2}$$

其中,  $n_{c_i}$  表示  $n$  个对象的组合数量。

为了找到智能代理最优解,需要计算智能代理的能量值,通过输出向量的比特位表示,通过布尔表达式计算该输出向量。设  $A_i$  为蚁群智能代理,式(3)和式(4)分别给出了真值表输入向量和智能代理输出向量,利用式(5)计算代理能量。

$$T=(t_1, t_2, t_3, t_4), \quad t_i=0, 1 \tag{3}$$

$$(A_i) = (o_i^{(1)}, o_i^{(2)}, o_i^{(3)}, o_i^{(4)}), \quad o_i^{(j)} = 0, 1 \tag{4}$$

$$(A_i) = count(t_j = o_i^{(j)}) \tag{5}$$

其中,  $count(w_k=z_k)$  为实例的数量,  $w_k$  与  $z_k$  等价。代理信息素的能量值与最大群组对应的最小布尔表达式值相等。

最小布尔表达式获取的最小值表示分发给群组警报节点的辅助密钥的数量最小。使用每个警报节点的辅助密钥加密群密钥且分发给群组警报节点。算法 3 显示了 ABXES 算法伪代码。

算法 3 ABXES 算法伪代码

ABXES()

$K=0$ ;

随机选择蚁群智能代理,表示信息素;

根据能量计算式计算每个智能代理  $A_i$  能量;

能量( $A_i$ ) =  $count(t_j = o_i^{(j)})$ ;

if(代理能量等于群组警报节点最大数量) then

    return(代理的信息素表示布尔表达式);

else

repeat

    通过改变表达式更新信息素且计算代理能量值;

    若当前代理能量值  $\geq$  以前路由代理能量值,选择能量值大的代理信息素;

if(代理能量等于群组警报节点的最大数量) then

    return(代理的信息素表示布尔表达式);

end if

until(能量值等于群组警报节点的最大数量)

end if

end ABXES

5 识别攻击节点

本文利用 P2P 信任模型计算可疑节点的信任值,从而确定攻击节点。P2P 网络信任模型常用来评估节点的可信度<sup>[10]</sup>。其通常根据 5 个因素来计算节点的可信度<sup>[11]</sup>: 邻居节点对该节点的评价;给出评价的邻居节点的可信度;节点交易次数;与交易相关的因素;与交易相关的社会因素。节点  $u$  的信任值的计算式为:

$$T(u) = \alpha \sum_{i=1}^{I(u)} S(u, i) \cdot CR(p(u, i)) \cdot TF(u, i) + \beta \cdot CF(u) \tag{6}$$

其中,  $T(u)$  为节点  $u$  的信任值,  $S(u, i)$  为节点  $u$  第  $i$  次交易所获得的评价,  $p(u, i)$  为与节点  $u$  进行第  $i$  次交易的邻居节点,  $CR(p(u, i))$  为节点  $p(u, i)$  对节点  $u$  的评价的可信度,  $TF(u, i)$  为在节点  $u$  的第  $i$  次交易中,与交易相关的因素(交

易时间和交易额)对信任值的影响, $\alpha$ 为交易因素的权重因子, $\beta$ 为社会因素的权重因子, $CF(u)$ 表示与交易相关的社会因素(奖励机制)所产生的影响。

由于恶意节点可能会对与其交易的节点给出一个虚假评价,例如,恶意节点可能会对一个正常节点给出低信任度评价,需要对评价的可信度进行评估。P2P信任模型中通常有2种对评价进行可信度评估的机制<sup>[12]</sup>:基于节点的可信度;基于评价的相似度度量(PSM)。

本文信任模型中利用PSM机制对邻居节点给出的评价进行可信度评估。PSM机制中,考虑了与节点 $u$ 进行交易的2个节点所给出的评价,并计算这2个评价的相似度,相似度越高,表明该评价可信度越高<sup>[13,14]</sup>。可信度计算公式如式(7)所示。

$$CR(p(u,i),w) = \frac{Sim(p(u,i),w)}{\sum_{i=1}^{I(u)} Sim(p(u,i),w)} \quad (7)$$

其中, $Sim(p(u,i),w)$ 为节点 $w$ 和节点 $p(u,i)$ 给出评价的相似性,如式(8)所示。

$$Sim(p(u,i),w) =$$

$$\sqrt{\sum_{x \in IJS(p(u,i),w)} \left( \frac{\sum_{i=1}^{I(x,p(u,i))} S(x,p(u,i))}{I(x,p(u,i))} - \frac{\sum_{i=1}^{I(x,w)} S(x,w)}{I(x,w)} \right)^2} \quad (8)$$

其中, $IJS(p(u,i),w)$ 为节点 $w$ 和节点 $p(u,i)$ 与节点 $u$ 的交易集合, $S(p(u,i),w)$ 表示节点 $w$ 和节点 $p(u,i)$ 给出的评价

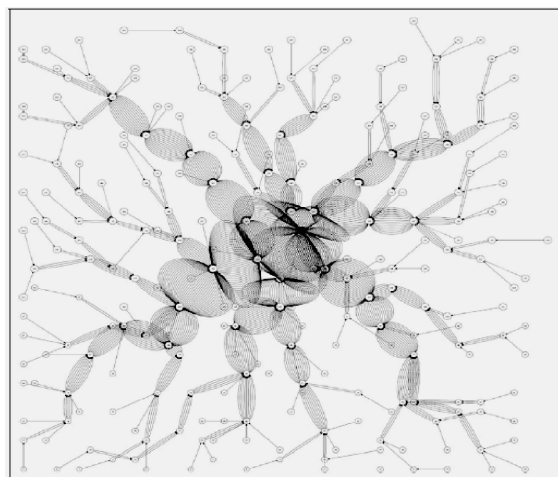
$$\text{向量, } \left( \frac{\sum_{i=1}^{I(x,p(u,i))} S(x,p(u,i))}{I(x,p(u,i))} - \frac{\sum_{i=1}^{I(x,w)} S(x,w)}{I(x,w)} \right)^2 \text{ 为两个评}$$

价向量的标准差。

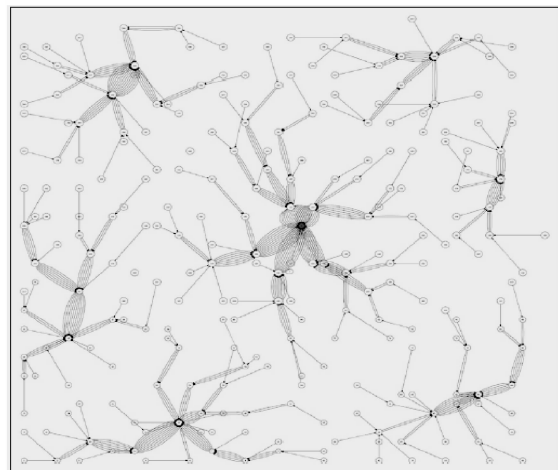
群组中每个警报节点利用它们的辅助密钥解密群组密钥,并将结果存储在内存中。根据可疑节点ID和群组密钥生成消息认证代码。警报节点使用群组密钥标记消息,并将结果传输给群组中的其他警报节点。接收到消息认证代码的警报节点获取了群组密钥,通过比较内存中存储的群组密钥来确定可疑节点。根据P2P信任模型,计算可疑节点的信任值,将低于预设信任阈值的节点认定为攻击节点。

## 6 仿真实验

为了评估本文算法的有效性和优越性,利用基于OMNet++的无线传感器网络仿真器Castalia进行了大量仿真<sup>[15]</sup>,设置节点分散在50 m×50 m的正方形区域内,节点传送所有数据分组到位于区域中央的基站。仿真节点配置如图5所示,图5(a)为无攻击时的网络结构,而图5(b)为Sinkhole攻击下的网络结构,小圆圈代表传感器节点,两个节点之间的连接代表数据分组传输。将本文算法的性能与几种现有的Sinkhole攻击检测算法进行比较。



(a) 无攻击



(b) Sinkhole攻击

图5 两种情况下的WSN拓扑结构

### 6.1 匹配搜索次数比较

将本文算法的匹配搜索次数与对分查算法、RMNN算法进行比较,WSN中传感器节点分别取100、1 000、10 000、100 000,记录各个算法的最佳结果,具体见表2。

表 2 各个算法的匹配搜索次数

| 节点数量/个  | 搜索次数/次 |         |      |
|---------|--------|---------|------|
|         | 二分查找算法 | RMNN 算法 | 本文算法 |
| 100     | 10     | 9       | 6    |
| 1 000   | 15     | 13      | 9    |
| 10 000  | 21     | 18      | 14   |
| 100 000 | 27     | 20      | 16   |

从表 2 可以看出,相比二分查找算法、RMNN 算法,本文算法的匹配搜索次数均为最低,由于本文算法结合了 ACO 与二分查找算法,二分查找匹配节点的数量减少,表明 ACO 在匹配过程中需要更少的匹配时间,提高了算法执行效率。

6.2 检测率比较

仿真环境分别由 100、1 000、10 000、100 000 个随机分布的节点组成,每次仿真中设定 25%的节点为恶意节点(25%),每个节点产生 1 500 个数据分组。每个模拟环境进行 30 次仿真,置信区间为 95%。在 P2P 信任模型中,设定信任阈值为正常节点平均信任值的 50%。表 3 为各算法在存在恶意节点场景中的检测率。

表 3 在不同节点数情况下的检测率

| 节点数量/个  | 检测率     |       |
|---------|---------|-------|
|         | RMNN 算法 | 本文算法  |
| 100     | 100%    | 100%  |
| 1 000   | 98.1%   | 100%  |
| 10 000  | 94.7%   | 98.3% |
| 100 000 | 90.3%   | 96.4% |

从表 3 可以看出,当网络中的节点数量只有 100 个时,2 种算法的攻击检测率均为 100%;当节点数增加到 1 000 个时,本文算法的检测率仍然可以保持在 100%,而 RMNN 算法的检测率则开始降低;节点数增加至 100 000 个时,本文算法也可取得 96%的检测率,比 RMNN 算法高出 6%。本文算法根据规则库中的节点 ID 来识别异常链接,相比 RMNN 算法,能够更加准确地检测 Sinkhole 攻击。

误报率表示攻击检测机制检测到攻击发生,但网络中并未发生攻击,而造成误报的主要原因是无线信道质量不稳定,误报率比较结果见表 4。

可以看出,本文算法的误报率较低,因为本文算法采用了 P2P 信任模型,信任值根据节点的行为和邻居评价计算获得,是节点行为一贯表现的量化,因此基于信任的检

表 4 在不同节点数情况下的误报率

| 节点数量/个  | 误报率     |      |
|---------|---------|------|
|         | RMNN 算法 | 本文算法 |
| 100     | 0       | 0    |
| 1 000   | 1.1%    | 0    |
| 10 000  | 2.3%    | 0.5% |
| 100 000 | 3.6%    | 1.4% |

测机制能够很好地避免因无线信道而产生的误报。

7 结束语

为了检测 WSN 中 Sinkhole 攻击并识别 WSN 中的攻击节点,本文提出了一种基于群体智能的入侵检测算法——P-ACO。实验结果显示,相比经典的匹配算法,P-ACO 算法能准确检测 Sinkhole 攻击,不会产生误检;相比二分查找算法和神经网络算法,P-ACO 算法匹配搜索次数更少,大大提高了算法执行效率;相比 RMNN 算法,P-ACO 算法的内存需求更低。使用 ABXES 算法可以识别攻击者节点,相比 RMNN 算法中的单向散列函数和跳数算法,减少了需要存储的密钥数量,节省了内存。利用 P2P 信任模型进一步确定攻击节点,提高了检测准确度,降低了误报率。

未来将考虑引入其他优化算法,如粒子群优化、遗传算法等,在其他 Sinkhole 攻击环境下进行实验,进一步改善算法的检测性能。

参考文献:

[1] 叶苗,王宇平.一种新的容忍恶意节点攻击的无线传感器网络安全定位方法[J]. 计算机学报, 2013, 36(3): 532-545.  
YE M, WANG Y P. A new malicious nodes attack-resistant security location method in wireless sensor network [J]. Chinese Journal of Computers, 2013, 36(3): 532-545.

[2] 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.  
HU R H, DONG X M, WANG D L. SenLeash: a restricted defense mechanism against wormhole attacks in wireless sensor network[J]. Journal of Communications, 2013, 34(10): 65-75.

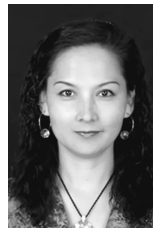
[3] ZHANG F J, ZHAI L D, YANG J C, et al. Sinkhole attack detection based on redundancy mechanism in wireless sensor networks[J]. Procedia Computer Science, 2014, 31(3): 711-720.

[4] LU F, WANG L. Intrusion detection system based on integration of neural network for wireless sensor network[J]. Journal of Software Engineering, 2014, 8(4): 225-238.



- [5] ABDULLAH I, RAHMAN M M, ROY M C. Detecting sinkhole attacks in wireless sensor network using hop count [J]. International Journal of Computer Network and Information Security (IJCNIS), 2015, 7(3): 50-57.
- [6] 李睿, 林亚平, 易叶青, 等. 两层传感器网络中安全 Top-k 查询协议[J]. 计算机研究与发展, 2012, 49(9): 1947-1958.  
LI R, LIN Y P, YI Y Q, et al. A secure Top-k query protocol in two tiered sensor networks [J]. Journal of Computer Research and Development, 2012, 49(9): 1947-1958.
- [7] MENDONCA M, AGUILAR J S, PEROZO N. An emergent ontology for ambient intelligence based on an ant colony optimization algorithm [C]//Computing Conference (CLEI), September 15-19, 2014, Montevideo, Uruguay. New Jersey: IEEE Press, 2014: 1-11.
- [8] WANG H Y, LIU Z Y, YING B U. Ant colony optimization algorithm for WSN cross-layer routing protocol [J]. Journal of Changzhou University, 2014.
- [9] 宋立新, 戴赫. 基于蚁群算法的 WSN 路由协议研究[J]. 哈尔滨理工大学学报, 2014, 42(6): 88-92.  
SONG L X, DAI H. Research on WSN routing protocol based on ant colony algorithm [J]. Journal of Harbin University of Science and Technology, 2014, 42(6): 88-92.
- [10] XIONG L, LIU L. Peertrust: supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.
- [11] 张乐君, 邓鑫, 国林, 等. 基于关联度分析的 WSN 节点信任模型研究[J]. 电子科技大学学报, 2015, 34(1): 106-111.  
ZHANG L J, DENG X, GUO L, et al. A CMP energy consumption estimate model for computer systems [J]. Journal of University of Electronic Science and Technology of China, 2015, 34(1): 106-111.
- [12] 蔡绍滨, 潘虹杞, 姚念民, 等. 基于云信任模型和蚁群算法的 WSN 簇可信路由算法[J]. 软件学报, 2014, 25(s1): 122-130.  
CAI S B, PAN H Q, YAO N M, et al. Cluster reliability routing algorithm based on cloud trust model and ant colony algorithm[J]. Journal of Software, 2014, 25(s1): 122-130.
- [13] WANG M, XU Z, ZHANG Y, et al. Modeling and analysis of PeerTrust-like trust mechanisms in P2P Networks [C]//Global Communications Conference (GLOBECOM), December 3-7, 2012, Anaheim, California, USA. New Jersey: IEEE Press, 2012: 2689-2694.
- [14] LIU S, QI D, MENG J, et al. Study and implementation of wireless sensor networks collaboration based on bio-inspired trust and reputation model (BTRM)[J]. International Journal of Digital Content Technology & Its Applications, 2012, 6 (1): 53-66 .
- [15] LIN C, WU G. Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach [J]. Journal of Supercomputing, 2013, 66(2): 989-1007.

#### [作者简介]



合尼古力·吾买尔 (1976-), 女 (维吾尔族), 新疆交通职业技术学院副教授, 主要研究方向为网络安全、信息安全。