INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
*Int. J. Commun. Syst.* 2016; **00**:1–17
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/dac

# Topology Control in the Presence of Jammers for Wireless Sensor Networks

Prasenjit Bhavathankar, Ayan Mondal, and Sudip Misra*†

*Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India*

## SUMMARY

In this paper, the problem of ensuring packet delivery ratio and high network lifetime in wireless sensor networks (WSNs) in the presence of single or multiple jammers is studied using *Single-Leader-Multiple-Followers Stackelberg game theory*. A topology control scheme is proposed, in which the sink node, which acts as the leader, identifies the set of jamming affected nodes. On the other hand, the sensor nodes, which act as followers, need to decide an optimum transmission power level, while ensuring an optimal set of neighbor nodes covered. A scheme, named TC-JAM, for ensuring packet delivery ratio, while avoiding jammers and increasing network lifetime in WSNs, is proposed. In existing literatures, the sensor nodes are envisioned to be equipped with multiple interfaces, while having access for multiple channels. However, in TC-JAM, the sensor nodes have simple hardware with single interface for communication, i.e., the sensor nodes have single channel for communication. Additionally, in the proposed scheme, TC-JAM, each sensor node has a provision to vary its transmission power according to the chosen strategies. Using TC-JAM, the energy consumption of the overall network reduces by up to 62%, and the network lifetime increases by 56-73%.

Received . . .

KEY WORDS: Topology Control, Jammer, Dynamic Transmission power level Model, Wireless Sensor Network, Stackelberg Game, Network Lifetime.

## 1. INTRODUCTION

WSNs are highly vulnerable to the different types attacks [1]. *Jamming* [2] is one of the popular ways of attacking WSNs [3]. The jammer nodes transmit radio signals in the same frequency as that done by the normal nodes. Thus, the jmmers restrict communication between the nodes. Hence, due to multiple unsuccessful retransmissions, the network lifetime gets reduced. The communication of the nodes gets affected due to presence of jammers. Therefore, if the jammers stop sending jamming radio signals, the nodes starts behaving normally. Hence, the effect of jamming is temporary in nature.

### *1.1. Motivation*

In the existing literature, researchers have considered several kinds of jammers. Jamming can be done using a single transmitter or by a jamming station consisting of multiple transmitters. Mpitziopoulos *et al.* [4] classified the jamming nodes to be divided into four categories of jammers

†

*Correspondence to: Sudip Misra, Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India.
†E-mail:smisra@sit.iitkgp.ernet.in

— proactive or constant, deceptive, random, and reactive. In this work, we consider that the jamming nodes can follow any of the aforementioned jamming models. Hence, in case of jamming, the jammers keep wireless channel busy, causes interference, and corrupt the transmitted packets. In the existing literature, several jamming node detection techniques and models to countermeasure the jamming effects are proposed. However, these approaches are hard to realize in real-life scenarios. Additionally, in existing literature, the sensor nodes are envisioned to be equipped with multiple interfaces, while considering that the sensor nodes can communicate through any of the available multiple communication channel. Mpitziopoulos *et al.* [4] surveyed the difficulties encountered with the existing countermeasure mechanisms — regulated transmitted power, antenna polarization, frequency-hopping spread spectrum, direct-sequence spread spectrum [5], directional transmission, and use of ultra wide band (UWB) technology. However, in the existing literature, no *topology control* mechanism is envisioned for anti-jamming, while deciding the transmission power level in a dynamic and distributed manner with consideration that the sensor nodes are equipped with single interface for communication.

### *1.2. Contribution*

We focus on ensuring high network lifetime in the presence of jamming nodes in WSNs, while maintaining the packet delivery ratio intact. In this work, we consider that all nodes are able to modify their transmission power levels according to their requirements. Initially, each node decides an optimum transmission power level, while covering the optimum number of neighbor nodes. On the other hand, the sink node finds out the set of jamming affected nodes, based on the information provided by the nodes deployed in the network. The *contributions* of this work are summarized as follows:

a) In this paper, we propose a *topology control* scheme, named TC-JAM, for the sensor nodes with single interface in the presence of jamming in wireless sensor networks. TC-JAM confirms the integrity of packet delivery, while ensuring minimal energy consumption and increased network lifetime. In this process, the sink node collects the neighbor node table information from each node and tries to detect jamming affected area.

b) The proposed topology scheme ensures increase in network lifetime. We consider that the sensor nodes have single interface for communication, as these nodes are energy constrained and need to have simple hardware interface.

c) We propose a topology control mechanism, using which each node decides an optimal transmission power level, while ensuring the coverage of the optimal set of neighbor nodes.

d) For topology control, we use the *Single-Leader-Multiple-Follower Stackelberg game*. The sink node acts as the leader, and the sensor nodes act as the followers. We propose an algorithm for nodes to avoid jamming, while exploring topology control with modifying the transmission power levels.

### *1.3. Paper Organization*

The remainder of the paper is organized as follows. We briefly present the related literature in Section 2. Section 3 describes the system model, while mentioning the assumptions. In Section 4, we formulate the game-theoretic method using the Single-Leader-Multiple-Follower Stackelberg game, and, thereafter, we establish the existence of Stackelberg equilibrium in Section 4.3. In Section 5, we also propose the different constituent algorithms of the scheme, TC-JAM, and discuss their performance in Section 6.4. Finally, we conclude the paper while citing few research directions in Section 7.

## 2. RELATED WORK

In the last few years, lot of research work on jamming in WSNs emerged, viz., [6–17]. Some of the existing literature are discussed in this section. Using Bayesian game, Garnaev *et al.* [17] studied jammer type identification to determine whether a jammer is a random jammer or an intelligent jammer. The authors formulated the problem as a dual linear programming problem. In this problem, the nodes identify the type of attack based on previous knowledge of jamming attack, and try to reduce the effect of jamming. Similarly, Xiao *et al.* [18] proposed an anti-jamming scheme, where the secondary users (SUs) try to estimate the transmitted jamming power. Thereafter, each SU decides the power required for transmission, while suppressing the jamming effect. For this problem, the authors used a Stackelberg game-theoretic approach. Sheikholeslami *et al.* [19] proposed an energy efficient routing scheme for wireless networks in the presence of jamming while calculating an approximation to the link outage probability. In another work, Hamouda *et al.* [20] proposed a new coalition game in presence of jammer, while considering that coalition value depends on the SUs' spectral efficiencies, the inter-SUs interference, and the interference caused to the primary user. Khan *et al.* [21] proposed a slotted based adaptive scheme for channel access in the presence of wireless nodes under unknown network conditions. On the other hand, Fang *et al.* [22] studied the effect of reactive jamming effect in wireless communication network. Viela *et al.* [23] studied the jamming strategies based on channel state information, and inferred that the effects of single jammer can be overcome, as there is a trade-off between jamming coverage and efficiency.

Noubir [24] proposed the varying of antenna gain to minimize jamming effects by minimizing the jamming-to-receiver-antenna gain factor. They also investigated the impact of the proposed method in multi-hop ad-hoc networks. They also explored the effects of the random-walk mobility model in a jamming environment. In another work, Li *et al.* [25] proposed an anti-jamming scheme, while using the incomplete information based game theory. Using game theory, they modeled strategies to assign random access to MAC layers. He *et al.* [26] considered the single and multi-commodity flow problems in the presence of mobile relays and single intelligent jammer. Considering that the other nodes, including the source and the destination nodes, are static, they tried to maximize the network flow, using spectral graph theory.

Amuru and Buehrer [27] proposed and characterized an optimal jamming scheme for optimal distribution of energy-constrained jamming signals over an additive white Gaussian noise channel. Baidas and Afghah [28] proposed a matching-theoretic approach to reduce bit error rate. They proposed that two paired node helps to minimize the total energy consumption, while ensuing end-to-end signal-to-noise ratio. Nguyen *et al.* [29] proposed strategies to transmit noise signals by a jammer to increase the privacy rate coefficient of the secondary users in the presence of multiple primary users in cognitive radio networks. Their focus was on increasing privacy, while introducing noise signal, and not of proposing a scheme for anti-jamming scheme. Li *et al.* [30] proposed an adaptive scheme to reduce the jamming effect, while adjusting the minimum contention window in the IEEE 802.11 MAC.

Tague [31] explored that mobility has impact on jamming attacks. They observed that different mobility factors can be used in order to get performance trade-offs. On the other hand, Wood *et al.* [32], Amiz *et al.* [33], Misra *et al.* [34] studied the problem of jamming area identification. Additionally, Li *et al.* [35], listed a survey of different anti-jamming schemes, while varying the transmission power. In another work, Xu *et al.* [36] proposed a scheme for switching in different available frequencies in order to avoid the jamming effects. Ma *et al.* [13] considered in their study a system comprising of mobile nodes and single static or mobile jammer. They proposed a random mobility model for the jamming affected nodes to be placed to a "safe" area. Mpitziopoulos *et al.* [37] proposed a jamming avoidance scheme, while considering mobile agents and tried to decide optimal trajectory for the mobile agent. However, these works do not consider the nodes to be static and the energy constraint of the nodes.

In contrast to the existing works, a game-theoretic model is used in this paper to improve the energy consumption of the network and the network lifetime in the presence of jamming nodes in

DOI: 10.1002/dac

WSNs, while taking advantage of varying transmission power levels. We use the Single-Leader-Multiple-Follower Stackelberg game to develop an topology control mechanism for WSNs.

## 3. SYSTEM MODEL

We assume a 2D WSN exposed to single or multiple jammers. We consider that the sink node is not affected by jamming. Each node $n \in \mathbb{N}$, where $\mathbb{N}$ is the set of sensor nodes in the network, is placed at location $(x_n, y_n)$, which is known to the sink node. However, the sink node does not know the location of the jammers. Each node $n$ has $|\mathbb{N}_n|$ number of neighbor nodes, where $\mathbb{N}_n \subseteq \mathbb{N}$, and communication range of $r_n$. The jammer can be either proactive or reactive. The schematic digram of the network is shown in Figure 1. Additionally, each node $n$ is considered to send its neighbor list to the sink, periodically, or in response to the query generated by the sink. Additionally, each node $n$ is capable of varying the transmission power level in order to ensure reduced energy consumption of the nodes, and increased in network lifetime. In WSNs, as the nodes are energy-constrained, and they lose its energy because of three different activities – sensing, transmission, and reception. In most of the WSNs, each node uses a sleep/wake schedule [38, 39]. Consequently, the nodes in jamming affected area lose its energy by receiving unrelated data. Therefore, we need to have a topology control mechanism, where each node chooses its optimum transmission power level. Let the maximum and the minimum transmission power levels of each node be denoted by $p_{max}$ and $p_{min}$, respectively. Each node needs to decide an optimum transmission power level, $p_n^*$, where $p_{min} \leq p_n^* \leq p_{max}$. If a node $n$ having transmission power level $p_n$ has a communication range of $r_n$, the mapping function between $r_n$ and $p_n$, i.e., $f : r_n \rightarrow p_n$, is one-to-one, as shown in Lemma 1.

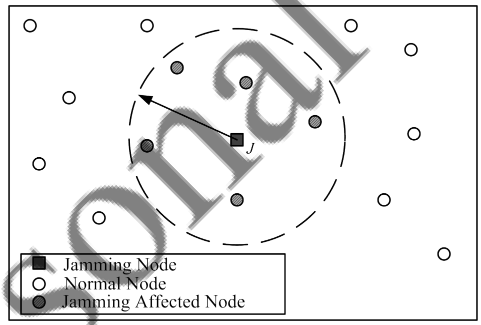

Figure 1. Schemtic Diagram of the Network in the Presence of Jammer

*Lemma 1*
Mapping function $f : r_n \rightarrow p_n$ is a bijective function.

*Proof*
In order to prove that $f : r_n \rightarrow p_n$ is a bijective function, we need to prove that $f : r_n \rightarrow p_n$ is both surjective and injective function. From the definition of a surjective function $g : x \rightarrow y$, we get that each element $y$ has a paired element $x$. For each value of transmission power level, $p_n$, we have a defined communication range $r_n$. Hence, we have a tuple or pair, i.e., $< r_n, p_n >$, for each value of $p_n$. Therefore, we conclude that $f : r_n \rightarrow p_n$ is a surjective function. Additionally, from the definition of an injective function $g : x \rightarrow y$, we get that for each $x$, there must be a distinct $y$ value. Each $r_n$ value corresponds to a distinct $p_n$ value. Therefore, we claim that $f : r_n \rightarrow p_n$ is an injective function. Finally, we conclude that $f : r_n \rightarrow p_n$ is a bijective function. □

Therefore, we define $k$ number of transmission power levels, i.e., $\mathbb{P} = \{\nu_1, \nu_2, \cdots, \nu_k\}$, where $\mathbb{P}$ is the set of transmission power levels having cardinality $k$. Accordingly, from Lemma 1, we get the set of communication ranges, i.e., $\mathbb{R} = \{\varphi_1, \varphi_2, \cdots, \varphi_k\}$. We represent the network to be a directed graph, $G = (V, E)$, where $V$ is the set of vertices, and $E$ is the set of edges.In the rest of the manuscript, we use $V$ and $\mathbb{N}$ analogously. We define that in graph $G$, there exits an edge from node $i$ to node $j$, i.e., $e_{ij}$, if the Euclidean distance between the nodes, $d(i, j)$, is lesser or equal to the communication range of node $i$, $r_i$. Mathematically,

$$e_{ij} = \begin{cases} 1, & \text{if } d(i,j) \leq r_i \text{ and } r_i \in \mathbb{R} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

### 3.1. Assumptions

In this section, we clearly define the bounds of the proposed scheme, TC-JAM, by outlining the assumptions below:

1. We consider a uniform random deployment of wireless nodes over a planer terrain.
2. We consider that the sink node is not affected by the jammers.
3. The sensor nodes are capable of varying the transmission power level, i.e., varying the communication range.
4. The jammers are reactive in nature, and are static.
5. The nodes are static and have a single channel to communicate.
6. Each node is capable of deciding its own strategy, i.e., its transmission power level or communication range.
7. The sender nodes always have packets to send.
8. We consider the network to be an ideal one, in which, there is no packet loss due to collision between two packets. Packets can be lost due to jamming only.

## 4. TC-JAM: THE PROPOSED TOPOLOGY CONTROL SCHEME

### 4.1. Justification of Using the Single-Leader-Multiple-Follower Stackelberg Game

In wireless sensor networks (WSNs), the nodes are energy constrained. On the other hand, the source nodes choose paths to the sink, in a distributed manner. Hence, if the intermediate nodes are in a jamming affected area, and the source nodes do not have any information about the jamming affected nodes, the nodes might deplete energy by sending multiple duplicate packets. In such a scenario, the nodes can choose a path consisting of unjammed nodes, while having information of the jammed nodes. In this process, the sink node helps the normal nodes, while identifying the presence of jammer. We propose a *topology control* scheme for increasing network lifetime in the presence of jammers, using the *single-leader-multiple-follower Stackelberg game* [40, 41], where the sink acts as an the leader, and the deployed sensor nodes act as the followers. This is represented as ‘oligopolistic market scenario’, where each individual, i.e., the leader and the followers, attempt to identify the jammers, and achieve high payoff.

### 4.2. Game Formulation

We consider a WSN exposed to multiple jammers. We use a *single-leader multiple-follower Stackelberg game-theoretic* approach for identifying the jamming affected nodes and decide the optimal strategies for *topology control* in the presence of jammers. The sink node acts as the leader, and the sensor nodes act as the followers. Additionally, we consider that the jammers are non-follower nodes, which affect the network performance, while deciding strategies locally. The sink, i.e., the leader, informs the follower nodes about the jamming affected nodes. On the other hand, the sensor nodes, i.e., the followers, decide the optimal transmission power and calculate the one-hop neighbor list. In this paper, the strategic form of the overall game is denoted as follows:

$$\zeta = \{\mathbb{N}, G, V, E, (p_n, r_n, \mathbb{N}_n, \mathbb{U}_n(\cdot))_{n \in \mathbb{N}}, \mathbb{S}(\cdot), \mathbb{L}(\cdot)\} \tag{2}$$

The components of the strategic form $\zeta$ are as follows:

i) $\mathbb{N}$ denotes the set of sensor nodes deployed in the wireless sensor network.

ii) $G = (V, E)$ represents the graph formed by the sensor nodes, where $V$ and $E$ denote the set of vertices and the set of edges, respectively, in the graph $G$.

iii) $p_n$ denotes the transmission power level chosen by sensor node $n$.

iv) $r_n$ is the chosen communication range by node $n$ corresponding to the transmission power level $p_n$.

v) $\mathbb{N}_n$ is the set of neighbor nodes of node $n$.

vi) $\mathbb{U}_n(p_n, \mathbb{N}_n)$ defines the utility function for each node $n$, and signifies the payoff, while choosing an optimal transmission power level, $p_n$ in order to increase the network lifetime.

vii) $\mathbb{S}(\mathbb{N}_n)$ defines the revenue of the network, and needs to be calculated by the sink node. The sink node always tries to cover at most many nodes, while reducing the energy loss due to packet loss and packet re-transmission.

viii) $\mathbb{L}(\mathbb{N}_J)$, which is to be calculated by the jammers, defines the loss incurred due to the effects of jammers over the jamming affected nodes.

*4.2.1. Utility Function for Each Sensor Node:* For each sensor node $n \in \mathbb{N}$, the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, signifies the maximization of payoff, locally, while ensuring the properties of the oligopolistic market. Each node $n$ needs to decide the optimum transmission power level, $p_n$, while considering that it can cover an optimum number of neighbor nodes. Additionally, if any neighbor node is affected by the jammers, eventually, no node would consider the affected node as a neighbor node. Hence, the network lifetime is increased. On the other hand, if node $i$ is affected by any jammer $j \in \mathbb{J}$, where $\mathbb{J}$ is the set of jammers present in the network, the node $i$, eventually, reduces it transmission power level to minimum value, i.e., $p_i = p_{min}$. Each node $n \in \mathbb{N}$ tries to maximize the payoff of the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$. Therefore, each node $n$ must satisfy the following properties:

1. The utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, is considered to be non-increasing, marginally, as with the increase in transmission power level, $p_n$, the energy consumption profile of node $n$ will increase. However, choosing the minimum transmission power level, $p_{min}$, reduces the payoff of the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, significantly. Hence, each node $n$ needs to decide an optimum transmission power level, while satisfying the following constraint:

$$\frac{\partial^2 \mathbb{U}_n(p_n, \mathbb{N}_n)}{\partial {p_n}^2} \leq 0 \tag{3}$$

2. With the increase in transmission power level, the cardinality of the set of neighbor nodes, i.e., $|\mathbb{N}_n|$, increases. Hence, each node has an increment in number of choice for choosing its next hop from the available neighbor nodes. For example, if a node $n$ chooses either of the available two transmission power level, i.e., $p_n$ and ${p_n}'$, where $p_n < {p_n}'$, the node $n$ covers $\mathbb{N}_n$ and $\mathbb{N}^{'}_n$ neighbors. Here, we claim that $\mathbb{N}_n \subseteq \mathbb{N}^{'}_n$. Hence, we get,

$$p^*_n = \begin{cases} p_n, & \text{if } \mathbb{N}_n \equiv \mathbb{N}^{'}_n \\ p^{'}_n, & otherwise \end{cases} \tag{4}$$

DOI: 10.1002/dac

Therefore, each node $n$ must consider the following condition:

$$\frac{\partial \mathbb{U}_n(p_n, \mathbb{N}_n)}{\partial p_n} \geq 0 \tag{5}$$

3. The payoff of the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, also increases with the increase in cardinality of the set of the neighbor nodes, i.e., $|\mathbb{N}_n|$. Mathematically,

$$\frac{\partial \mathbb{U}_n(p_n, \mathbb{N}_n)}{\partial |\mathbb{N}_n|} \geq 0 \tag{6}$$

4. The payoff of the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, also increases with the increase in cardinality of the set of the neighbor nodes of node $n$, i.e., $|\mathbb{N}_n|$ and the set of the neighbor nodes covered by other nodes $\tilde{n} \in \mathbb{N}$, where $n \neq \tilde{n}$. Hence, the payoff of the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, is expressed as follows:

$$\frac{\partial \mathbb{U}_n(p_n, \mathbb{N}_n)}{\partial |\bigcup_{n=1}^{\mathbb{N}} \mathbb{N}_n|} \geq 0 \tag{7}$$

Therefore, we define the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, as follows:

$$\mathbb{U}_n(p_n, \mathbb{N}_n) = \tan^{-1}\left(e^{\frac{p_n^{'} - p_n}{p_n^{'}}}\right) + \frac{1}{\mathbb{S}(\mathbb{N}_n)}\left[\frac{|\mathbb{N}_n^{'}| - |\mathbb{N}_n|}{(|\mathbb{N}_n|)_{max}}\right]\frac{p_n}{p_{max}} \tag{8}$$

where $p_n$ and $p_n^{'}$ denote the current and previous transmission power level, respectively, chosen by node $n$; $|\mathbb{N}_n^{'}|$, $|\mathbb{N}_n|$ and $(|\mathbb{N}_n|)_{max}$ are the number of neighbor nodes covered with transmission power levels – $p_n^{'}$, $p_n$, and $p_{max}$, respectively. Hence, each node $n$ tries to maximize its payoff, while satisfying following constraints:

$$p_{min} \leq p_n, p_n^{'} \leq p_{max} \tag{9}$$

$$\mathbb{N}_n, \mathbb{N}_n^{'} \subseteq \mathbb{N} \tag{10}$$

*4.2.2. Utility Function for the Sink Node:* Utility function for the sink node, $\mathbb{S}(\mathbb{N}_n)$, signifies the connectedness of the network. It symbolizes that the deployment topology of the network, and the presence of jammers. Here, the sink node collects the neighbor list information from the nodes deployed in the network. Here, the sink node calculates the set of the jamming affected nodes and informs the normal nodes to avoid those nodes, while deciding the paths. On the other hand, the jamming affected nodes does not get any information from the sink. Hence, it shrinks the transmission power level to the minimum value, i.e., the minimum transmission power level, $p_{min}$. Therefore, the sink node tries to maximize the payoff, while maximizing the number nodes covers by at least *one* neighbor node. Mathematically,

$$\frac{\partial \mathbb{S}(\mathbb{N}_n)}{\partial |\mathbb{N}_n|} \geq 0 \tag{11}$$

Therefore, we define the utility function, $\mathbb{S}(\mathbb{N}_n)$, as follows:

$$\mathbb{S}(\mathbb{N}_n) = \frac{|\bigcup_{n=1}^{\mathbb{N}} \mathbb{N}_n|}{|\mathbb{N}|} \tag{12}$$

where $\mathbb{N}_n$ is the set of neighbor nodes of node $n \in \mathcal{N}$; $|\cdot|$ defines the cardinality of a set. Hence, the sink node tries to maximize its payoff of the utility function, $\mathbb{S}(\mathbb{N}_n)$, while satisfying the constraint given below:

$$|\bigcup_{n=1}^{\mathbb{N}} \mathbb{N}_n| \leq |\mathbb{N}| \tag{13}$$

*4.2.3. Utility Function for Each Jammer:* Each jammer tries to maximize its payoff by blocking multiple nodes from communicating. Hence, each jammer tries to maximize the payoff of its utility function, $\mathbb{L}_J$. However, from network performance point, the sink node tries to reduce the payoff of the jammers, while suggesting the nodes to communicate through other paths. Hence, we can have the utility function for each jammer, $\mathbb{L}_J$ as follows:

$$\mathbb{L}_J = |\mathbb{N}_J| \tag{14}$$

where $\mathbb{N}_J$ defines the set of sensor nodes affected by the jammer $J$, and $|\cdot|$ defines the cardinality of the set, as mentioned earlier.

### *4.3. Existence of Generalized Stackelberg Equilibrium*

In this Section, we tried to establish that there exists an equilibrium called as the generalized Stackelberg equilibrium. Hence, we observe the first and second order derivatives of the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, in order to find out that the payoff can be maximized for optimum value of $p_n$. In Section 4.4, we get the actual solution of $p_n$. Additionally, we consider that the cardinality of the set of neighbor nodes of node $n$, i.e., $\mathbb{N}_n$, varies proportionally with the transmission power level, $p_n$. Mathematically,

$$\mathbb{N}_n = \alpha p_n \tag{15}$$

where $\alpha$ is a constant, as the nodes are considered to be distributed uniformly. Hence, performing first order partial derivation, we get,

$$\begin{aligned}\frac{\partial \mathbb{U}_n(p_n,\mathbb{N}_n)}{\partial p_n} &= \frac{e^{\frac{\Delta p_n}{p_n^{'}}}(-\frac{1}{p_n^{'}})}{1+e^{\frac{2\Delta p_n}{p_n^{'}}}} + \frac{\Delta p_n - p_n}{p_{max}^2}, \quad \text{where } \Delta p_n = p_n^{'} - p_n \\ &= -\frac{1}{p_n^{'}} \frac{1}{e^{\frac{\Delta p_n}{p_n^{'}}} + e^{-\frac{\Delta p_n}{p_n^{'}}}} + \frac{\Delta p_n - p_n}{p_{max}^2}\end{aligned} \tag{16}$$

However, we know that

$$\begin{aligned} e^x + e^{-x} &= (1 + x + \tfrac{1}{2}x^2 + \cdots) + (1 - x + \tfrac{1}{2}x^2 - \cdots) \\ &\approx 2 + x^2 \end{aligned} \tag{17}$$

Hence, from Equation (16), we get,

$$\begin{aligned}\frac{\partial \mathbb{U}_n(p_n,\mathbb{N}_n)}{\partial p_n} &= -\frac{1}{p_n^{'}} \left[\frac{1}{2+\left(\frac{\Delta p_n}{p_n^{'}}\right)^2}\right] + \frac{\Delta p_n - p_n}{p_{max}^2} \\ &= -\frac{1}{3p_n^{\prime} - 2p_n + \frac{p_n^2}{p_n^{'}}} + \frac{p_n^{'} - 2p_n}{p_{max}^2}\end{aligned} \tag{18}$$

Further, taking the second order derivative of $\mathbb{U}_n(\cdot)$, we get,

$$\begin{aligned}\frac{\partial^2 \mathbb{U}_n(p_n,\mathbb{N}_n)}{\partial {p_n}^2} &= \frac{1}{\left[3p_n^{\prime} - 2p_n + \frac{p_n^2}{p_n^{'}}\right]^2} \left[-2(1 + \frac{p_n}{p_n^{'}})\right] - \frac{2}{p_{max}^2} \\ &= -\frac{2}{p_n^{'}} \left[\frac{1}{2+\left(\frac{\Delta p_n}{p_n^{'}}\right)^2}\right] \left[1 + \frac{p_n}{p_n^{'}}\right] - \frac{2}{p_{max}^2}\end{aligned} \tag{19}$$

Here, we know that $p_n^{'} > 0$, $(\Delta p_n)^2 \geq 0$, and $\frac{p_n}{p_n^{'}} > 0$. Therefore, from Equation (19), we get,

$$\frac{\partial^2 \mathbb{U}_n(p_n, \mathbb{N}_n)}{\partial {p_n}^2} < 0 \tag{20}$$

Hence, we conclude that for the proposed scheme, TC-JAM, there exist a generalized Stackelberg equilibrium, i.e., an optimum value of $p_n$, for which the payoff of the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, is maximum. After getting that optimum value, i.e., $p_n^*$, each node does not change its strategy. Hence, we have a generalized Stackelberg equilibrium solution which can be expressed as tuple $< p_n^*, \mathbb{N}_n^* >$

### 4.4. *Solutions of the Proposed TC-JAM Scheme*

In this section, we discuss about the optimum strategy, i.e., the optimum transmission power, $p_n^*$, chosen by each node $n$. We equate the first order derivative of the utility function, $\mathbb{U}_n(p_n, \mathbb{N}_n)$, to zero. Mathematically,

$$\frac{\partial \mathbb{U}_n(p_n, \mathbb{N}_n)}{\partial p_n} = 0 \tag{21}$$

Therefore, from Equation (18), we get:

$$\begin{aligned} & -\frac{1}{3p_n^{'} - 2p_n + \frac{p_n^2}{p_n^{'}}} + \frac{p_n^{'} - 2p_n}{p_{max}^2} = 0 \\ \Rightarrow \quad & (p_n^{'} - 2p_n)\left(3p_n^{'} - 2p_n + \frac{p_n^2}{p_n^{'}}\right) - p_{max}^2 = 0 \\ \Rightarrow \quad & \frac{4}{p_n^{'}}{p_n}^3 - 6{p_n}^2 + 8p_n^{'}p_n + (p_{max}^2 - 3{p_n}^2) = 0 \end{aligned} \tag{22}$$

We consider that $a = \frac{4}{p_n^{'}}$, $b = -6$, $c = 8p_n^{'}$, and $d = (p_{max}^2 - 3{p_n}^2)$. Hence, from Equation (22), we get:

$$a{p_n}^3 - b{p_n}^2 + cp_n + d = 0 \tag{23}$$

Considering that $p_n = y - \frac{b}{3a}$, we rewrite the Equation (23) as follows:

$$\begin{aligned} & ay^3 + \left(c - \frac{b^2}{3a}\right)y + (d + \frac{2b^3}{27a^3} - \frac{bc}{3a}) = 0 \\ \Rightarrow \quad & y^3 + \left(\frac{3ac - b^2}{3a^2}\right)y + \frac{2b^3 - 9abc + 27a^2d}{27a^3} = 0 \end{aligned} \tag{24}$$

Hence, Equation (24), can be represented as follows:

$$y^3 + 3Qy - 2R = 0 \tag{25}$$

where $y = S + T$, $ST = -Q$. Therefore, we get:

$$\begin{aligned} & (S+T)^3 + 3Q(S+T) - 2R = 0 \\ \Rightarrow \quad & [S^3 + T^3 + 3ST(S+T)] - 3ST(S+T) - 2R = 0, \quad \text{as } Q = -ST \\ \Rightarrow \quad & S^3 + T^3 = 2R \\ \Rightarrow \quad & S^3 - \frac{Q^3}{s^3} - 2R = 0, \quad \text{as } T = -\frac{Q}{S} \\ \Rightarrow \quad & s^6 - 2RS^3 - Q^3 = 0 \end{aligned} \tag{26}$$

From Equation (26), we get:

$$\begin{aligned} & S^3 = \frac{2R \pm \sqrt{4R^2 + 4Q^3}}{2} \\ \Rightarrow \quad & S^3 = R \pm \sqrt{R^2 + Q^3} \\ \Rightarrow \quad & S = \sqrt[3]{R \pm \sqrt{R^2 + Q^3}} \end{aligned} \tag{27}$$

Considering that $S = \sqrt[3]{R + \sqrt{R^2 + Q^3}}$, from Equation (26), we get:

$$\begin{aligned} & S^3 + T^3 = 2R \\ \Rightarrow\ & T^3 = 2R - S^3 \\ \Rightarrow\ & T^3 = 2R - [R + \sqrt{R^2 + Q^3}] \\ \Rightarrow\ & T^3 = R - \sqrt{R^2 + Q^3}] \\ \Rightarrow\ & T = \sqrt[3]{R - \sqrt{R^2 + Q^3}} \end{aligned} \tag{28}$$

From Equations (27) and (28), we get:

$$y = \sqrt[3]{R + \sqrt{R^2 + Q^3}} + \sqrt[3]{R - \sqrt{R^2 + Q^3}} \tag{29}$$

and

$$p_n = \sqrt[3]{R + \sqrt{R^2 + Q^3}} + \sqrt[3]{R - \sqrt{R^2 + Q^3}} - \frac{b}{3a} \tag{30}$$

Hence, we get that the optimum transmission power level, $p_n^*$ is as follows:

$$p_n^* = \sqrt[3]{R + \sqrt{R^2 + Q^3}} + \sqrt[3]{R - \sqrt{R^2 + Q^3}} - \frac{b}{3a} \tag{31}$$

where $p_{min} \leq p_n^* \leq p_{max}$ and $|\mathbb{N}_n| = f(p_n^*)$. Here, $f(\cdot)$ defines a uniform distribution function.

Based on the set of neighbor nodes covered by each node, i.e., follower, the sink node, i.e., the leader calculates the payoff of the utility function, $\mathbb{S}(\mathbb{N}_n)$, as shown in Equation (12).

**Algorithm 1** Optimal Transmission Power Level Finding Algorithm

```
INPUTS:
  $G(V, E)$                                ▷ Graph of the network
  $\mathbb{N}$                              ▷ Set of deployed nodes
  $\mathbb{P}$                              ▷ Set of transmission power levels
  $p_{max}$                                 ▷ Maximum transmission power level
OUTPUT:
  $p_n^*$                                   ▷ Optimum transmission power level
  $\mathbb{N}_n^*$                          ▷ Optimum set of neighbor nodes
PROCEDURE:
  Calculate $(\mathbb{N}_n)_{max}$;         ▷ Set of neighbor nodes where $p_n = p_{max}$
  $p_n = p_{max}$;
  do
      $p_n^{'} = p_n$;
      Calculate $\mathbb{N}_n^{'}$;
      Choose $p_n$, where $p_n \neq p_n^{'}$ and $p_n \in \mathbb{P}$;
      Calculate $\mathbb{N}_n$;
  while $(\mathbb{U}_n\,(p_n, \mathbb{N}_n) \ngeq \mathbb{U}_n\left(p_n^{'}, \mathbb{N}_n^{'}\right)))$;
  $p_n^* = p_n$;
  $\mathbb{N}_n^* = \mathbb{N}_n$;
  return $(p_n^*, \mathbb{N}_n^*)$;
```

## 5. PROPOSED ALGORITHMS

In this section, we discuss the proposed algorithms elaborately. In TC-JAM, after the deployment over a terrain, each node needs to find its neighborhood graph, and accordingly needs to decide the optimum transmission power level. Thereafter, the sink node collects these neighborhood node information from each node, and finds the set of nodes under jamming affected area. Hence, we propose two algorithms, which are needed to be executed by each node and the sink in oder to decide the optimum transmission power level and the set of jamming affected nodes, respectively. In the proposed scheme, TC-JAM, the nodes, i.e., the followers, decide the transmission power level, non-cooperatively. Thus, their communication ranges are also defined non-cooperatively. Thereafter, the nodes inform the the set of neighbor nodes to the leader, i.e., the sink node. Based on that, the leaders calculates its payoff using utility function, $\mathbb{S}(\mathbb{N}_n)$, defined in Equation (11). These algorithms are as follows — optimal transmission power level finding and set of jamming affected nodes identification, i.e., Algorithms 1 and 2, respectively. Using Algorithm 1, each node tries to find the set of optimum neighbors, $\mathbb{N}_n \subseteq \mathbb{N}$. Before finding the optimum transmission power level, each node tries for $k$ times, where $k$ is a constant. Therefore, the time complexity of the Algorithm 1 is $O(k\mathbb{N}_n)$, i.e., $O(\mathbb{N})$. On the other hand, Algorithm 2 calculates the set of neighbor nodes coved by each individual node, which is having time complexity $\Theta(\mathbb{N})$. The calculation of remaining steps takes a constant time, i.e., $O(1)$. Hence, the time complexity of the Algorithm 2 is $\Theta(\mathbb{N})$.

**Algorithm 2** Set of Jamming Affected Nodes Algorithm

```
INPUTS:
  $G(V, E)$                          ▷ Graph of the network
  $\mathbb{N}$                       ▷ Set of deployed nodes
  $\mathbb{N}_n$                     ▷ Set of neighbor nodes of each node $n$
  $p_{max}$                          ▷ Maximum transmission power level
OUTPUT:
  $\mathbb{N}_J$                     ▷ Set of jamming affected nodes
PROCEDURE:
  Calculate $\bigcup \mathbb{N}_n$;  ▷ Set of connected nodes in the network
  Calculate $\mathbb{S}(\mathbb{N}_n)$;
  Calculate $\mathbb{N}_J = \mathbb{N} - (\bigcup \mathbb{N}_n)$;
  return $\mathbb{N}_J$;
```

## 6. PERFORMANCE EVALUATION

### 6.1. Simulation Parameters

For performance evaluation, we considered randomly generated values of the deployed nodes and jammers, as shown in Table I, on a MATLAB simulation platform. For simulation, both the sender and the destination nodes are selected randomly. The sensor nodes are homogeneous in nature, and capable of varying transmission power level. The initial setup of each sensor node is mentioned in Table I. Additionally, we assumed that the jammer starts to transmit random packets after the sender has successfully sent 10 packets, and the sender has a total 100 packets to send.

### 6.2. Benchmark

The performance of the proposed scheme, TC-JAM, is evaluated while comparing with two existing schemes – RPMSN05 [13] and CA-JAM [44].

We refer to these topology control schemes as TC-JAM, RPMSN05, CA-JAM through the rest of the paper. Ma *et al.* [13] considered mobile nodes and single static or mobile jammer. They proposed a jamming avoidance technique for the jamming affected nodes to the "safe" area. Jembre and Choi [44] proposed a jamming avoidance scheme, where each node has multiple interfaces at the same time, and can switch between multiple channels. However, unlike their work, we focused on designing a novel topology control scheme such that the network lifetime is increased, where nodes are having a single channel for communication without any complex hardware. Additionally, we have considered that the nodes are static in nature.

Table I. Simulation Parameters

| Parameter | Value |
|---|---|
| Simulation area | 1000 $m \times$ 1000 $m$ |
| Number of jammers | 4 |
| Number of normal nodes | 100-400 |
| Initial energy of each node | 20 $J$ [42] |
| Maximum communication range | 100 $m$ |
| Packet interval | 4 $sec$ |
| Packet Header size | 34 $bytes$ |
| Packet Payload size | 2034 $bytes$ |
| Energy consumption at Tx circuitry | 50 $nJ/bit$ [43] |
| Energy consumption at Rx circuitry | 50 $nJ/bit$ [43] |
| Energy consumption at amplifier | 100 $pJ/bit\text{-}m^2$ [43] |

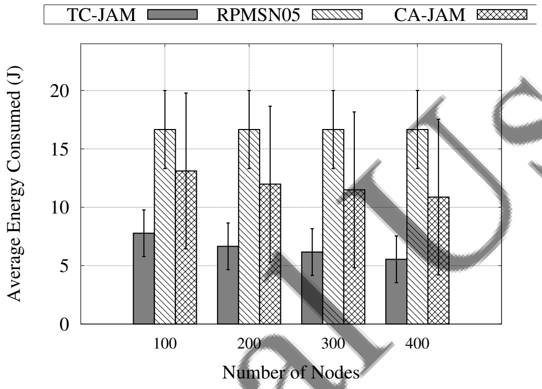

Figure 2. Average Energy Consumption of Each Node

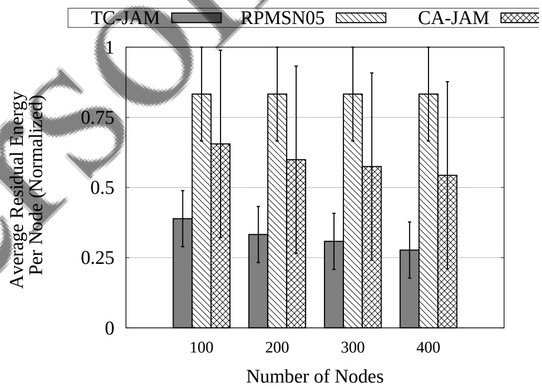

Figure 3. Average Residual Energy of Each Node

### 6.3. *Performance Metrics*

For performance evaluation, we have considered the following parameters:

- *Transmission power level and Communication Range*: We consider that the nodes can vary their transmission range. Hence, each node decides the transmission power level according to the deployment, i.e., based on the topology. Thereby, the network lifetime increases, while ensuring higher packet delivery ratio.

- *Energy Consumption*: We know that WSN is an energy-constrained network. Therefore, the reduction of energy consumption of the sensor nodes is one of the important issues. Each node consumes energy for activities such as sensing, message transmission, message receiving, and over-hearing. Using the sleep/wake schedule, each node reduces the energy consumption for over-hearing. However, energy consumption for message transmission and receiving can be reduced, while modifying the transmission range of the nodes, while ensuring connectivity of the network.
- *Network Lifetime*: The time duration between the network deployment and the time on which first node dies is defined as network lifetime. If the nodes are deployed at time instant $t_0$, and the first node dies in the network at time instant $t_d$, we define the network lifetime as follows:

$$\text{Network Lifetime} = t_d - t_0 \tag{32}$$

- *Packet Delivery*: In a communication network, we need to ensure higher packet delivery ratio ($PDR$). We define packet delivery ratio as a fraction of the number message delivered to the destination, and the total number of message sent.

$$PDR = \frac{\mathcal{P}_D}{\mathcal{P}_T} \tag{33}$$

where $\mathcal{P}_D$ and $\mathcal{P}_T$ define the number message delivered to the destination and the total number of message sent by the sender, respectively.

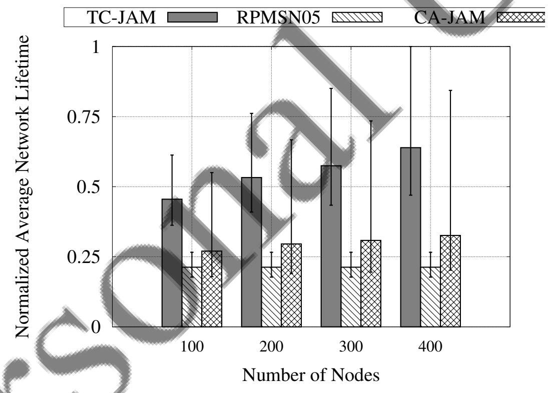

Figure 4. Normalized Average Lifetime of Each Network

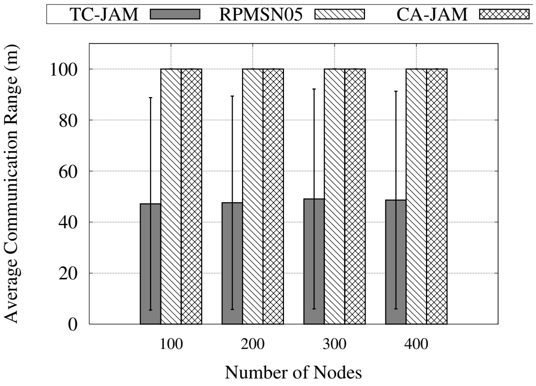

Figure 5. Average communication Range of Each Node

Copyright © 2016 John Wiley & Sons, Ltd.
*Prepared using* dacauth.cls

### 6.4. *Results and Discussions*

For the sake of simulation, we assume that each node sends a data packet at 4 seconds interval. Initially, for exploration, each node sends `Hello` packets to its neighbor nodes with maximum transmission power. After exploring the set of maximum number of neighbor nodes, each node optimizes the transmission power level and starts transmitting the `Data` packets. We consider that each node explores its neighbor nodes after an fixed interval of 5 $min$. Using the proposed scheme, TC-JAM, the average energy consumption of each node is reduced by 50-62% than using RPMSN05 and CA-JAM, as shown in Figure 2. The simulation results yield a higher variation in simulated result, as we considered that the nodes are deployed randomly. Here, we argue that using a dynamic topology control mechanism, i.e., the proposed scheme, TC-JAM, the energy consumption of the network is reduced. Additionally, from Figure 3, we get that the residual energy per node is higher using TC-JAM, than using RPMSN05 and CA-JAM.

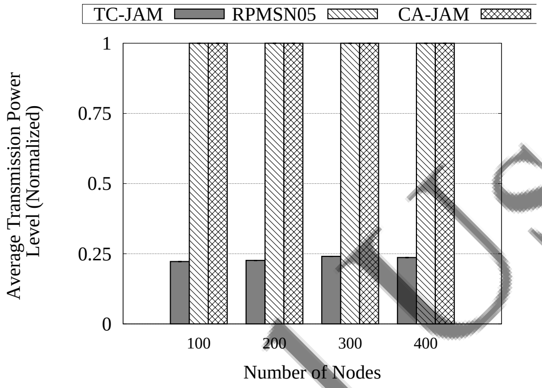

Figure 6. Average Transmission Power Level of Each Node

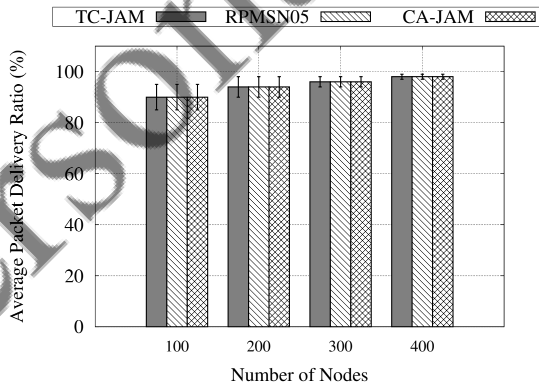

Figure 7. Average Packet Delivery Ratio of Each Node

Figure 4 shows that the network lifetime increases by 56-73% and 10-15% using TC-JAM, than using RPMSN05 and CA-JAM, respectively. Using TC-JAM, network lifetime increases due to less energy consumption due to transmission and reception of packets. Hence, Figure 4 reestablishes the fact claimed earlier.

Figure 5 shows that using TC-JAM, the average communication range of each node is reduced to a lesser value than the maximum communication range, i.e., 100 $m$. Additionally, Figure 6 depicts that the transmission power level is optimum using TC-JAM, than using RPMSN05 and CA-JAM. On the other hand, RPMSN05 and CA-JAM do not provide any topology control mechanism. Hence, using TC-JAM, each node reduces its energy consumption profile by reducing the transmission power level, which, eventually, helps in reduction communication range of the nodes. Additionally, TC-JAM ensures connectivity between the nodes and the sink in the network. From Figure 7, it is evident that using TC-JAM, the packet delivery ratio does not vary from using other approaches – RPMSN05 and CA-JAM. In addition to that, using TC-JAM, packet drop rate gets reduced than using RPMSN05 and CA-JAM, as shown in Figure 8. Hence, we conclude that using TC-JAM, we can improve energy consumption profile of the nodes in WSNs. Additionally, TC-JAM improves the network lifetime of WSNs, significantly, while ensuring reduced degradation in packet delivery ratio, as shown in Figures 4 and 7, respectively.

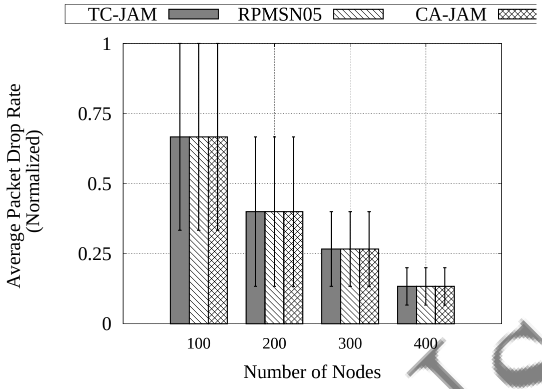

Figure 8. Average Packet Drop Rate

## 7. CONCLUSION

In this paper, we formulated a Single-Leader-Multiple-Follower Stackelberg game-theoretic approach to ensure less energy consumption and high network lifetime in the presence of jammers in WSNs. Based on proposed scheme, TC-JAM, we show how using the proposed topology control mechanism, each node chooses optimal transmission power level, while consuming less energy. Additionally, the network lifetime increases using TC-JAM. From simulated results, we get that the proposed scheme, TC-JAM, ensures at most 62% reduction in energy consumption that using existing techniques. Additionally, due to less energy consumption, the network lifetime increases by 56-73% than using existing schemes. TC-JAM scheme also ensures integrity of the packet delivery.

Future extension of this work includes understanding how packet delivery ratio can be increased in the presence of jammers. This work also can be extended, while considering the jammers are reactive in nature and each node has hardware configuration enabled with multiple communication channel. Additionally, we can extend this work to ensure QoS of the network, while considering the mobility for the nodes and the jammers.

## REFERENCES

1. Martins D, Guyennet H. Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey. *Proceedings of the 13$^{th}$ International Conference on Network-Based Information Systems*, 2010; 313–320.
2. Grover K, Lim A, Yang Q. Jamming and Anti-jamming Techniques in Wireless Networks: A Survey. *International Journal on Ad Hoc Ubiquitous Computing* December 2014; **17**(4):197–215.
3. Vadlamani S, Eksioglu B, Medal H, Nandi A. Jamming Attacks on Wireless Networks: A Taxonomic Survey. *International Journal of Production Economics* 2016; **172**:76–94.
4. Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G. A Survey on Jamming Attacks and Countermeasures in WSNs. *IEEE Communications Surveys Tutorials* Fourth Quarter 2009; **11**(4):42–56.
5. Falahati A, Sanandaji N. Nested and Interleaved Direct Sequence Spread Spectrum to Enhance CDMA Security and Bit Error Rate Performance. *International Journal of Communication Systems* 2016; **29**(12):1907–1915.
6. Bras L, Carvalho NB, Pinho P. Pentagonal Patch-Excited Sectorized Antenna for Localization Systems. *IEEE Transactions on Antennas and Propagation* March 2012; **60**(3):1634–1638.
7. Javed I, Loan A, Mahmood W. An Energy-Efficient Anti-Jam Cognitive System for Wireless OFDM Communication. *International Journal of Communication Systems* 2014; **27**(11):3460–3487.

DOI: 10.1002/dac

8. Weber SP, Yang X, Andrews JG, de Veciana G. Transmission Capacity of Wireless Ad-Hoc Networks with Outage Constraints. *IEEE Transactions on Information Theory* DecEMBER 2005; **51**(12):4091–4102.
9. Dhurandher SK, Misra S, Agrawal D, Rayankula A. Using Honeynodes along with Channel Surfing for Defense against Jamming Attacks in Wireless Networks. *The Third International Conference on Systems and Networks Communications*, 2008; 197–201.
10. Skiani ED, Mitilineos SA, Thomopoulos SA. A Study of the Performance of Wireless Sensor Networks Operating with Smart Antennas. *IEEE Antennas and Propagation Magazine* June 2012; **54**(3):50–67.
11. Khatua M, Misra S. CURD: Controllable Reactive Jamming Detection in Underwater Sensor Networks. *Pervasive and Mobile Computing* 2014; **13**:203–220.
12. Lall S, Maharaj B, van Vuuren PJ. Null-frequency Jamming of a Proactive Routing Protocol in Wireless Mesh Networks. *Journal of Network and Computer Applications* 2016; **61**:133–141.
13. Ma K, Zhang Y, Trappe W. Mobile Network Management and Robust Spatial Retreats Via Network Dynamics. *IEEE International Conference on Mobile Adhoc and Sensor Systems*, 2005; 1–8.
14. Ojha T, Misra S. MobiL: A 3-dimensional localization scheme for Mobile Underwater Sensor Networks. *National Conference on Communications*, 2013; 1–5.
15. Misra S, Dhurandher SK, Rayankula A, Agrawal D. Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks. *Computers & Electrical Engineering* 2010; **36**(2):367–382.
16. Zhang Z, Mukherjee A. Friendly channel-oblivious jamming with error amplification for wireless networks. *Proceedings of the $35^{th}$ Annual IEEE International Conference on Computer Communications*, 2016; 1–9.
17. Garnaev A, Liu Y, Trappe W. Anti-jamming Strategy Versus a Low-Power Jamming Attack When Intelligence of Adversarys Attack Type is Unknown. *IEEE Transactions on Signal and Information Processing over Networks* March 2016; **2**(1):49–56.
18. Xiao L, Chen T, Liu J, Dai H. Anti-Jamming Transmission Stackelberg Game With Observation Errors. *IEEE Communications Letters* June 2015; **19**(6):949–952.
19. Sheikholeslami A, Ghaderi M, Pishro-Nik H, Goeckel D. Energy-Efficient Routing in Wireless Networks in the Presence of Jamming. *IEEE Transactions on Wireless Communications* October 2016; **15**(10):6828–6842.
20. Hamouda S, El-Bessi S, Tabbane S. New Coalition Formation Game for Spectrum Sharing in Cognitive Radio Networks. *International Journal of Communication Systems* 2016; **29**(10):1605–1619.
21. Khan Z, Lehtomäki J, Vasilakos AV, MacKenzie AB, Juntti M. Adaptive Wireless Communications under Competition and Jamming in Energy Constrained Networks. *Wireless Networks* 2016; :1–21.
22. Fang S, Liu Y, Ning P. Wireless Communications under Broadband Reactive Jamming Attacks. *IEEE Transactions on Dependable and Secure Computing* May 2016; **13**(3):394–408.
23. Vilela JP, Bloch M, Barros J, McLaughlin SW. Wireless Secrecy Regions With Friendly Jamming. *IEEE Transactions on Information Forensics and Security* June 2011; **6**(2):256–266.
24. Noubir G. On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility. *Proceedings of the $2^{nd}$ International Conference Wired/Wireless Internet Communications*, Berlin, Heidelberg, 2004; 186–200.
25. Li G, He Z, Xing C, Chen C, Liao Q. QoS-Based Anti-Jamming Algorithm Design for Distributed Wireless Networks. *Proceedings of International Conference on Wireless Communications Signal Processing (WCSP)*, 2013; 1–5.
26. He X, Dai H, Ning P. Dynamic Adaptive Anti-Jamming via Controlled Mobility. *IEEE Transactions on Wireless Communications* August 2014; **13**(8):4374–4388.
27. Amuru S, Buehrer RM. Optimal Jamming Against Digital Modulation. *IEEE Transactions on Information Forensics and Security* October 2015; **10**(10):2212–2224.
28. Baidas MW, Afghah MM. Energy-Efficient Partner Selection in Cooperative Wireless Networks: A Matching-Theoretic Approach. *International Journal of Communication Systems* 2016; **29**(8):1451–1470.
29. Nguyen VD, Duong TQ, Dobre O, Shin OS. Joint Information and Jamming Beamforming for Secrecy Rate Maximization in Cognitive Radio Networks. *IEEE Transactions on Information Forensics and Security* 2016; DOI:10.1109/TIFS.2016.2594131.
30. Li Y, Wang C, Zhao W, You X. The Jamming Problem in IEEE 802.11-based Mobile Ad Hoc Networks with Hidden Terminals: Performance Analysis and Enhancement. *International Journal of Communication Systems* 2009; **22**(8):937–958.
31. Tague P. Improving Anti-Jamming Capability and Increasing Jamming Impact with Mobility Control. *Proceedings of IEEE $7^{th}$ International Conference on Mobile Adhoc and Sensor Systems*, 2010; 501–506.
32. Wood AD, Stankovic JA, Son SH. JAM: A Jammed-Area Mapping Service for Sensor Networks. *Proceedings of the $24^{th}$ IEEE Real-Time Systems Symposium*, 2003; 286–297.
33. Azim A, Mahiba S, Sabbir TAK, Ahmad S. Efficient Jammed Area Mapping in Wireless Sensor Networks. *IEEE Embedded Systems Letters* December 2014; **6**(4):93–96.
34. Misra S, Singh R, Mohan SVR. Geomorphic Zonalisation of Wireless Sensor Networks Based on Prevalent Jamming Effects. *IET Communications* August 2011; **5**(12):1732–1743.
35. Li M, Koutsopoulos I, Poovendran R. Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks. *IEEE Transactions on Mobile Computing* August 2010; **9**(8):1119–1133.
36. Xu W, Wood T, Trappe W, Zhang Y. Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service. *Proceedings of the $3^{rd}$ ACM Workshop on Wireless Security*, New York, NY, USA, 2004; 80–89.
37. Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G. JAID: An Algorithm for Data Fusion and Jamming Avoidance on Distributed Sensor Networks. *Pervasive and Mobile Computing* 2009; **5**(2):135 – 147.
38. Ye W, Heidemann J, Estrin D. An Energy-Efficient MAC Protocol for Wireless Sensor Networks. *Proceedings of IEEE INFOCOM 2002*, vol. 3, 2002; 1567–1576.
39. Ye W, Heidemann J, Estrin D. Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks. *IEEE/ACM Transactions on Networking* June 2004; **12**(3):493–506.

40. Hanif D Sherali FHM Allen L Soyster. Stackelberg-Nash-Cournot Equilibria: Characterizations and Computations. *Operations Research* 1983; **31**(2):253–276.
41. Misra S, Ojha T, Mondal A. Game-Theoretic Topology Controlfor Opportunistic Localization in Sparse Underwater Sensor Networks. *IEEE Transactions on Mobile Computing* May 2015; **14**(5):990–1003.
42. Misra S, Mali G, Mondal A. Distributed Topology Management for Wireless Multimedia Sensor Networks: Exploiting Connectivity and Cooperation. *International Journal of Communication Systems* 2015; **28**(7):1367–1386.
43. Heinzelman WR, Chandrakasan A, Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. *Proceedings of the 33$^{rd}$ Annual Hawaii International Conference on System Sciences*, 2000; 1–10.
44. Jembre YZ, Choi YJ. Beacon-based Channel Assignment and Jammer Mitigation for MANETs with Multiple Interfaces and Multiple Channels. *Computer Communications* March 2016; **78**(C):74–85.

DOI: 10.1002/dac