# Blocking all Receiving Links of Wireless Sensor Network

https://doi.org/10.3991/ijoe.v13i09.6957

Zhang Yu(✉),
Southwest University, Chongqing, China
zhangyu@swu.edu.cn

Peng Xiaodong
Neijiang Normal University, Neijiang, China

Liu Feng
Southwest University, Chongqing, China

**Abstract—**Jamming attack is an effective way to disrupt the communication of adversaries. This paper tries to design methods for blocking all receiving links (BARL) of a wireless sensor network (WSN). Firstly the condition for blocking a receiving link is derived and Area for Jamming a Receiving Link (AJRL) is defined. Then BARL jamming method for a network with an unlimited JSR parameter is discussed. Finally, with a limited JSR parameter, BARL jamming attack problems on several networks types, i.e. JN (N,≥N), JN(2,1), JN(3,1) and JN(N,≥2), are discussed; and jamming methods are presented and proved mathematically respectively.

**Keywords—**Jamming, Blocking All Receiving Links, Area for Jamming a Receiving Link, JSR parameter

## 1 Introduction

Wireless sensor network (WSN) plays an important role in various fields. Its communication is based on the open medium and has abroad cast nature[1, 2].Therefore an attacker may launch jamming attack on WSN. Jamming is a malicious attack on WSN[3]. Its objective is to disrupt the communication of the victim network[4]. An attacker is referred as a jammer, which can send radio signals intentionally leading to collide with legitimate signals[5]. Some works [2, 6-8]study on detecting the existence of jammers and preventing them from attacking normal communications. Ref. [9] presents some defense strategies for sensor networks. Unlike these works, we consider using jammers to disrupt the communications of WSN [10, 13].

A jammer in [10] takes advantage of IEEE 802.11 MAC's back off mechanism to disrupt the communications. The jammer targets its actions at the medium access control (MAC) layer and tries to cause collisions to make the contention window large and make the stations transmit less often. Different form [10], the jammer in this paper works at the physical layer. It emits interference to degrade the signal-to-noise ratio and to make the communication impossible. A jamming attack model from spatial perspective[14] is defined as a problem of deployment jammers to minimize the pair-wise connectivity among WSN nodes. The problem is proved to be NP-complete. The authors present a heuristic algorithm to block the links partially. We focus on blocking all receiving links of a WSN. Cognitive radio has characteristics of fast channel switching and quick response time. In[13], a jammer is used to sense traffics on 802.11g networks and create collisions. The jammer locates at a fixed place. Different from them, this paper tries to search and assign locations for jammers.

The remainder of this paper is organized as follows. The BARL jamming problem is formatted in Section 2. Section 3 solves problem of jamming with an unlimited JSR parameter. Section 4 does BARL jamming with a limited JSR parameter. BARL jamming methods for JN(N,≥N), JN(2,1), JN(3,1) and JN(N,≥2) networks are presented respectively. Finally, Section 5 concludes the paper.

## 2 Problem formulation

We focus on the problem of blocking all receiving links of a WSN. To carry out such attacking, the jammer listens to the open medium and broadcast with the same frequency band [15]. Each node in network has bidirectional communication links. $Link_{i\to k}$ represents the sending link for $Node_i$ and the receiving link for $Node_k$. The jamming power to signal power ratio at the receiver determines the degree to which jamming will be successful. For digital signals, the jammer's goal is to raise this ratio to a level such that the bit error ratio[16] is above a certain threshold. The JSR models[17] at the receiver's antenna are defined as

$$\xi = P_{JT}G_{JR}G_{RJ} / P_T G_{TR} G_{RT} * 10^{4\log_{10} D_{TR}/D_{JR}} \tag{1}$$

where $P_{JT}$ is the power of the jammer's transmitting antenna; $P_T$ is the power of the transmitter; $G_{TR}$ is the antenna gain from transmitter to receiver; $G_{RT}$ is the antenna gain from receiver to transmitter; $G_{JR}$ is the antenna gain from jammer to receiver; $G_{RJ}$ is the antenna gain from receiver to jammer; $D_{TR}$ and $D_{JR}$ are the distance between transmitter and receiver, and the distance between jammer and receiver respectively.

The JSR model can be reformatted as

$$D_{JR} = D_{TR}(P_{JT}G_{TR}G_{RJ} / \xi P_T G_{TR} G_{RT})^{1/4} \tag{2}$$

Let $\varphi = (P_{JT}G_{TR}G_{RJ} / \xi P_T G_{TR} G_{RT})^{1/4}$, where $\varphi \geq 0$ .Variable $\varphi$ is referred as JSR parameter. When jamming a link, the condition that a receiving link is blocked can be represented as inequality

$$D_{JR} \leq \varphi D_{TR} \tag{3}$$

From Inequality(3), we see $D_{JR}$ determines whether a link can be blocked. For blocking all receiving links of a WSN, the main task is placing the jammers on appropriate locations to let

$$\forall J, R, T : D_{JR} \leq \varphi D_{TR} \tag{4}$$

The problem of this paper is similar to the Jammer Deployment Problem defined in[14, 18]. For convenience, we define AJRL (Area of Jamming a Receiving Link) to represent an area in which Inequality(3) holds. The WSN works in 3D spaces, therefore the shape of $AJRL_{i\to k}$ is a sphere, and the center of the sphere is the point that $Node_k$ locates. BARL jamming network is represented as $JN(x,y)$, where $x$ is the number of nodes of a WSN, $y$ is the number of jammers.

## 3 BARL attack with an unlimited JSR parameter φ

Several ways may be used to increase the JSR parameter φ, such as 1) increasing the power of jammers' transmitting antenna, the antenna gain from jammer to receiver, or the antenna gain from the receiver to jammer; 2) decreasing the power of transmitter, the antenna gain from receiver to transmitter, or the antenna gain from receiver to transmitter; 3) decreasing the threshold $\xi$.In this section we assume JSR parameter $\varphi$ can be increased unlimitedly.

**Theorem 1**: One jammer can block all receiving links in any network with an unlimited JSR parameter $\varphi$.

Proof: In a $JN(N,1)$ network, there is only one jammer. The distance between the jammer and $Node_k$ is represented as $Dis(Node_k, Jammer_1)$. Let $\varphi^{'} = \max\left(Dis\left(Node_i, Jammer_1\right)/d_{ik}\right), 1 \le i, k \le N, i \ne k$. For JSR parameter $\varphi$ can increase unlimitedly, we can set $\varphi = \varphi^{'} + \Delta$, where $\Delta \ge 0$. At this case, $Dis(Node_k, Jammer_1) \le \varphi d_{ik}$ holds, where $1 \le i,k \le N$ and $i \ne k$. Therefore, all receiving links of each node will be blocked.

According to Theorem 1, Method 1 can be designed for BARL attack on $JN(N,1)$ network. Therefore, BARL attack can be implemented on $JN(N,\ge 1)$network.

**Method 1**: Attracting a WSN through setting JSR parameter to the infinity.

## 4 BARL attack with a limited JSR parameter φ

Usually only a limited JSR parameter is available when attacking a WSN. In this section, we discuss the BARL attack problems on $JN(N,\ge N)$, $JN(2,1)$, $JN(3,1)$ and $JN(N,\ge 2)$networks respectively.

### 4.1 AttackingJN(N, ≥ N)network

When a jammer move towards a node, the distance $D_{JR}$ between them decreases. If a jammer locates on the same position of a node, then $D_{JR} = 0$and $D_{JR} \le \varphi D_{TR}$ holds.

**Theorem 2:** all receiving links of a $Node_k$ can be blocked by a $Jammer_j$.

Proof: $Jammer_j$ can be moved towards the position of $Node_k$. With the moving process, the distance $D_{JR}$ decreases and finally reaches 0. Then $D_{JR} \le \varphi D_{TR}$ holds, all receiving links of $Node_k$ will be blocked by $Jammer_j$. □

From Theorem 2, it is possible to block all receiving links of a $JN(N, \geq N)$ network.

**Theorem 3:** all receiving links of all nodes can be blocked in a $JN(N, \geq N)$ network.

Proof: As the number of jammers is greater than the number of WSN nodes, $N$ jammers can be selected and placed on the same positions of $N$ nodes respectively. From Theorem 2, it is obvious that all receiving links of any $Node_k$ are blocked. Therefore all receiving links of all nodes can be blocked in a $JN(N, \geq N)$ network.

According to **Theorem 2** and **Theorem 3**, **Method 2** can be used for BARL attacking on $JN(N, \geq N)$ networks.

**Method 2:** For $JN(N, \geq N)$ network, select $N$ jammers and place them on the same locations of the $N$ nodes respectively. The rest of the jammers are placed randomly.

### 4.2 Attacking JN(2, 1)network

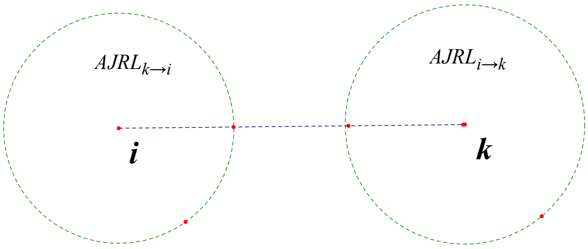
Whether BARL attack can be launched on $JN(2,1)$ network depends on the value of JSR parameter $\varphi$.

**Theorem 4:** when $\varphi < 0.5$, it is impossible to block all receiving links in $JN(2,1)$networks.

Proof: Let the two nodes are $\mathrm{Node_i}$ and$\mathrm{Node_k}$. The distance between them is $d_{ik}$.There are two AJRLs ( $AJRL_{k\to i}$ and $AJRL_{i\to k}$ ). The radii of them are $\varphi d_{ik}$. The center points of $AJRL_{k\to i}$ and $AJRL_{i\to k}$ locate on the positions of $Node_i$ and $Node_k$ respectively.

$$\varphi d_{ik} + \varphi d_{ik} = 2\varphi d_{ik}$$
$$\varphi < 0.5$$
$$\therefore 2\varphi d_{ik} < d_{ik}$$

There is no intersection between $AJRL_{k\to i}$ and $AJRL_{i\to k}$. It is impossible to find a point for the jammer to block all receiving links of $Node_i$ and $Node_k$.

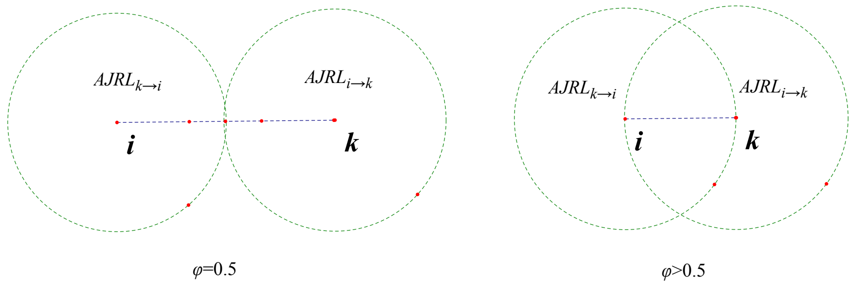


$\varphi$<0.5

**Fig. 1.** The AJRLs of JN(2,1) under φ<0.5

**Theorem 5:** when $\varphi \geq 0.5$, it is possible to block all receiving links in $JN(2,1)$networks.

Proof: Let the two nodes are $\text{Node}_\text{i}$ and $\text{Node}_\text{k}$. The distance between them is $d_{ik}$. There are two AJRLs ( $AJRL_{k\to i}$ and $AJRL_{i\to k}$ ). The radii of them are $\varphi d_{ik}$. The center points of $AJRL_{k\to i}$ and $AJRL_{i\to k}$ locate on the positions of $Node_i$ and $Node_k$ respectively.



φ=0.5

φ>0.5

**Fig. 2.** The AJRLs of JN (2, 1) under φ≥0.5

$$\text{Q}\ \ \varphi Dis(Node_i, Node_j) + \varphi Dis(Node_i, Node_j) = 2\varphi Dis(Node_i, Node_j)$$

$$\varphi \geq 0.5$$

$$\therefore 2\varphi Dis(Node_i, Node_j) \geq Dis(Node_i, Node_j)$$

When $\varphi = 0.5$ , there is one and only one intersection point between $AJRL_{k\to i}$ and $AJRL_{i\to k}$ .When $\varphi > 0.5$ , there are more than one intersection points between $AJRL_{k\to i}$ and $AJRL_{i\to k}$ .If the jammer is placed on the intersection points, all receiving links in $JN(2,1)$ networks will be blocked.

According to Theorem 4 and Theorem 5, Method 3 can be used for BARL attack on $JN(2,1)$ network.

**Method 3:** When jamming $JN(2,1)$ network, if $\varphi \geq 0.5$, place the jammer on the middle point of the two nodes; if $\varphi < 0.5$, it's impossible to launch BARL attack.

### 4.3 Attacking JN(3, 1) network

To block all receiving links in $JN(3,1)$ networks, there should be intersection points among all AJRLs. As shown in **Error! Reference source not found.**, there are three nodes, $Node_i$, $Node_k$ and $Node_q$. The distances between one node and another are $d_{ik}$, $d_{iq}$ and $d_{kq}$. If an intersection existed among all AJRLs, then following inequity holds.

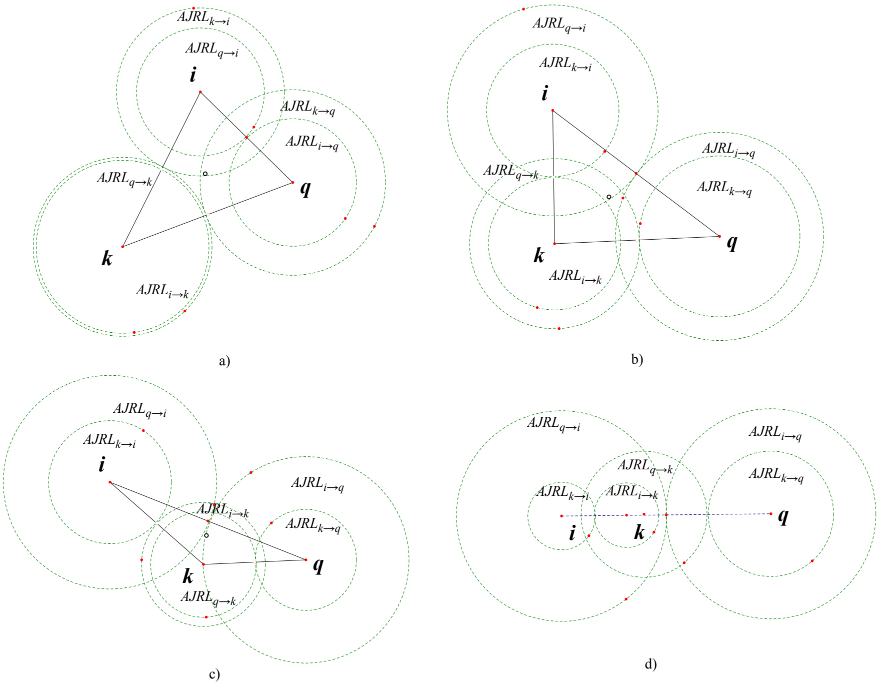
$$\begin{cases} \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{ik}, \varphi d_{qk}) \geq d_{ik} \\ \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{iq}, \varphi d_{kq}) \geq d_{iq} \\ \min(\varphi d_{ik}, \varphi d_{qk}) + \min(\varphi d_{iq}, \varphi d_{kq}) \geq d_{kq} \end{cases} \tag{5}$$

$\varphi < 0.5$

**Theorem 6:** when $\varphi < 0.5$, it is impossible to block all receiving links in $JN(3,1)$ networks.

Proof: Let the nodes are $Node_i$, $Node_k$ and $Node_q$. When $\varphi < 0.5$, there is no intersection between $AJRL_{k\to i}$ and $AJRL_{i\to k}$. Therefore there is no intersection point among $AJRL_{k\to i}$, $AJRL_{k\to q}$, $AJRL_{i\to k}$, $AJRL_{i\to q}$, $AJRL_{q\to i}$ and $AJRL_{k\to q}$. It is impossible to find a point for the jammer to block all receiving links in $JN(3,1)$ networks.

$\boldsymbol{\varphi = 0.5}$



a) b) c) d)

**Fig. 3.** The AJRLs of JN(3,1) under φ=0.5

**Theorem 7:** when $\varphi = 0.5$, it is impossible to block all receiving links in $JN(3,1)$ networks.

Proof: according to the relationship of $d_{ik}$, $d_{iq}$ and $d_{kq}$, there are three cases. Without loss of generality, assume case 1) as $d_{ik} < d_{iq} < d_{kq}$; case 2) as $d_{ik} = d_{iq} < d_{kq}$ or $d_{ik} < d_{iq} = d_{kq}$; case 3) as $d_{ik} = d_{iq} = d_{kq}$.

1) $d_{ik} < d_{iq} < d_{kq}$

Q $\varphi = 0.5$

$d_{ik} < d_{iq} < d_{kq}$

$$\therefore \begin{cases} \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{ik}, \varphi d_{qk}) = \varphi d_{ki} + \varphi d_{ki} = d_{ik} \\ \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{ki} + \varphi d_{iq} < d_{iq} \\ \min(\varphi d_{ik}, \varphi d_{qk}) + \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{ik} + \varphi d_{iq} < d_{kq} \end{cases}$$

Inequality(5) does not hold.

2) $d_{ik} = d_{iq} < d_{kq}$ or $d_{ik} < d_{iq} = d_{kq}$

Q $\varphi = 0.5$

$d_{ik} = d_{iq} < d_{kq}$

$$\therefore \begin{cases} \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{ik}, \varphi d_{qk}) = \varphi d_{ki} + \varphi d_{ki} = d_{ik} \\ \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{ki} + \varphi d_{iq} < d_{iq} \\ \min(\varphi d_{ik}, \varphi d_{qk}) + \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{ik} + \varphi d_{iq} < d_{kq} \end{cases}$$

Inequality(5) does not hold.

Q $\varphi = 0.5$

$d_{ik} < d_{iq} = d_{kq}$

$$\therefore \begin{cases} \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{ik}, \varphi d_{qk}) = \varphi d_{ki} + \varphi d_{ki} = d_{ik} \\ \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{ki} + \varphi d_{iq} < d_{iq} \\ \min(\varphi d_{ik}, \varphi d_{qk}) + \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{ik} + \varphi d_{iq} < d_{kq} \end{cases}$$

Inequality(5) does not hold.

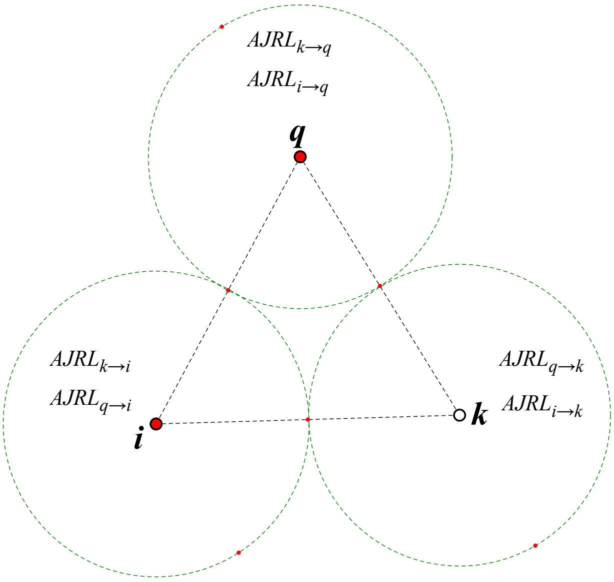


**Fig. 4.** The AJRLs of JN(3,1) under φ=0.5 and $\mathrm{d_{ik}} = \mathrm{d_{ik}} = \mathrm{d_{kq}}$

3) $d_{ik} = d_{iq} = d_{kq}$

Q $\varphi = 0.5$

$d_{ik} = d_{iq} = d_{kq}$

$$\therefore \begin{cases} \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{ik}, \varphi d_{qk}) = \varphi d_{ki} + \varphi d_{ki} = d_{ik} \\ \min(\varphi d_{ki}, \varphi d_{qi}) + \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{ki} + \varphi d_{iq} = d_{iq} \\ \min(\varphi d_{ik}, \varphi d_{qk}) + \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{ik} + \varphi d_{iq} = d_{kq} \end{cases}$$

Inequality(5) holds.

As shown in Figure, $AJRL_{k\to i}$ and $AJRL_{q\to i}$ have same size, their center point locates on $\mathrm{Node_i}$; $AJRL_{i\to q}$ and $AJRL_{k\to q}$ have same size, their center point locates on $\mathrm{Node_q}$; $AJRL_{i\to k}$ and $AJRL_{q\to k}$ have same size, their center point locates on $\mathrm{Node_k}$. $AJRL_{k\to i}$ and $AJRL_{i\to k}$ have only one intersection point. $AJRL_{i\to q}$ and $AJRL_{q\to i}$ have only one intersection point. $AJRL_{k\to q}$ and $AJRL_{q\to k}$ have only one intersection point. The three points locate on different locations. So there is no intersection among $AJRL_{i\to q}$, $AJRL_{i\to q}$ and $AJRL_{k\to q}$.

Therefore, when $\varphi = 0.5$, it is impossible to block all receiving links in $JN(3,1)$ networks.

$\boldsymbol{\varphi \geq 1}$

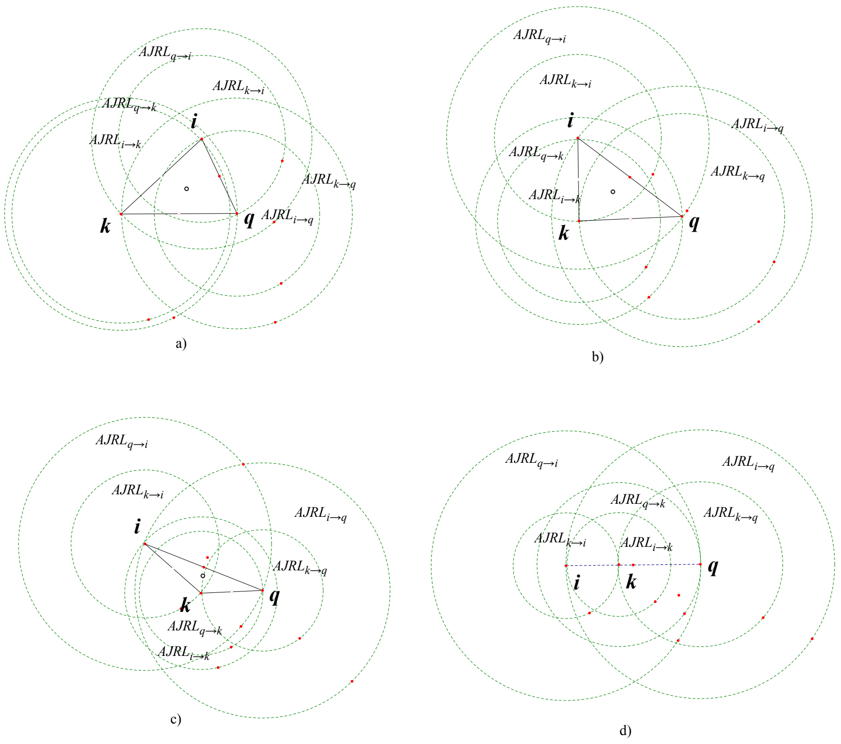


**Fig. 5.** The AJRLs of JN (3, 1) under φ ≥ 0.5

**Theorem 8:** when $\varphi \geq 1$, it is possible to block all receiving links in $JN(3,1)$ networks.

Proof: we provide a method finding a point for the jammer to block all receiving links. The point should locate in the intersection of all AJRLs, i.e. inequality(6) should hold.

$$\begin{cases} Dis(Node_i, Jammer_j) \leq \min(\varphi d_{ki}, \varphi d_{qi}) \\ Dis(Node_k, Jammer_j) \leq \min(\varphi d_{ik}, \varphi d_{qk}) \\ Dis(Node_q, Jammer_j) \leq \min(\varphi d_{iq}, \varphi d_{kq}) \end{cases} \tag{6}$$

Without loss of generality, let $d_{ik} \leq d_{iq} \leq d_{kq}$.

Q $d_{ik} \leq d_{iq} \leq d_{kq}$

$$Dis(Node_i, Jammer_j) \leq \min(\varphi d_{ki}, \varphi d_{qi}) = \varphi d_{ik} \tag{7}$$

$$Dis(Node_k, Jammer_j) \leq \min(\varphi d_{ik}, \varphi d_{qk}) = \varphi d_{ik} \tag{8}$$

$$Dis(Node_q, Jammer_j) \leq \min(\varphi d_{iq}, \varphi d_{kq}) = \varphi d_{iq} \tag{9}$$

Let $Line_{ik}$ be the line segment between $Node_i$ and $Node_k$. If place the jammer on any point on $Line_{ik}$, inequality(7) and (8) hold.

Let $Line_{iq}$ be the line segment between $Node_i$ and $Node_q$. If place the jammer on any point on $Line_{iq}$, inequality(9) holds.

The line segments $Line_{ik}$ and $Line_{iq}$ have a common point $Node_i$.

Therefore, if place the jammer on the position of $Node_i$, all receiving links in $JN(3,1)$ networks will be blocked.

**$0.5 < \varphi < 1$**

Without loss of generality, let $d_{ik} \le d_{iq} \le d_{kq}$.

$$
\begin{cases}
Dis(Node_i, Jammer_j) \le \min(\varphi d_{ki}, \varphi d_{qi}) \\
Dis(Node_k, Jammer_j) \le \min(\varphi d_{ik}, \varphi d_{qk}) \\
Dis(Node_q, Jammer_j) \le \min(\varphi d_{iq}, \varphi d_{kq})
\end{cases}
$$

$$
\xleftarrow{d_{ik} \le d_{iq} \le d_{kq}}
\begin{cases}
Dis(Node_i, Jammer_j) \le \varphi d_{ik} \\
Dis(Node_k, Jammer_j) \le \varphi d_{ik} \\
Dis(Node_q, Jammer_j) \le \varphi d_{iq}
\end{cases}
\tag{10}
$$

$$
\Leftrightarrow
\begin{cases}
\varphi \ge Dis(Node_i, Jammer_j) / d_{ik} \\
\varphi \ge Dis(Node_k, Jammer_j) / d_{ik} \\
\varphi \ge Dis(Node_q, Jammer_j) / d_{iq}
\end{cases}
\Leftrightarrow
$$

$$
\varphi \ge \max\left(\frac{Dis(Node_i, Jammer_j)}{d_{ik}}, \frac{Dis(Node_k, Jammer_j)}{d_{ik}}, \frac{Dis(Node_q, Jammer_j)}{d_{iq}}\right)
$$

Equality (10) gives out the lower limit value of JSR parameter $\varphi$, which needed to block all receiving links. Method **4**is introduced to search the lower limit value of $\varphi$ and the position for the jammer. Step 1-2 initialize JSR parameter's upper bound $ub$ and lower bound $ul$ to 10 and 0 respectively. Step 3 sets variable $jamall$ to $false$ (unable to block all receiving links). Step 4 starts a loop to look for lower JSR parameter which can be used to block all receiving links. Step 5 calculates the mean value of $ub$ and $ul$, and assigns it to variable $\varphi$. Step 6 selects minimal distance of $d_{ik}$, $d_{kq}$ and $d_{iq}$, and assigns to $d_{\min}$. Step 7-9 draw three spheres with centers locating on $Node_i$, $Node_k$ and $Node_q$ respectively. All spheres have radii of $\varphi d_{\min}$. Step 10 checks whether intersection existed among the three spheres. If existed, all receiving links can be blocked using current JSR parameter $\varphi$. So $ub$ is set to $\varphi$ (step 11) and $jamall$ is set to $true$ (step 12). Otherwise, $ul$ is set to $\varphi$ (step 14). Step 5-14 continue till $ub$ equals $ul$.

**Attacking method**

**Method 4:**

```
FindMinimal()
$ub = 10;$ //upper bound
$lb = 0;$ //lower bound
$jamall$ = false
while ($ub \neq lb$)
    $\varphi = (ub + lb) / 2$
    $d_{\min} = \min(d_{ik}, d_{kq}, d_{iq})$
    DrawSphere (Sphere$_i$.$Radius = \varphi d_{\min}$; Sphere$_i$.$Center = U_i.loc$)
    DrawSphere ( Sphere$_k$.$Radius = \varphi d_{\min}$; Sphere$_k$.$Center = U_k.loc$)
    DrawSphere ( Sphere$_q$.$Radius = \varphi d_{\min}$; Sphere$_q$.$Center = U_q.loc$)
    if HaveIntersection(Sphere$_i$, Sphere$_k$, Sphere$_q$, $nil$) then
        $ub = \varphi$
        $jamall$ = true
    else
        $lb = \varphi$
```

**Method 5:** When jamming $JN(3,1)$ network, 1) if $\varphi \geq 1$, compute the length of $Line_{ik}$, $Line_{iq}$ and $Line_{kq}$. Find the intersection point between the shortest two lines. Place the jammer on the intersection point; 2) if $\varphi \leq 0.5$, it's impossible to launch BARL attack; 3)if $0.5 < \varphi < 1$, use Method **4** for jamming attack.

### 4.4 Attacking JN(N, ≥ 2) network

As respect to $JN(N, \geq 2)$ network, 2 or more jammers are available. It can be divided into sub networks. We use Method 6 for jamming attack.

**Method 6:** If possible, divide $JN(N, \geq 2)$ networks into $JN(3,1)$, $JN(2,1)$ and $JN(1,1)$ networks, then use

Method **5**, Method 3 and Method 2 to launch BARL attack respectively.

When dividing a $JN(N, \geq 2)$ network, it may not be divided sub network with types of $JN(3,1)$, $JN(2,1)$ and $JN(1,1)$. There may be sub-networks of $JN(\geq 4,1)$ types. We will discuss the BARL attack on $JN(\geq 4,1)$ network later.

## 5 Conclusion

This paper discusses the problem of blocking all receiving links of a WSN. We formulate the jamming problem and the condition that a receiving link is blocked ( $D_{JR} \leq \varphi D_{TR}$ ). Then AJRL is defined to represent an area in which $D_{JR} \leq \varphi D_{TR}$ holds. We study the problem of jamming attack with an unlimited JSR parameter and provide a method for it. In case of jamming with an limited JSR parameter, several network types, i.e. $JN(N, \geq N)$, $JN(2,1)$, $JN(3,1)$ and $JN(N, \geq 2)$, are discussed. Then jamming methods are provided for them respectively. Our contributions include 1) Unlike the work of references, we stand on the attacking side and propose BARL jamming methods for dynamic change networks; 2) Theorems are provided and proved mathematically for constructing jamming methods. Most of the BARL jamming methods are based on these theorems; 3) The BARL methods are useful for launching attack to block all receiving links of WSNs. Our work may also provide ideas for designing methods to disrupt part of the links.

## 6 Acknowledgements

This research is supported by the Fundamental Research Funds for the Central Universities (XDJK2016C044), the Fund for the Doctoral Program, the Research Project of Sichuan Provincial Education Department and the Chongqing Intelligent Instrument and Control Equipment Engineering Technology Research Center.

## 7 References

[1] D. Niyato, P. Wang, I. K. Dong, Z. Han, and L. Xiao, "Game Theoretic Modeling of Jamming Attack in Wireless Powered Networks," pp. 1-8, 2014.

[2] R. Naresh and K. P. Kumar, "Prevention of Selective Jamming Attacks Using Packet Hiding Methods in Wireless Networks," International Journal of Computer Science & Mobile Computing, vol. 3, pp. 25-28, 2014.

[3] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Security Issues and Attacks in Wireless Sensor Network," World Applied Sciences Journal, vol. 30, pp. 1224-1227, 2014.

[4] Y. Zhang and L. Yang, "Triangle and GA Methods for UAVs Jamming," Mathematical Problems in Engineering, vol. 2014, pp. 1-8, 2014. https://doi.org/10.1155/2014/917147

[5] K. Venkatraman, J. V. Daniel, and G. Murugaboopathi, "Various Attacks in Wireless Sensor Network: Survey," International Journal of Soft Computing and Engineering (IJSCE) ISSN, pp. 2231-2307, 2013.

[6] T. Nguyen, B. Nguyen, V. Mai, H. Pham, and T. Truong, "An efficient solution for preventing dis' ing attack on 802.11 networks," in The International Conference on Green Technology and Sustainable Development, 2013, pp. 1-10.

[7] G. J. Lakshmi, S. Babu, B. L. Rao, P. Mohan, and B. S. Kumar, "Jamming Attacks Prevention in Wireless Sensor Networks Using Secure Packet Hiding Method," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, pp. 3429-3433, 2013.

[8] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11 p Vehicular Networks," IEEE communications letters, vol. 18, pp. 110-113, 2014. https://doi.org/10.1109/LCOMM.2013.102213.132056

[9] W. Y. Xu, K. Ma, W. Trappe, and Y. Y. Zhang, "Jamming sensor networks: Attack and defense strategies," Ieee Network, vol. 20, pp. 41-47, May-Jun 2006. https://doi.org/10.1109/MNET.2006.1637931
[10] R.-T. Chinta, T. F. Wong, and J. M. Shea, "Energy-efficient jamming attack in IEEE 802.11 MAC," in Military Communications Conference, 2009. MILCOM 2009. IEEE, 2009, pp. 1-7. https://doi.org/10.1109/MILCOM.2009.5379992
[11] Y. Sun, X. Wang, and X. Zhou, "Jamming attack in WSN: a spatial perspective," in Proceedings of the 13th international conference on Ubiquitous computing, 2011, pp. 563-564. https://doi.org/10.1145/2030112.2030214
[12] S. Prasad and D. J. Thuente, "Jamming attacks in 802.11 g—A cognitive radio based approach," in MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011, 2011, pp. 1219-1224.
[13] S. Prasad and D. J. Thuente, "Jamming attacks in 802.11g — A cognitive radio based approach," in Military Communications Conference, 2011 - Milcom, 2011, pp. 1219-1224.
[14] Y. Sun, X. Wang, and X. Zhou, "Jamming attack in WSN: a spatial perspective," in International Conference on Ubiquitous Computing, 2011, pp. 563-564. https://doi.org/10.1145/2030112.2030214
[15] P. Chaturvedi and K. Gupta, "Detection and Prevention of various types of Jamming Attacks in Wireless Networks," ed: IJCNWC, 2013, pp. 75-19.
[16] H. Li and W. Ye, "A Study on the Influence of Bit Error Ratio against Jamming Signal Ratio under Different Channel Jamming," in International Symposium on Computational Intelligence and Design, 2016, pp. 58-61. https://doi.org/10.1109/ISCID.2016.1022
[17] R. Poisel, Modern communications jamming principles and techniques: Artech House Publishers, 2011.
[18] X. Wei, Y. Hu, J. Fan, and B. Kan, "A Jammer Deployment Method for Multi-hop Wireless Network Based on Degree Distribution," in Ninth International Conference on Broadband and Wireless Computing, Communication and Applications, 2014, pp. 261-266.

## 8 Authors

**Zhang Yu** received the Undergraduate Degree of Computer Science and Technology in 2002, the Post Graduate degree of Automation in 2005 from Southwest University and Ph.D of Communication Engineering in 2016 from Chongqing University of China. He has more than 30publications in National, International Conference and International Journals. He has more than12 years of teaching experience. He is an associate professor in Southwest University of China. His main research interests include Network and Data Security, Mobile Ad-hoc Networks, Wireless Sensor Networks, Network Jamming Attack, Industrial Wireless Communication, etc.

**Peng Xiaodong** is a lecture of Neijiang Normal University of China.

**Liu Feng** is a professor of the School of Computer and Information Science.Southwest University of China

Article submitted 28 March 2017. Published as resubmitted by the authors 16 June 2017.