Computer Networks 128 (2017) 172–185

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Optimal decision rule-based ex-ante frequency hopping for jamming avoidance in wireless sensor networks

Prasenjit Bhavathankar[a], Subhadeep Sarkar[b,1], Sudip Misra[a,2,*]

[a] Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, West Bengal - 721302, India
[b] School of Medical Science and Technology, Indian Institute of Technology Kharagpur, West Bengal - 721302, India

ARTICLE INFO

Article history:
Received 29 June 2016
Revised 28 November 2016
Accepted 10 March 2017
Available online 24 April 2017

Keywords:
Wireless sensor networks (WSNs)
Jamming avoidance
Frequency hopping
Optimal decision rule

ABSTRACT

In this paper, we consider a static wireless sensor network (WSN) affected by a constant, static jammer. Both the nodes in the network and the jammer are capable of switching frequencies. Existing literature mostly thrive on mechanisms with a mutually pre-decided hopping-sequence or on random frequency-hopping techniques. However, these mechanisms often fall short in the context of energy-constrained WSNs. We propose a frequency-hopping strategy based on the optimal decision rule. The proposed solution takes into account the individual decision profiles of all the concerned nodes, and finally, makes the decision for the welfare of the overall network. The objective is to find an optimal frequency hopping rule to obtain the maximum throughput. We observe that the packet delivery ratio of the network improves by approximately 30% after the application of the optimal decision rule for frequency-hopping. The overall network energy consumption is also improved by approximately 53% by the application of the proposed solution approach, as observed from the results.

1. Introduction

Jamming in wireless sensor networks (WSNs) disrupts the communication between the sensor nodes and affects the network severely in terms of energy drainage. A jammer transmits a high power signal, which corrupts the ongoing data transmissions in the network, resulting in packet drops. This causes the nodes to retransmit the data packets repeatedly, thereby inflicting huge energy wastage. Also, a constant jammer keeps the channel busy continuously, so that no other node gets access to the channel [1–3]. Although there are numerous techniques to avoid jamming [4–12], few are applicable in the context of WSNs [13–18]. We discuss the different state-of-the-art jamming avoidance mechanisms and examine their applicability in the reference of WSNs. One of the popular techniques to avoid the effects of jamming is through regulating the transmission power. However, transmitting in a low-power mode is strictly hardware-dependent and low-power transmission implies a decrease in the communication range of the sensor node as well. An alternative way of avoiding the jammer's influence is antenna polarization which thrives on the principle of the line of sight (LoS) communication. The left circular polarization will not receive the signal of right circular polarization. Therefore, the nodes in the network change the polarization to avoid the jamming effect. The important point is that the nodes should be informed about the change in the polarization. This technique, however, is also reliant on the sensor-hardware and is costly. Moreover, not many sensor nodes are equipped with this technology. Directional transmission is another jamming avoidance mechanism, in which the antenna transmits or receives the signals in a particular direction only, and thus, avoids the jamming by changing the direction of the antenna. The main problem with this method is that multipath routing becomes difficult [19], as in WSNs, one node usually communicates with multiple other nodes. Considering the limited energy resources of a sensor node, communication using ultra wide band (UWB) technology, in order to bypass the jammer's effect, may not always be suitable for WSNs.

Frequency hopping spread spectrum (FHSS) is another effective mechanism for jamming avoidance. In this method the nodes are allowed to switch among different frequencies within the channel [20–24]. FHSS minimizes unauthorized communication interceptions and interference while supporting co-existence of multiple WSNs in the same region. It also efficiently mitigates the adverse effects of multipath fading for multi-hop communications in WSNs. Clearly, FHSS is the most suitable jamming avoidance technique for WSNs as it is energy-friendly and requires minimal hardware-

* Corresponding author.
E-mail addresses: pbbhavathankar@gmail.com (P. Bhavathankar), subhadeep@smst.iitkgp.ernet.in (S. Sarkar), smisra@sit.iitkgp.ernet.in, sudip_misra@yahoo.com (S. Misra).

[1] Student Member, IEEE.
[2] Senior Member, IEEE.

http://dx.doi.org/10.1016/j.comnet.2017.03.009
1389-1286/© 2017 Published by Elsevier B.V.

support. However, traditional FHSS algorithms are either periodic in nature or event-driven, which makes them vulnerable to advanced jamming strategies. Moreover, FHSS-based solutions often fall short in scenarios where the jammer is also capable for hopping between frequencies and strategically block ongoing communications in the network.

1.1. Motivation

Although frequency-hopping provides an efficient solution to jamming avoidance in most cases, it falls short if the jammer is intelligent and advanced enough to update its jamming strategy. In existing periodic FHSS-based solutions, the nodes in the network switch their operating frequencies periodically after a certain time-interval irrespective of the network-state. In presence of a jammer in the network, this may lead to unnecessary packet drops as a node may, by its routine, switch to the jammer's operating frequency. On the other hand, in event-driven FHSS-based solution techniques, a node switches its frequency only after it is affected adversely due to some undesired phenomenon, i.e., a node switches to an alternate frequency only if it is affected by the jammer for a certain duration. In this case, however, if the jammer is also capable of switching frequencies and is intelligent enough to ascertain the frequency in which communication is presently ongoing, then it will rapidly switch to the desired frequency affecting the network throughput. Existing FHSS-based solutions [20–22], therefore, fail to provide an optimal solution to the problem of jamming in cases where the jammer is also capable of frequency-hopping.

In this paper, we use an optimal decision rule to analyze the network's condition periodically and act in a way to maximize the benefit of the network as a whole. The proposed frequency-hopping mechanism is event-driven and stochastic in nature. We have considered a sensor network with static deployment of the sensor nodes and a constant static jammer, which however, is capable of switching between frequencies. Our discussion, however, is limited to the situation in which both the sensor nodes and the jammer are capable of switching between two operating frequencies only. We consider that the nodes, as well as the jammer may communicate in either of the two different frequencies, viz., f_α and f_β. In this work we consider the problem of taking the decision on whether to switch between the frequencies or not, for the nodes in the network while we envision to maximize the throughput of the network. Note that, at any point of time, any node in the network may operate in either f_α or f_β. An aggregator node, chosen dynamically in each iteration, executes the optimal decision rule based on the mean packet drop rate of the nodes in the network and optimizes the payoff of the whole WSN.

1.2. Contribution

The main contributions of our work are as follows.

- Each node in the network makes its own decision independently on whether to switch its present operating frequency or not. Based on this, the aggregator node finally outputs the decision which is best-fit for the network, using the optimal decision rule. The decision, therefore, is collaborative and maximizes the payoff for the society.
- An optimal decision rule is used to stochastically model the jammer's behavior, and thus, reform the network topology accordingly. Our work addresses the problem of jamming avoidance in WSNs in critical scenarios when the jammer is capable of switching frequencies as well.
- The performance of the system is evaluated in terms of throughput of the network and energy consumption. A thorough analysis of the energy consumption of the nodes in the network against variable frame size and with time projects the applicability and utility of the optimal decision rule in the context of frequency-hopping in an elaborated manner.

Note that, the decision is taken based on the overall network condition directing towards a globally optimal solution, rather than a locality-specific temporal solution.

1.3. Paper organization

The rest of the manuscript is organized in the following sections. In Section 2, we discuss the existing literature on jamming avoidance techniques primarily focusing on the different frequency-hopping mechanisms. The problem statement is mathematically formulated in Section 3. We propose an optimal decision rule-based solution to the problem of jamming avoidance in Section 4. The performance of the proposed solution is analyzed thoroughly in Section 5. Finally, in Section 6, we conclude our discussion and explore the future research scope in this domain.

2. Related work

In this paper, we address the problem of jamming avoidance in WSNs by frequency hopping using the optimal decision rule. We discuss some of the relevant literature in this section.

Quan et al. [25] have proposed a multi-pattern frequency hopping method to mitigate the effects of jamming. There are two channels, viz. the data channel and the complementary channel which have their own frequency hopping patterns. It uses convolution encoding and maximum likelihood decoding to improve the method of anti jamming. However, the synchronization of the different frequency patterns takes a prolonged time. A jamming resistance broadcast technique was discussed for both single-hop and multi-hop communication networks by Xiao et al. in [26,27]. Wang et al. [28] have formulated an anti-jamming strategy based on uncoordinated frequency hopping (UFH) communication in which the sender and the receiver hop to random frequencies in order to avoid jamming attacks. The nodes are able to communicate with each other only when they are operating on the same frequency [29,30]. The authors have formulated this problem as a non-stochastic multi-armed bandit problem and the proposed solution is based on an online optimization theory with frequency hopping strategy. However, the nodes jump randomly to different frequencies based on the UFH, and communication between a pair of nodes may only resume if they hop on to the same frequency. In our work, the centralized aggregator node takes the decision for the society based on the optimal decision rule and broadcasts the same to all the nodes in the network.

Zhang et al. [22] have proposed another anti-jamming technique which is based on message-driven frequency hopping. In this method the transmitter transmits a secure ID-sequence alongside the data which acts as a pseudo-noise sequence for selecting the frequency at the transmitter. The secure-ID sequence is shared between the sender-receiver pair, and the receiver extracts the ID-sequence and to the information regarding the frequency-hopping. However, this mechanism is ineffective if the message bearing the ID-sequence is dropped itself due to the jammers influence. Achutan and Kishore [21] have developed a security based architecture which generates the hopping sequence. This generator-unit is embedded within the sensor nodes and the unit executes the channel selection for all nodes of a route after the detection of jamming. However, nodes under the influence of the jammer may not be able to communicate with the other nodes in the route, and thus, may fail to coordinate with them. Also, the computations involved within each sensor node in order to generate the frequency sequence consumes more power. In contrast, in our proposed solution, the network topology is reformed based on the outcome of the optimal decision rule and nodes which are affected by the jammer are avoided in the process. Also, computationally, each node in the network performs preliminary mathematical operations and sends only a single frame to the centralized node suggesting their individual preference profile. In [31], the authors have proposed an anti-jamming technique for unicast communication. They have used the Steiner triple system and transversal design for channel selection. However, in case of WSNs it is barely applicable as nodes in a WSN usually broadcast their messages in the medium.

Chang et al. [20] have proposed an algorithm for the symmetric-role uncoordinated frequency-hopping in asynchronous environment in order to prevent jamming. In this case it is not required to assign the role of sender and receiver in advance before frequency hopping. Liu et al. have proposed a method which helps in communication between nodes in presence of the jammer in WSNs. It uses the uncoordinated seed disclosure technique in frequency hopping for establishing the shared secret key between the transmitter and receiver. However, the work thrives on a big assumption that the sender and the receiver nodes must be on the same frequency at the time of the seed disclosure and the jammer should not listen on the same channel. Alagil et al. [32] have considered the randomized positioning direct sequence spread spectrum scheme as a countermeasure for jamming attack. The index codes for each message is placed at random position. The receiver finds the position of the code in the payload of a new message and encode the message. In this process the authors have removed the requirement of shared key.

Li et al. [33] have considered a WSN in which a jammer communicates over a single channel. The channel is sensed to detect collision and if a collision is detected, a jamming message is broadcast to all the nodes of the network. In this work, the authors have considered two cases. In the first case, they consider that the network has a prior knowledge of the strategy of the jammer and the instants of jamming and the jammer is also aware of the policies undertaken by the network when jamming occurs. In the other case, neither the jammer nor the network have the complete information about the decision of the other. The authors formulated this scenario as an optimization problem. The payoff considered in this work is based on the channel access, and the occurrence of collision in presence and absence of the jammer. However, the work does not consider packet dropping and the overall reduction of the network throughput due to jamming.

Zhang et al. [34] have focused on the jamming tolerance of the network that is the maximum number of jammers that can be placed among the finite number of nodes to achieve the reliability. Similarly, Rouissi et al. [35] have combined the direct sequence spread spectrum, frequency hopping spread spectrum and time hopping spread spectrum techniques to avoid the effect of jamming and secure the wireless sensor network from the jamming attack.

Du and Roussos [36] have focused on the problem of interference when multiple networks are co-located over the same region. In such a scenario, the authors have proposed an adaptive slotted channel hopping technique which is the enhanced version of time slotted channel hopping. In this technique, the frequency which creates the maximum interference is avoided and omission of high interference channel improves the packet delivery ratio [37–39]. Shih et al. [40] have designed a new algorithm for generating the frequency hopping sequence by removing those channels which has maximum interference. In the proposed solution approach, however, we encounter the individual decision-profiles of all the nodes in the network and holistically decide on the jamming avoidance strategy using an optimal decision rule.

3. Problem definition

In this section, we define the problem scenario and mathematically model the problem. However, it is important to define the bounds of the problems clearly by mentioning the assumptions of the work.

3.1. Assumptions

a) We consider a static and uniform random deployment of wireless sensor nodes across a planer terrain and the nodes, deployed, are static in nature.
b) The jammer, $\mathcal{J}$, is also static in nature and the location of the jammer within the terrain, $(x_{\mathcal{J}}, y_{\mathcal{J}})$ is known *a priori*.
c) A node is only allowed to toggle between frequencies, i.e., the entire bandwidth available to a node for transmission is divided into two frequency bands, viz., f_α and f_β. The jammer is also capable of switching between f_α and f_β with a view to affect the network communication maximally.
d) Each node is capable of making its own decision on whether to toggle between the frequencies or not.

3.2. System model

We consider a system with n nodes, given by $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ distributed uniform-randomly over a planer terrain. The network topology, thus formed, can be translated into a graph, G. Let $\mathcal{V}^\alpha(t)$ and $\mathcal{V}^\beta(t)$ denote the sets of nodes operating in the frequency band f_α and f_β, respectively, at time t with $|\mathcal{V}^\alpha(t)| = n_\alpha(t)$ and $|\mathcal{V}^\beta(t)| = n_\beta(t)$. Clearly, at any given time instant t, $\mathcal{V}^\alpha(t) \cup \mathcal{V}^\beta(t) = \mathcal{V}$ and $n_\alpha(t) + n_\beta(t) = n$. Let $G^\alpha(t)$ and $G^\beta(t)$ be the (sub)graphs constructed at time instant t, using the vertices in $\mathcal{V}^\alpha(t)$ and $\mathcal{V}^\beta(t)$, respectively. Evidently, at any time instant t, $G^\alpha(t)$, $G^\beta(t) \subseteq G$.

Let $\mathcal{E}^\alpha(t)$ and $\mathcal{E}^\beta(t)$ be the adjacency matrices (of dimensions $n_\alpha(t) \times n_\alpha(t)$ and $n_\beta(t) \times n_\beta(t)$, respectively), at time t, corresponding to the graph set of all edges present in the graphs $G^\alpha(t)$ and $G^\beta(t)$, respectively. Mathematically, the elements of the matrix $\mathcal{E}^\alpha(t)$, denoted by $e^\alpha_{i,j}(t)$, $\forall i, j \in (1, n_\alpha)$ is expressed as:

$$e^\alpha_{i,j}(t) = \begin{cases} 1, & \text{if there exists an edge from } v_i \text{ to } v_j \text{ in } \mathcal{V}^\alpha(t) \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

Similarly, we also have the matrix $\mathcal{E}^\beta(t)$ representing the adjacency matrix corresponding to the graph $G^\beta(t)$. The justification behind considering the graph to be directed is that, at any given time instant t, while a node v_i may be able to receive a packet from its neighboring node v_j, v_i may not be able to transmit a packet to v_j due to inadequate energy. Therefore, existence of $e^x_{i,j}(t)$ does not confirm the existence of $e^x_{j,i}(t)$, $\forall i, j \in (1, n_x)$, $x \in \{\alpha, \beta\}$. Also, to avoid redundancy in subsequent computations, we eliminate all self-looping edges from the graph, i.e., $e^x_{i,j} = 0 \ \forall i, j \in (1, n_x); i = j; x \in \{\alpha, \beta\}$. Having defined the graph and the corresponding adjacency matrices, we now define a route in the network.

Definition 1. A *route, R*, in the network is defined as an ordered sequence of k vertices $(v_{s_1}, v_{s_2}, \ldots, v_{s_k})$ where v_{s_1} and v_{s_k} are the source and destination vertices of the route, respectively. For a pair of vertices $(v_{s_i}, v_{s_{i+1}})$, $1 \le i \le k-1$, there exists an edge $e^x_{i,i+1}$, $x \in \{\alpha, \beta\}$.

Any node v_i, $i \in (1, n)$ is capable of toggling between frequencies f_α and f_β as it uses frequency hopping as an anti-jamming measure. While the goal of the jammer is to reduce the throughput of the network by affecting as many nodes and the corresponding communication links, the nodes tend to switch frequencies intelligently to avoid the adverse effects of jamming. It is worthy of mentioning that in the absence of a jammer, all nodes communicate using the same frequency band, i.e., either of f_α and f_β. Clearly, under such circumstances, either (a) $\mathcal{V}^\alpha(t) = \mathcal{V}$; $\mathcal{V}^\beta(t) = \Phi$; $\mathcal{E}^\beta(t) = 0_{n_\beta(t)\times n_\beta(t)}$ and $G^\alpha(t) = G$, or (b) $\mathcal{V}^\beta(t) = \mathcal{V}$; $\mathcal{V}^\alpha(t) = \Phi$; $\mathcal{E}^\alpha(t) = 0_{n_\alpha(t)\times n_\alpha(t)}$ and $G^\beta(t) = G$, where $0_{n\times n}$ represents a zero matrix of order $n \times n$. In presence of a jammer, however, a number of nodes and corresponding links are affected, and nodes switch frequencies to avoid the influence of the jammer. However, it should be noted that for any given time instant t, $G^\alpha(t) \cup G^\beta(t) \neq G$. Although for every t, $\mathcal{V}^\alpha(t) \cup \mathcal{V}^\beta(t) = \mathcal{V}$, the other necessary condition for graph union strictly does not hold true, i.e., $\sum_{i=1}^{n_\alpha}\sum_{j=1}^{n_\alpha} e^\alpha_{i,j}(t) + \sum_{i=1}^{n_\beta}\sum_{j=1}^{n_\beta} e^\beta_{i,j}(t) < \sum_i^n \sum_j^n e_{i,j}$, where $\sum_{i=1}^{n}\sum_{j=1}^{n} e_{i,j}$ is the total number of edges in graph G.

3.3. Problem statement

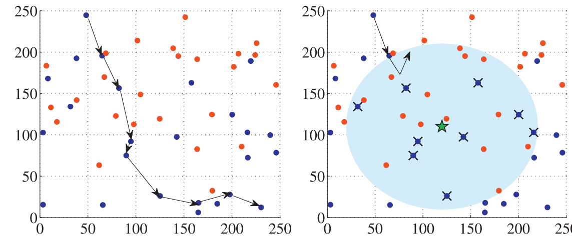
In this work, we consider a static WSN subjected to the influence of a constant, high-power, static jammer, the position of which $(x_\mathcal{J}, y_\mathcal{J})$ is known. Both the jammer and the nodes present in the WSN are capable of switching between frequencies f_α and f_β. Given the traffic flow pattern in the neighborhood of $(x_\mathcal{J}, y_\mathcal{J})$ at time t, the problem is to determine the optimal frequency hopping rule which would maximize the overall network throughput by minimizing the packet drop rate of individual links. Therefore, at any time instant t, our goal is to ascertain the magnitude of $\bar{\Gamma}(t)$, where $\bar{\Gamma}(t)$ is the minimal mean packet drop rate of the overall network. Mathematically,

$$\bar{\Gamma}(t) = \min\left[\sum_{i=1}^{n_\alpha(t)}\sum_{j=1}^{n_\alpha(t)} e^\alpha_{i,j}(t)\rho^\alpha_{i,j}(t) + \sum_{k=1}^{n_\beta(t)}\sum_{l=1}^{n_\beta(t)} e^\beta_{k,l}(t)\rho^\beta_{k,l}(t)\right] \tag{2}$$

where $\rho^\alpha_{i,j}(t)$ and $\rho^\beta_{k,l}(t)$ denote the mean packet drop rates, at time t, across the links $e^\alpha_{i,j}(t)$ and $e^\beta_{k,l}(t)$, $\forall i, j \in (1, n_\alpha(t))$; $\forall k, l \in (1, n_\beta(t))$ of the graphs $G^\alpha(t)$ and $G^\beta(t)$, respectively. The product terms $e^\alpha_{i,j}(t)\rho^\alpha_{i,j}(t)$ and $e^\beta_{k,l}(t)\rho^\beta_{k,l}(t)$ eliminates redundancy in computation, as it eliminates the additive components for the edges which do not exist in the network. Clearly, minimizing the mean packet drop rate of the overall network, requires optimal hopping between frequencies to minimize the effects of jamming. In the following Section, we design the optimal group decision rule which effectively diminishes the packet drop rate of the network maximally by using the preference profiles of the unaffected nodes.

3.4. Case study - problem scenario

In this Section, we provide an example case study on the jammer's effect on the ongoing communications in the network. An extension of this case study, where the solution to the problem is highlighted, is presented in Section 4.3. In Fig. 1, we elaborate the problem and discuss on the proposed solution approach using the optimal decision rule. Fig. 1(a) highlights a planar terrain of dimensions 250 m × 250 m with 50 nodes distributed uniform-randomly across it. The nodes are either operating in frequency f_α (denoted by *blue* color) or in the f_β frequency (denoted by *red* color). We concentrate on the sample case of one particular route in the network and elaborate the operation of the optimal decision algorithm. Initially, when the jammer is not present in the network, the nodes in the sample route are assumed to operate in frequency f_α and the flow of data packet along the route R is shown by the black arrowheads.



(a) Absence of jammer (b) Jammer operating in f_α frequency

Fig. 1. Communication disruption in presence of jammer.

Fig. 1(b) depicts the state of the network under the influence of the jammer $\mathcal{J}$, positioned at $(x_\mathcal{J}, y_\mathcal{J}) = (120, 110)$ and operating in the f_α frequency. It is to be noted that the nodes within the communication range of $\mathcal{J}$ and operating in f_α become non-functional at this point and are marked by a cross. Communication along the route R, at this point of time, is disrupted and the route packet delivery ratio as well as the packet delivery ratio of the overall network drops down consequently. Under such a situation, the goal of our work is to decide optimally on whether to switch their operating frequency of the nodes to f_β or to continue operating in f_α. The solution to this problem, as achieved through the application of an optimal decision rule, is presented in the following section.

4. Proposed solution

We use the optimal group decision rule as the framework to solve the aforementioned problem. Motivated by the work of Ben-Yashar and Nitzan [41,42], we choose the generalized 'pair-wise choice' scheme as the basis of determination of the corresponding optimal decision rule. The justification behind choosing the optimal group decision rule to build the solution strategy is that our system model allows all the four possible pair-wise choices and the payoffs corresponding to each pair determines the overall welfare of the society. The optimal group decision rule gives the global optimal solution based on the individual decision profile of the nodes which takes part in the decision making.

While the location of jammer, $\mathcal{J}$, is considered to be fixed at $(x_\mathcal{J}, y_\mathcal{J})$, location of any node v_i is given by (x_{v_i}, y_{v_i}), $\forall v_i \in \mathcal{V}$. We describe the term *eligibility factor*, and hence, define the principles used to form a *society*.

Definition 2. The *eligibility factor* (ϑ_{v_i}) of a node, v_i, determines whether a node is eligible to be a member of the decision making group, and ϑ_{v_i}, $\forall v_i \in \mathcal{V}$, is mathematically classified as:

$$\vartheta_{v_i} = \begin{cases} 1, & \text{if } \delta_{v_i,\mathcal{J}} \le \delta_{th} \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

where $\delta_{v_i,\mathcal{J}}$ is the distance between node v_i and the jammer, $\mathcal{J}$ and is computed as:

$$\delta_{v_i,\mathcal{J}} = \left| \left[(x_{v_i} - x_\mathcal{J})^2 + (y_{v_i} - y_\mathcal{J})^2 \right]^{1/2} \right| \tag{4}$$

and δ_{th} is a predefined threshold distance determined based on the communication range of $\mathcal{J}$, $r(\mathcal{J})$, and is taken considerably larger than $r(\mathcal{J})$.

Definition 3. A *society*, $\mathcal{S}(t)$, formed at time t, is defined as a collection of nodes which are not under the influence of the jammer at that time instant and for which $\vartheta_* = 1$. $\mathcal{S}(t)$ is mathematically defined as:

$$\mathcal{S}(t) = \Big\{\hat{v}_i : \hat{v}_i \in \mathcal{V}; \mathcal{F}_{\hat{v}_i}(t) \neq \mathcal{F}_{\mathcal{J}}(t); \vartheta_{\hat{v}_i} = 1; \delta_{\hat{v}_i,\mathcal{J}} \leq r(\mathcal{J}) \text{ or } \hat{v}_i \in \mathcal{V}; \vartheta_{\hat{v}_i} = 1; \delta_{\hat{v}_i,\mathcal{J}} > r(\mathcal{J})\Big\}, \forall \hat{v}_i \in \mathcal{V} \quad (5)$$

where $\mathcal{F}(\hat{v}_i)$ and $\mathcal{F}(\mathcal{J})$ denote the operating frequencies of node $\hat{v}_i$ and jammer $\mathcal{J}$, respectively. Also $\forall t$, $\mathcal{S}(t) \subseteq \mathcal{V}$.

We assume that all the members of the society $\mathcal{S}(t)$ have the capability of making decisions on whether to switch frequency based on its packet drop rate and distinguish between a potentially correct and incorrect decision. However, the members are fallible to optimal decision making, and hence, the importance of group decision making remains persistent.

4.1. Generalized pair-wise choice framework

Let us assume that at time t, the number of members present in the society $\mathcal{S}(t)$ is denoted by $\hat{n}(t)$ such that $\hat{n}(t) = |\mathcal{S}(t)|$. Each member is capable of estimating, based on its mean packet delivery rate, the existence of a jammer along a particular route and make decision on whether to switch frequency or not. Therefore, the two potential factors driving node $\hat{v}_i$'s decisions are:

(i) $E(J_{\hat{v}_i}) = \{+1, -1\}$: Whether the medium is jammed $(+1)$ or not (-1).
(ii) $E(T_{\hat{v}_i}) = \{+1, -1\}$: Whether to switch (toggle) frequency $(+1)$ or not (-1).

Based on these two factors a node makes its individual decision which, however, is fallible with certain probability. Let, $\mathbb{P}^+_{\hat{v}_i}$ and $\mathbb{P}^-_{\hat{v}_i}$ be the probabilities with which a member node $\hat{v}_i$ $(\forall \hat{v}_i \in \mathcal{S}(t))$ switched frequency in presence of a jammer and operates in the current frequency if it is unaffected by the jammer, respectively. Therefore, mathematically,

$$\mathbb{P}^+_{\hat{v}_i} = P(E(J_{\hat{v}_i}) = +1)\Big|P(E(T_{\hat{v}_i}) = +1) = P(+1 : +1)_{\hat{v}_i} \quad (6)$$

$$\mathbb{P}^-_{\hat{v}_i} = P(E(J_{\hat{v}_i}) = -1)\Big|P(E(T_{\hat{v}_i}) = -1) = P(-1 : -1)_{\hat{v}_i} \quad (7)$$

Also, $0 < \mathbb{P}^+_{\hat{v}_i}, \mathbb{P}^-_{\hat{v}_i} < 1$ and $\mathbb{P}^+_{\hat{v}_i} > (1 - \mathbb{P}^-_{\hat{v}_i})$. Now, considering the fallibility of node $\hat{v}_i$, we define the corresponding Type I and Type II errors.

Definition 4. The *Type I* and *Type II errors* associated with the decision making of node $\hat{v}_i$ are defined as the probability with which it continues to operate in its present frequency band despite being affected by the jammer and the probability with which it switches frequency despite being unaffected by the jammer, respectively. Mathematically, $\forall \hat{v}_i$, $P(+1 : -1)_{\hat{v}_i}$ and $P(-1 : +1)_{\hat{v}_i}$ denote the Type I and Type II errors, respectively, and are expressed as:

$$P(+1 : -1)_{\hat{v}_i} = P(E(J_{\hat{v}_i}) = +1)\Big|P(E(T_{\hat{v}_i}) = -1) = 1 - \mathbb{P}^+_{\hat{v}_i} \quad (8)$$

$$P(-1 : +1)_{\hat{v}_i} = P(E(J_{\hat{v}_i}) = -1)\Big|P(E(T_{\hat{v}_i}) = +1) = 1 - \mathbb{P}^-_{\hat{v}_i} \quad (9)$$

Now to ascertain the probability that a node $\hat{v}_i$ is affected by the presence of jammer $\mathcal{J}$ in the network, i.e., the probability that $\hat{v}_i$ experiences a decrease in packet delivery ratio, we define the following metrics.

Definition 5. The *edge packet delivery ratio*, $\chi_{e^x_{i,j}}(t)$, at time t, is defined as the ratio of the number of packets sent by the node v_i and successfully received by the node v_j to the total number of packets transmitted by v_i to v_j, since the two nodes started operating on the frequency $x \in \{\alpha, \beta\}$. Note that, v_i and v_j here, are connected by the edge $e^x_{i,j}$, i.e., the two nodes are single-hop neighbors of each other. Mathematically expressing, we have:

$$\chi_{e^x_{i,j}}(t) = \frac{\sum_{\tau=t'}^{t} \Lambda^{ack}_{v_j,v_i}(\tau)}{\sum_{\tau=t'}^{t} \Lambda^{tot}_{v_i,v_j}(\tau)}, \forall v_i, v_j \in \mathcal{V}_x, x \in \{\alpha, \beta\} \quad (10)$$

where $\tau \leq t$ and $\tau = t'$ marks the time instant at which the nodes v_i and v_j started to operate in the same frequency $x \in \{\alpha, \beta\}$. $\Lambda^{tot}_{v_i,v_j}(\tau)$ and $\Lambda^{ack}_{v_j,v_i}(\tau)$ denote the number of packets sent from v_i to v_j at the τth time instant and the number of packets for which the acknowledgments are received by v_i, respectively. Clearly, in presence of the jammer $\mathcal{J}$, the edge packet delivery ratio drops to zero if the nodes are operating in the same frequency as $\mathcal{J}$ and either of nodes or both are within the coverage area of $\mathcal{J}$.

Definition 6. For a route $R = (v_{s_1}, v_{s_2}, \ldots, v_{s_k})$ the *route packet delivery ratio, $\psi_R(t)$*, at time t for a given source-destination pair of nodes is characterized by mean edge packet delivery ratio corresponding to the edges in the route since the time-instant when all nodes in the route started communicating in the same frequency. Mathematically, $\forall v_i, v_j \in \mathcal{V}$, we have:

$$\psi^x_R(t) = \frac{1}{k}\sum_{i=1}^{k-1} \chi_{e^x_{s_i,s_{i+1}}}(t) \quad (11)$$

where $x \in \{\alpha, \beta\}$.

Also, a node may send packets destined to several different nodes within the network over a given period of time. We, therefore, define the term nodal packet delivery ratio as follows.

Definition 7. The *nodal packet delivery ratio*, $\Psi^x_{v_i}(t)$, at time t, is defined as the ratio of the cumulative number of packets transmitted directly by node v_i to its one-hop neighboring nodes which are operating in the same frequency as v_i to the cumulative number of packets successfully received by the corresponding nodes. Mathematically,

$$\Psi^x_{v_i}(t) = \frac{\sum_{m=1}^{k^*} \chi_{e^x_{i,j}}(\tau_m)}{k^*}, \forall v_i, v_j \in \mathcal{V}_x, x \in \{\alpha, \beta\} \quad (12)$$

where k^* denotes the number of single-hop neighbor nodes to which node v_i is communicating at the time t, and τ_m ($\tau_m \leq t$, $\forall m$) marks the time instant since which the nodes v_i and v_j have started to communicate with each other.

Clearly, $\forall v_i \in \mathcal{V}$, at any time t, $0 \leq \Psi^x_{v_i}(t) \leq 1$. Moreover, the nodal packet delivery ratio acts as a measure for the degree of affliction for a (member) node due to presence of the jammer in the network. Therefore, at any given time t, for a member node of the society, i.e., $\forall \hat{v}_i \in \mathcal{S}(t)$, we have:

$$P(E(J_{\hat{v}_i}) = +1) = \Psi^x_{\hat{v}_i}(t) \quad (13)$$

$$P(E(J_{\hat{v}_i}) = -1) = 1 - \Psi^x_{\hat{v}_i}(t) \quad (14)$$

Now, probability that a node $\hat{v}_i$ will switch its frequency at time t, $\eta_{\hat{v}_i}(t)$, is computed based on $\hat{v}_i$'s behavior during the last t'' time instants, where $t'' < t$. Therefore, at time t, $\eta_{\hat{v}_i}(t)$ is statistically computed as:

$$\eta_{\hat{v}_i}(t) = \frac{\sum_{\tau=t''}^{t} c_{\hat{v}_i}(\tau)}{t - t''}, \qquad \forall \hat{v}_i \in \mathcal{S}(t) \quad (15)$$

where $c_{\hat{v}_i}(\tau)$ is a counter the value of which is incremented if node $\hat{v}_i$ has switched frequency at time τ. Therefore, clearly, $0 \leq \sum_{\tau=t''}^{t} c_{\hat{v}_i}(\tau) \leq t - t''$, $\forall \hat{v}_i$; i.e., $0 \leq \eta_{\hat{v}_i}(t)) \leq 1$. Therefore, $\forall \hat{v}_i \in \mathcal{S}$, at any given time t, we have:

$$P(E(T_{\hat{v}_i}) = +1) = \eta_{\hat{v}_i}(t) \quad (16)$$

$$P(E(T_{\hat{v}_i}) = -1) = 1 - \eta_{\hat{v}_i}(t) \tag{17}$$

Let $x_{\hat{v}_i(t)}$ be the decision of node $\hat{v}_i$ on whether it should switch its frequency at time t, such that $x_{\hat{v}_i(t)} \in \{+1, -1\}$. $x_{\hat{v}_i(t)} = 1$ indicates that node $\hat{v}_i$ switches its operating frequency at time t, whereas, $x_{\hat{v}_i(t)} = -1$ indicates otherwise.

Definition 8. A *decision profile* at time t is a vector containing the decisions of all the $\hat{n}(t)$ nodes of the society $\mathcal{S}(t)$, at that time, and is expressed as: $x(t) = (x_{\hat{v}_1}, x_{\hat{v}_2}, \ldots, x_{\hat{v}_{\hat{n}(t)}})$ and $\forall i$, $x_{\hat{v}_i} \in \{+1, -1\}$.

Considering the fallibility in decision making of the nodes, our goal is to formulate an optimal group decision rule based on which all the nodes in the network act, i.e., either the nodes switch frequency or they keep operating in their present frequency. Individual node decisions, however, are transmitted as a single-bit binary signal (0 and 1 indicating 'no' (i.e., $x_{\hat{v}_i} = -1$) and 'yes' (i.e., $x_{\hat{v}_i} = +1$) to the switching decision, respectively) to a central coordinator where subsequent optimal decisions are taken based on the decision profile.

4.2. Determination of the optimal decision rule

In this section, we first define the payoff associated with the decision making process. Based on this, the optimal decision rule is determined with a view to maximize the payoff of the overall network.

Definition 9. The *payoff* of a network is defined as the cumulative energy consumption of the network subjected to the network conditions, i.e., whether the jammer is active or not, and the decision made by the society, i.e., whether to switch frequency or not. The payoff of the network is denoted by $\Omega(i, j)$ where i corresponds to the decision of the society ($+1$ if the decision is to switch frequency and -1 if it decides to continue its operation in the present operating frequency) and j corresponds to the state of the jammer ($+1$ if the jammer is active and -1 otherwise). The payoffs associated with the following events, are given as follows.

(i) $\Omega(+1:+1)$: The payoff for switching frequency and successfully avoiding the jammer's adverse effects.
(ii) $\Omega(-1:-1)$: The payoff for retaining operations in the present operating frequency when there is no influence of the jammer.
(iii) $\Omega(+1:-1)$: The payoff for switching frequency despite there being no influence of the jammer on the network.
(iv) $\Omega(-1:+1)$: The payoff for continuing to work in the present operating frequency despite it being affected by the jammer.

Clearly, while we have: $\Omega(+1:+1) > \Omega(+1:-1)$ and $\Omega(-1:-1) > \Omega(-1:+1)$.

Again, $\lambda(t)$ is the proportion of nodes in $\mathcal{S}(t)$ experiencing an increased packet drop rate at time t due to the presence of $\mathcal{J}$. Clearly, $\forall t$, $0 < \lambda(t) < 1$. The magnitude of $\lambda(t)$ is, however, computed as a part of learning based on the variation in its magnitude is the prior time instants. At time t, $\lambda(t)$ is mathematically computed as:

$$\lambda(t) = \zeta\lambda(t-2) + (1-\zeta)\lambda(t-1), \forall t \tag{18}$$

where ζ is a predefined learning constant and the value of which is typically set to 0.5.

Now, let $\phi(x)$ be a function that works on the decision profile $x(t) \in X(t)$ and yields $+1$ (decision to switch frequency) or -1 (decision not to switch frequency) as its output. $X(t)$ denotes the total number of possible preference profiles available at time t. It is worthy of mentioning that for a society with $\hat{n}(t)$ members, the total number of distinct decision profiles is $2^{\hat{n}(t)}$, i.e., $|X(t)| = 2^{\hat{n}(t)}$, and also, $\phi(x) : X(t) \to \{+1, -1\}$, $\forall t$. Our objective is to optimize the group decision making process and select the aggregation rule in such a way so that the overall payoff of the society is maximized at every time instant. In order to do so, we first partition the set of all decision profiles, $X(t)$, into $X_{+1,\phi(x)}(t)$ and $X_{-1,\phi(x)}(t)$, such that $X_{+1,\phi(x)}(t) = \{x(t) \in X(t) : \phi(x) = +1\}$ and $X_{-1,\phi(x)}(t) = \{x(t) \in X(t) : \phi(x) = -1\}$. Here $X_{+1,\phi(x)}(t)$ denotes the set of all preference profiles on which, if applied, $\phi(x)$ yields $+1$ as output, and similarly for $X_{-1,\phi(x)}(t)$. Clearly, $X_{+1,\phi(x)}(t) \cup X_{-1,\phi(x)}(t) = X(t)$ and $X_{+1,\phi(x)}(t) \cap X_{-1,\phi(x)}(t) = \emptyset$, $\forall t$. Again, let for a given rule $\phi(x)$, a node $\hat{v}_i$ correctly switches its frequency in presence of a jammer or correctly retains it operation at the current frequency in absence of a jammer with probabilities $P(E(\phi(x) : +1))$ and $P(E(\phi(x) : -1))$, respectively, such that:

$$P(E(\phi(x):+1)) = P(x(t) \in X_{+1,\phi(x)}(t) : +1) \tag{19}$$

$$P(E(\phi(x):-1)) = P(x(t) \in X_{-1,\phi(x)}(t) : -1) \tag{20}$$

Clearly, $P(x(t) \in X_{-1,\phi(x)}(t) : +1) = 1 - P(E(\phi(x):+1))$ and $P(x(t) \in X_{+1,\phi(x)}(t) : -1) = 1 - P(E(\phi(x):-1))$.

Now, the goal of our work is to find the optimal group decision rule for which the overall system payoff is maximum under all conditions, or in other words, to attain the optimal value for $\bar{\Gamma}(t)$. Let $\Upsilon(t)$ be the overall payoff of the system at time t. Therefore, we have:

$$\bar{\Gamma}(t) \propto \frac{1}{\Upsilon(t)}, \forall t \tag{21}$$

This boils down our problem statement to defining the optimal rule $\bar{\phi}(x)$ such that $\Upsilon(t)$ is maximized. $\Upsilon(t)$ is mathematically expressed as:

$$\begin{aligned}\Upsilon(t) =& \lambda(t)[\Omega(+1:+1)P(E(\phi(x):+1)) + \Omega(-1:+1)(1- \\ & P(E(\phi(x):+1)))] + (1-\lambda(t))[\Omega(-1:-1)\times \\ & P(E(\phi(x):-1)) + \Omega(+1:-1)(1-P(E(\phi(x):-1)))]\end{aligned} \tag{22}$$

Lemma 1. *The goal of minimizing the mean packet drop of the network (i.e., determining the magnitude of $\bar{\Gamma}(t)$) can be translated into maximization of the overall societal payoff ($\max \Upsilon(t)$) for any given rule $\phi(x)$, where $\bar{\Upsilon}(t) = \max \Upsilon(t)$ is expressed as:*

$$\begin{aligned}\bar{\Upsilon}(t) =& \lambda(t)\Omega(+1)P(E(\phi(x):+1)) \\ & + (1-\lambda(t))\Omega(-1)P(E(\phi(x):-1))\end{aligned}$$

such that $\Omega(+1) = \Omega(+1:+1) - \Omega(-1:+1)$ and $\Omega(-1) = \Omega(-1:-1) - \Omega(+1:-1)$.

Proof. As expressed in Eq. (21), $\forall t$, $\Upsilon(t)$ varies inversely with $\bar{\Gamma}(t)$. Now, expanding Eq. (22), we have:

$$\begin{aligned}\Upsilon(t) =& \lambda(t)[\Omega(+1:+1)P(E(\phi(x):+1)) + \Omega(-1:+1)(1- \\ & P(E(\phi(x):+1)))] + [\Omega(-1:-1)P(E(\phi(x):-1)) \\ & + \Omega(+1:-1)(1-P(E(\phi(x):-1)))] - \lambda(t)[\Omega(-1: \\ & -1)P(E(\phi(x):-1)) + \Omega(+1:-1)(1- \\ & P(E(\phi(x)-1)))]\end{aligned} \tag{23}$$

$$\begin{aligned}=& \lambda(t)P(E(\phi(x):+1))\{\Omega(+1:+1) - \Omega(-1:+1)\} \\ & + (1-\lambda(t))P(E(\phi(x):-1))\{\Omega(-1:-1) - \Omega(+1: \\ & -1)\} + \lambda(t)\Omega(-1:+1) + (1-\lambda(t))\Omega(+1:-1)\end{aligned} \tag{24}$$

Substituting $\Omega(+1:+1) - \Omega(-1:+1)$ and $\Omega(-1) = \Omega(-1:-1) - \Omega(+1:-1)$ by $\Omega(+1)$ and $\Omega(-1)$, respectively, we write Eq. (23) as:

$$\begin{aligned}\Upsilon(t) =& \lambda(t)P(E(\phi(x):+1))\Omega(+1) \\ & + (1-\lambda(t))P(E(\phi(x):-1))\Omega(-1)\end{aligned}$$

$$+\lambda(t)\Omega(-1:+1)+(1-\lambda(t))\Omega(+1:-1) \quad (25)$$

Examining Eq. (25), we observe that last two (third and fourth) terms are independent of $\phi(x)$. Therefore, maximization of the equation necessarily boils down to maximization of the first two (first and second) $\phi(x)$-dependent terms. The maximum value of Υ(t), denoted by $\bar{\Upsilon}(t)$, is therefore, expressed as:

$$\begin{aligned}\bar{\Upsilon}(t) =&\lambda(t)\Omega(+1)P(E(\phi(x):+1))\\ &+(1-\lambda(t))\Omega(-1)P(E(\phi(x):-1))\end{aligned} \quad (26)$$

□

Theorem 2. *The optimal group decision rule, $\bar{\phi(x)}$, is mathematically classified as:*

$$\bar{\phi}(x)=\xi\left(\mathfrak{A}+\mathfrak{B}+\sum_{i=1}^{\hat{n}(t)}(\mathfrak{C}+\mathfrak{D})\{(x_{\hat{v}_i}^2+x_{\hat{v}_i})!-1\}-\sum_{i=0}^{\hat{n}(t)}\mathfrak{D}x_{\hat{v}_i}\right) \quad (27)$$

where, $\ln\dfrac{\lambda(t)}{1-\lambda(t)}=\mathfrak{A}$, $\ln\dfrac{\Omega(+1)}{\Omega(-1)}=\mathfrak{B}$, $\ln\dfrac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}=\mathfrak{C}$, $\ln\dfrac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}=\mathfrak{D}$, *and $\xi(a)$ is given as:*

$$\xi(a)=\begin{cases}+1, & \text{if } a>0\\ -1, & \text{otherwise}\end{cases} \quad (28)$$

Proof. At any given time t. for any decision profile $x(t)\in X(t)$, we divide the members of the society $\mathcal{S}(t)$ into two partitions, viz., $\mathcal{S}_R(t)$ and $\mathcal{S}_L(t)$, such that $\forall \hat{v}_i\in\mathcal{S}(t)$, $\hat{v}_i\in\mathcal{S}_R(t)$ if $x_{\hat{v}_i}=+1$ and $\hat{v}_i\in\mathcal{S}_L(t)$ if $x_{\hat{v}_i}=-1$. Clearly, $\mathcal{S}_R(t)\cup\mathcal{S}_L(t)=\mathcal{S}(t)$ and $\mathcal{S}_R(t)\cap\mathcal{S}_L(t)=\emptyset$. Also, we have $|\mathcal{S}_R(t)|+|\mathcal{S}_L(t)|=\hat{n}(t)$.

Let $\gamma_{\hat{v}_i}(\phi(x):+1)$ and $\gamma_{\hat{v}_i}(\phi(x):-1)$ be the probabilities of switching the present operating frequency given that the jammer is also operating in the same frequency and of retaining operation in the current frequency given that it is not affected by the jammer, respectively. Therefore, mathematically, we have the following two equations.

$$\gamma_{\hat{v}_i}(\phi(x):+1)=\prod_{\hat{v}_i\in\mathcal{S}_R(t)}\mathbb{P}^+_{\hat{v}_i}\prod_{\hat{v}_i\in\mathcal{S}_L(t)}(1-\mathbb{P}^+_{\hat{v}_i}) \quad (29)$$

$$\gamma_{\hat{v}_i}(\phi(x):-1)=\prod_{\hat{v}_i\in\mathcal{S}_L(t)}\mathbb{P}^-_{\hat{v}_i}\prod_{\hat{v}_i\in\mathcal{S}_R(t)}(1-\mathbb{P}^-_{\hat{v}_i}) \quad (30)$$

Now, for any given $\phi(x)$, we have:

$$P(E(\phi(x):+1))=\sum_{x(t)\in X_{+1,\phi(x)}(t)}\gamma_{\hat{v}_i}(\phi(x):+1) \quad (31)$$

and

$$P(E(\phi(x):-1))=\sum_{x(t)\in X_{-1,\phi(x)}(t)}\gamma_{\hat{v}_i}(\phi(x):-1) \quad (32)$$

Now replacing the terms in $P(E(\phi(x):+1))$ and $P(E(\phi(x):-1))$ in the result obtained from Lemma 1, we have:

$$\begin{aligned}\bar{\Upsilon}(t)=&\lambda(t)\Omega(+1)\sum_{x(t)\in X_{+1,\phi(x)}(t)}\gamma_{\hat{v}_i}(\phi(x):+1)\\ &+(1-\lambda(t))\Omega(-1)\sum_{x(t)\in X_{-1,\phi(x)}(t)}\gamma_{\hat{v}_i}(\phi(x):-1)\end{aligned} \quad (33)$$

Now, for any decision profile $x(t)\in X(t)$, we have:

$$\phi(x)=\begin{cases}+1, & \text{if } \lambda(t)\Omega(+1)\gamma_{\hat{v}_i}(\phi(x):+1)>\\ & \quad (1-\lambda(t))\Omega(-1)\gamma_{\hat{v}_i}(\phi(x):-1)\\ -1, & \text{otherwise}\end{cases}$$

Therefore, the necessary and sufficient condition for optimality of the group decision rule which ensures maximization of the overall system payoff can be expressed as:

$$X_{+1,\bar{\phi}(x)}(t)=\{x(t)\in X(t):\bar{\phi}(x)=+1\} \quad (34)$$

where $\bar{\phi}(x)(t)$ denotes the optimal decision rule. Next, using Eq. (34), we have:

$$\begin{aligned}X_{+1,\bar{\phi}(x)}(t)=&\{x(t):x(t)\in X(t)\text{ and}\\ &\lambda(t)\Omega(+1)\gamma_{\hat{v}_i}(\phi(x):+1)>\\ &(1-\lambda(t))\Omega(-1)\gamma_{\hat{v}_i}(\phi(x):-1)\}\end{aligned} \quad (35)$$

Again, replacing the values of $\gamma_{\hat{v}_i}(\phi(x):+1)$ and $\gamma_{\hat{v}_i}(\phi(x):-1)$ using Eqs. (29) and (30), we rewrite the above equation as:

$$\begin{aligned}X_{+1,\bar{\phi}(x)}(t)=&\{x(t):x(t)\in X(t)\text{ and }\frac{\lambda(t)}{1-\lambda(t)}\times\frac{\Omega(+1)}{\Omega(-1)}\times\\ &\prod_{\hat{v}_i\in\mathcal{S}_R(t)}\mathbb{P}^+_{\hat{v}_i}\prod_{\hat{v}_i\in\mathcal{S}_L(t)}(1-\mathbb{P}^+_{\hat{v}_i})>\prod_{\hat{v}_i\in\mathcal{S}_L(t)}\mathbb{P}^-_{\hat{v}_i}\prod_{\hat{v}_i\in\mathcal{S}_R(t)}(1-\mathbb{P}^-_{\hat{v}_i})\}\\ =&\{x(t):x(t)\in X(t)\text{ and }\frac{\lambda(t)}{1-\lambda(t)}\times\frac{\Omega(+1)}{\Omega(-1)}\times\\ &\prod_{\hat{v}_i\in\mathcal{S}_R(t)}\frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}-\prod_{\hat{v}_i\in\mathcal{S}_L(t)}\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}>0\}\end{aligned} \quad (36)$$

Now, for sake of convenience, we separate out the aforementioned inequality as:

$$\frac{\lambda(t)}{1-\lambda(t)}\frac{\Omega(+1)}{\Omega(-1)}\prod_{\hat{v}_i\in\mathcal{S}_R(t)}\frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}-\prod_{\hat{v}_i\in\mathcal{S}_L(t)}\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}>0 \quad (37)$$

Taking logarithm (base 2) in both sides, we have:

$$\begin{aligned}&\ln\frac{\lambda(t)}{1-\lambda(t)}+\ln\frac{\Omega(+1)}{\Omega(-1)}+\sum_{\hat{v}_i\in\mathcal{S}_R(t)}\ln\frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}\\ &\quad-\sum_{\hat{v}_i\in\mathcal{S}_L(t)}\ln\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}>0\end{aligned} \quad (38)$$

$$\begin{aligned}\Rightarrow&\ln\frac{\lambda(t)}{1-\lambda(t)}+\ln\frac{\Omega(+1)}{\Omega(-1)}+\sum_{i=1}^{\hat{n}(t)}\ln\frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}[(x_{\hat{v}_i}^2+x_{\hat{v}_i})!-1]\\ &-\sum_{i=0}^{\hat{n}(t)}\ln\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}[x_{\hat{v}_i}-(x_{\hat{v}_i}^2+x_{\hat{v}_i})!+1]>0\end{aligned} \quad (39)$$

Subtituting $\ln\dfrac{\lambda(t)}{1-\lambda(t)}$ and $\ln\dfrac{\Omega(+1)}{\Omega(-1)}$ by $\mathfrak{A}$ and $\mathfrak{B}$, we have:

$$\begin{aligned}\Rightarrow&\mathfrak{A}+\mathfrak{B}+\sum_{i=1}^{\hat{n}(t)}\ln\frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}(x_{\hat{v}_i}^2+x_{\hat{v}_i})!-\sum_{i=1}^{\hat{n}(t)}\ln\frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}\\ &-\sum_{i=0}^{\hat{n}(t)}\ln\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}x_{\hat{v}_i}+\sum_{i=0}^{\hat{n}(t)}\ln\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}(x_{\hat{v}_i}^2+x_{\hat{v}_i})!\\ &-\sum_{i=0}^{\hat{n}(t)}\ln\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}>0\end{aligned} \quad (40)$$

$$\begin{aligned}\Rightarrow&\mathfrak{A}+\mathfrak{B}+\sum_{i=1}^{\hat{n}(t)}(x_{\hat{v}_i}^2+x_{\hat{v}_i})!\left[\ln\frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}+\ln\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}\right]\\ &-\sum_{i=0}^{\hat{n}(t)}\ln\frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}x_{\hat{v}_i}-\sum_{i=0}^{\hat{n}(t)}\left[\ln\frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}+\right.\end{aligned}$$

$$\ln \frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}\Bigg] > 0 \qquad (41)$$

$$\Rightarrow \mathfrak{A} + \mathfrak{B} + \sum_{i=1}^{\hat{n}(t)} \left[\ln \frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})} + \ln \frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})} \right] \times \{(x^2_{\hat{v}_i} + x_{\hat{v}_i})! - 1\} - \sum_{i=0}^{\hat{n}(t)} \ln \frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})} x_{\hat{v}_i} > 0 \qquad (42)$$

Replacing $\ln \frac{\mathbb{P}^+_{\hat{v}_i}}{(1-\mathbb{P}^-_{\hat{v}_i})}$ and $\ln \frac{\mathbb{P}^-_{\hat{v}_i}}{(1-\mathbb{P}^+_{\hat{v}_i})}$ by $\mathfrak{C}$ and $\mathfrak{D}$, we have:

$$\Rightarrow \mathfrak{A} + \mathfrak{B} + \sum_{i=1}^{\hat{n}(t)} (\mathfrak{C} + \mathfrak{D})\{(x^2_{\hat{v}_i} + x_{\hat{v}_i})! - 1\} - \sum_{i=0}^{\hat{n}(t)} \mathfrak{D} x_{\hat{v}_i} > 0 \qquad (43)$$

Finally, replacing the simplified inequality obtain in Eq. (43) in Eq. (36), we get:

$$X_{+1,\bar{\phi}(x)}(t) = \{x(t) : x(t) \in X(t) \text{ and } \mathfrak{A} + \mathfrak{B} + \sum_{i=1}^{\hat{n}(t)} (\mathfrak{C} + \mathfrak{D}) \times \{(x^2_{\hat{v}_i} + x_{\hat{v}_i})! - 1\} - \sum_{i=0}^{\hat{n}(t)} \mathfrak{D} x_{\hat{v}_i} > 0\} \qquad (44)$$

Similarly, we have:

$$X_{-1,\bar{\phi}(x)}(t) = \{x(t) : x(t) \in X(t) \text{ and } \mathfrak{A} + \mathfrak{B} + \sum_{i=1}^{\hat{n}(t)} (\mathfrak{C} + \mathfrak{D}) \times \{(x^2_{\hat{v}_i} + x_{\hat{v}_i})! - 1\} - \sum_{i=0}^{\hat{n}(t)} \mathfrak{D} x_{\hat{v}_i} \leq 0\} \qquad (45)$$

Therefore, it is concluded that:

$$\bar{\phi}(x) = \xi\left(\mathfrak{A} + \mathfrak{B} + \sum_{i=1}^{\hat{n}(t)} (\mathfrak{C} + \mathfrak{D})\{(x^2_{\hat{v}_i} + x_{\hat{v}_i})! - 1\} - \sum_{i=0}^{\hat{n}(t)} \mathfrak{D} x_{\hat{v}_i}\right) \qquad (46)$$

where:

$$\xi(a) = \begin{cases} +1 & \text{,if } a > 0 \\ -1 & \text{,otherwise} \end{cases} \qquad (47)$$

□

Having obtained the optimal group decision rule, we now illustrate the application of the optimal decision rule through a case study.

4.3. Case study - solution

This part of the manuscript demonstrates the optimal decision rule-based solution to the problem of jamming in reference to the example case presented in Section 3.4. In continuation with the pair of figures (Fig. 1(a) and (b)) presented in Section 3.4, Fig. 2 illustrates the solution to the aforementioned problem. Fig. 2(c) shows the resumption of communication between the given source-destination pair of nodes after the nodes in the society decide to switch frequency and start to operate in frequency f_β. The nodes communicate through a new route R^* to avoid the jammer's influence.

The jammer $\mathcal{J}$, may however, decide to switch its operating frequency and start operating in frequency f_β in which case communication along the R^* route will again be affected as shown in Fig. 2(d). Once again, we apply the optimal decision rule to analyze its impact on the overall network. In Fig. 2(e), the state of the network if the outcome of the decision rule is to switch frequency to f_α is shown. Communication between the source and destination nodes may re-initiate along the route R once more. We highlight two important characteristics regarding the execution of the optimal decision rule as a solution to the problem of jamming in WSNs. Firstly, we mention that the optimal decision rule as a periodic routine within an aggregator node and such an aggregator node is chosen dynamically based on the network conditions. We also point out that, as shown, in the sample case, it is not always the case that if a jammer is operating in frequency f_α all nodes within the society would switch their operating frequency to f_β and vice versa. The decision of frequency-switch or continued operation in the same frequency is directly dependent on the societal benefit as a whole and on the benefit of one particular route only. We illustrate this situation in the following section as we analyze the utility of the optimal decision rule in the context of jamming avoidance in a network where communication is taking place across multiple routes.

Table 1
Notations and descriptions.

Parameters	Values
Terrain	250 m × 250 m
Number of nodes	50
Deployment pattern	Uniform random
Communication range (node)	75 m
Communication range (jammer)	150 m
Frame header length	34 Bytes
Frame payload length	0 – 2034 Bytes
E_{elec}	115 nJ/bit
E_{amp}	100 pJ/bit/m^2
Inital nodal energy	200 J

5. Performance analysis

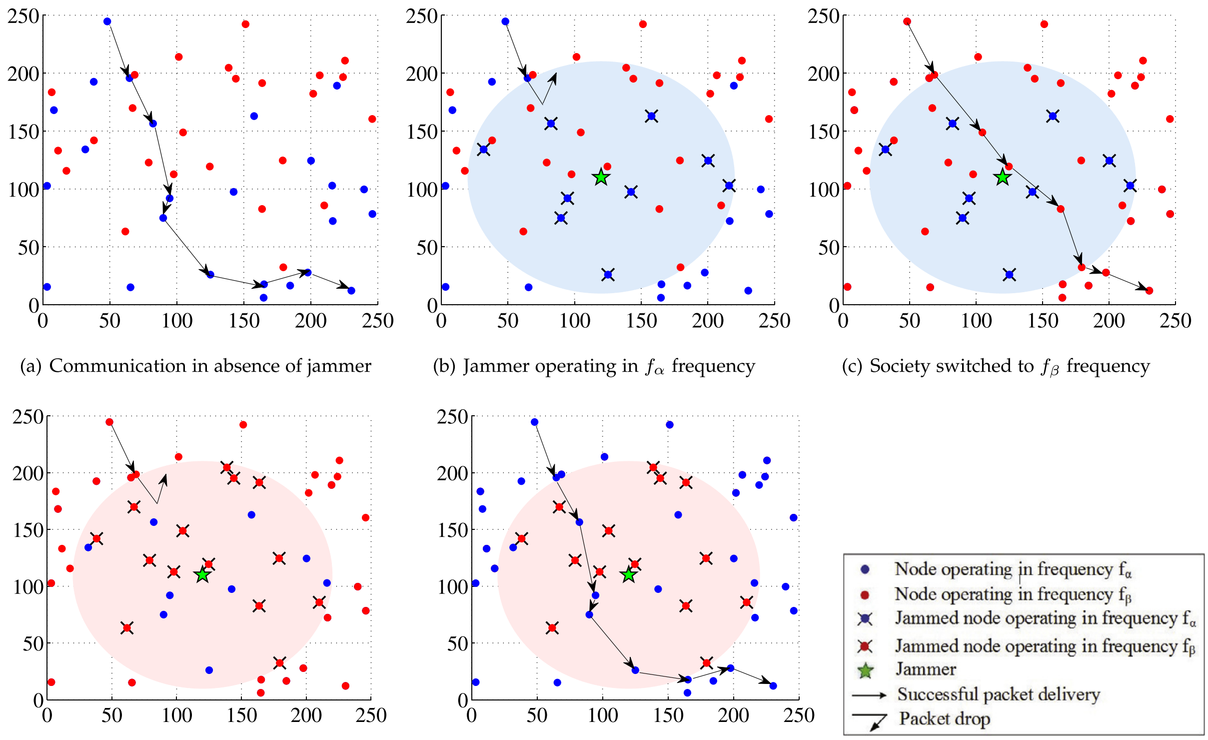
In this Section, we analyze the performance of the proposed solution both from the perspective of a particular sender-receiver pair and the network as a whole. We consider a single static jammer system for our simulation with frequency switching capabilities, i.e., the jammer, $\mathcal{J}$, may switch between frequencies f_α and f_β at its will with an intention to disrupt the network communications maximally. The location coordinates of $\mathcal{J}$ is fixed at $(x_\mathcal{J}, y_\mathcal{J}) = (120, 110)$. The 50 nodes distributed across the planer terrain are consider to operate in either of the frequencies at time $t = 0$. The nodes are static in nature and the corresponding deployment of the (numbered) nodes are presented in Fig. 3. The network traffic is taken to be of variable bitrate (VBR) with a mean of 1 and variance of 0.58 packets per minute. We considered the first order radio model [43] for the energy expended by the radio to transmit and receive the messages. The equations for the energy computation to transmit and receive the messages are as follows:

$$E_{Tx}(c, r) = E_{elec} * c + e_{amp} * c * r^2 \qquad (48)$$

$$E_{Rx}(c) = E_{elec} * c \qquad (49)$$

where $E_{Tx}(c, r)$ is the energy consumed by the radio to transmit c bits of data over a distance of r meters, and $E_{Rx}(c)$ is the energy consumed by the radio to receive c bits of data, respectively. E_{elec} denotes the energy (in nJ/bit) required to run the transmitter or receiver circuitry and e_{amp} (in $pJ/bit/m^2$) denotes the energy consumed by the transmitter amplifier. Table 1 highlights the key simulation parameters used for the purpose.

We consider the transmissions ongoing through 10 routes in the network, as shown in Table 2, and analyze the impact of the jammer on them. Note that, at any given time instant, a communication route may only consist of nodes operating in the same frequency. At $t = 0$, routes R_1 to R_5 are considered to communicate in



(a) Communication in absence of jammer (b) Jammer operating in f_α frequency (c) Society switched to f_β frequency

(d) Jammer switched to in f_β frequency (e) Society switched to f_α frequency

Fig. 2. Case study of jamming avoidance by frequency switching using the optimal decision rule.

Table 2
Route composition.

Fr.	Route	Constituent vertices										
f_α	R_1	v_{49}	v_7	v_{11}	v_{33}	v_3	v_5	v_{10}	v_{50}	v_{19}		
	R_2	v_{13}	v_1	v_5	v_2	v_{36}	v_{24}	v_{29}	v_{38}	v_{20}		
	R_3	v_{41}	v_{16}	v_{27}	v_{48}	v_7	v_{11}	v_{33}	v_2	v_{24}	v_{29}	
	R_4	v_{12}	v_{10}	v_{40}	v_{50}	v_{19}						
	R_5	v_1	v_5	v_{10}	v_{12}	v_{40}	v_{50}	v_{19}				
f_β	R_6	v_4	v_8	v_{32}	v_{35}	v_{34}	v_{30}	v_{17}	v_{25}	v_{43}	v_{45}	v_6
	R_7	v_8	v_{32}	v_{35}	v_{37}	v_{15}	v_{39}	v_{28}	v_{18}	v_{31}		
	R_8	v_4	v_{30}	v_{17}	v_{42}	v_6	v_{22}	v_{21}				
	R_9	v_{47}	v_{22}	v_6	v_{44}	v_{45}	v_{43}	v_{25}	v_{42}			
	R_{10}	v_9	v_{37}	v_{15}	v_{26}	v_{39}	v_{28}	v_{18}	v_{31}			

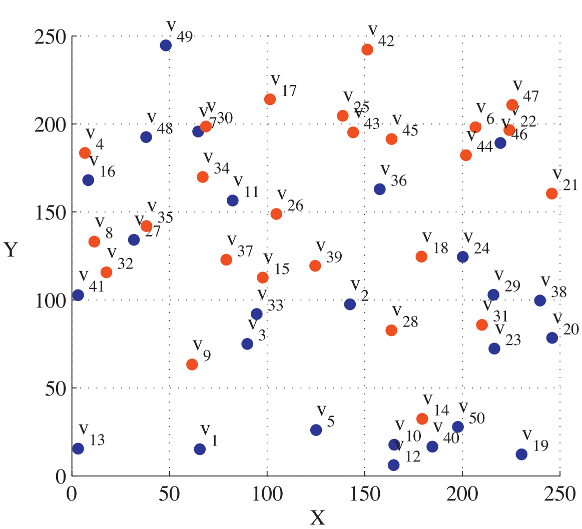
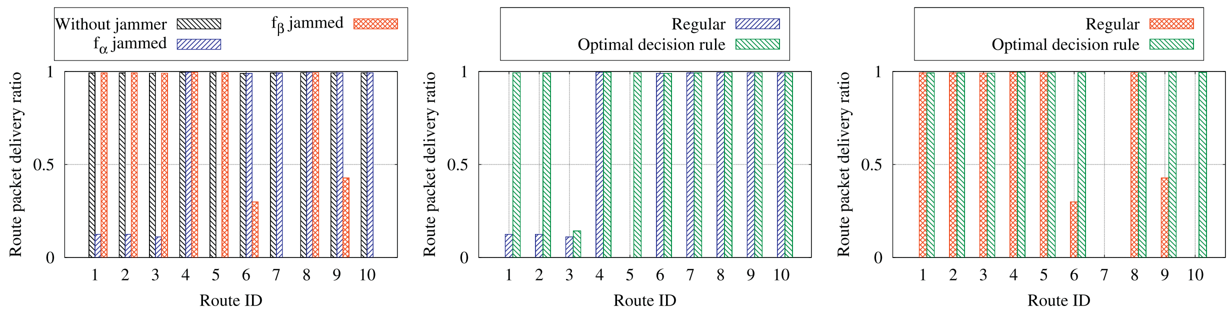


Fig. 3. Node deployment.

the frequency f_α, whereas, routes R_6 through R_{10} communicate in f_β. Also, all data are collected over 50 iterations in each case and the corresponding results are plotted with 95% confidence.

5.1. Packet delivery ratio

In Fig. 4, we plot the average packet delivery ratio of a route against the route IDs. We observe that in Fig. 4(a), initially, the PDR was close to 1 when the jammer $\mathcal{J}$ was inactive. However, in presence of $\mathcal{J}$ the PDR is observed to drop significantly. When $\mathcal{J}$ operates in f_α, only routes R_1 through R_5 except R_4 is observed to be affected. Clearly, as the nodes involved in routes R_6 to R_{10}, communication in these routes are unaffected by the presence of $\mathcal{J}$. It is noteworthy that despite operating in f_α, communication in route R_4 remains unaffected as the source and the destination nodes including the intermediates of nodes are all located outside the jammer's communication range. The overall network PDR decreases by 36.35% in this case. Similarly, if $\mathcal{J}$ switches to frequency f_β, all routes from R_6 to R_{10} except R_8 are affected. The network PDR, in this case drops by 32.65%. However, once again, we observed that route R_8 is unaffected by the jammer's presence as all nodes in this route are beyond its communication range.



(a) Effect of jammer on both frequencies (b) Jammer operating in f_α frequency (c) Jammer operating in f_β frequency

Fig. 4. Analysis of route packet delivery ratio vs route ID.

Table 3
Modified route compositions after switching frequency to f_β.

Route	Constituent vertices								
R_1	v_{49}	v_{30}	v_{26}	v_{39}	v_{28}	v_{14}	v_{50}	v_{19}	
R_2	v_{13}	v_1	v_9	v_{37}	v_{39}	v_{28}	v_{14}	v_{50}	v_{20}
R_3	v_{41}	v_{32}	v_{35}	v_{37}	v_{15}	v_{39}	v_{18}		
R_4	v_{12}	v_{10}	v_{40}	v_{50}	v_{19}				
R_5	v_1	v_9	v_{37}	v_{39}	v_{28}	v_{14}	v_{50}	v_{19}	

Table 4
Modified route compositions after switching frequency to f_α.

Route	Connecting vertices							
R_6	v_4	v_{48}	v_7	v_{30}	v_{17}	v_{42}	v_6	
R_7	v_8	v_{27}	v_{11}	v_{33}	v_2	v_{36}	v_{24}	
R_8	v_4	v_{48}	v_{30}	v_{17}	v_{42}	v_2	v_{22}	v_{21}
R_9	v_{47}	v_6	v_{42}					
R_{10}	v_9	v_1	v_5	v_{14}	v_{23}	v_{31}		

In Fig. 4(b), we compare the PDR of the routes when the jammer is operating in frequency f_α and the nodes continued to operate as per the regular FHSS policy with the case when the jammer $\mathcal{J}$ is operational in f_α but based on the optimal decision rule all nodes in the society decide to switch to frequency f_β. Table 3 presents the re-adjusted communication routes for routes R_1 through R_5. Note that routes R_6 through R_{10} remain unaffected by the presence of $\mathcal{J}$. We observe a 30.40% improvement in the PDR of the network as a whole, when the society decides to switch. However, for route R_3, as the destination node, v_{29}, is within the region affected by the influence of the $\mathcal{J}$, i.e., the node is not a member of the society and is unable to switch its frequency. The PDR for route R_3, is thus, remains unimproved by the decision of the society.

Similar observations are made in Fig. 4(c). The modified routes corresponding to routes R_6 through R_{10} are shown in Table 4 while routes R_1 through R_5 remain unaffected by the jammer's presence. We compute that using optimal decision rule we obtain 25.26% improvement over the scenario in which the nodes continue to operate in a same frequency. However, in this case as well, for route R_7 the PDR is not improved. Once again, this is because the destination node, v_{31}, in this case, is inside the jammer-affected region, and therefore, is unable to take part in the decision making process.

5.2. Energy consumption

We now, analyze energy dissipation of a node both route-wise and from the network's perspective and with variable frame size.

5.2.1. Route-wise analysis

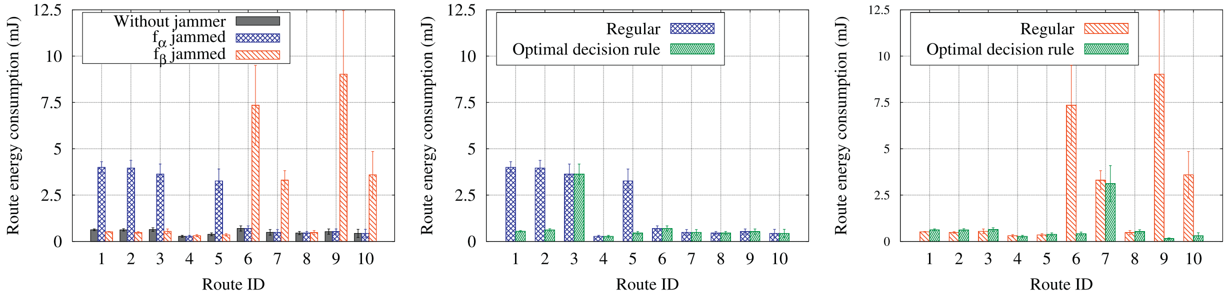
In Fig. 5, the cumulative energy consumption of all the nodes in a route is plotted against the route IDs and variation of energy consumption. we observed that, the mean energy consumption increases by multiple folds in presence of the jammer, as shown in Fig. 5(a). The multiple fold increase in the energy consumption of the particular route under the influence of the jammer is because of the repeated re-transmission of the dropped data packet. In our work the re-transmission limit for the particular data packet is set to 16. When the jammer is operating in f_α frequency. The overall energy consumption for all the routes in the network is observed to be increased by 3.44 times than that of when the jammer is absent. However, energy consumption corresponding to route R_4 is almost unaltered as no nodes within this route falls under the jammer's influence. A 5.03 times increment in the network's energy consumption is noted when the jammer is operating in f_β. Once again, it is noted that the energy consumption of route $R8$ remains unaffected by the presence of the jammer as it lies entirely outside the jammed region.

We analyze the impact of the optimal decision rule on the energy consumption in Fig. 5(b) and (c). Firstly, in Fig. 5(b), we study the impact of the decision taken by the society on the network. The overall network energy consumption of 54.16% is noted after the application of the proposed solution, which is only 1.58 times of that in absence of the jammer. Similar, pattern is observed in Fig. 5(c) where the network's energy consumption, as a whole, is improved by 72.73% compared to the jammed state which is only 1.37 times of the ideal state. Note that, in routes R_3 and R_7 in Fig. 5(b) and (c), respectively, do not show improvements in terms of energy consumption even after the application of the optimal solution as the source and destination nodes, respectively, are inside the jammed region. This implies that neither node may take part in the decision making process, nor are they capable of switching their frequencies based on the societal choices.

Next, we inspect the energy dissipation of the network as a whole, first with time, and then against variable frame size.

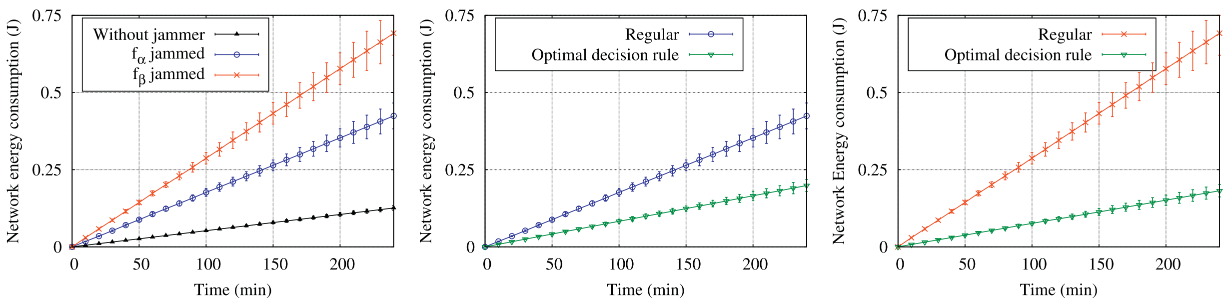
5.2.2. Network-level analysis with time

We plot the variation in the cumulative network energy consumption against time in Fig. 6. We analyze the energy dissipation of the network for 4 simulation hours (240 simulation minutes) and plot the results. In Fig. 6(a), we observe a steadily increasing linear curve for the cumulative energy consumption of the network in absence of the jammer. However, the slope of the plots corresponding to the network energy dissipation are observed to increase significantly when there is a jammer present in the network, operating in either frequencies. The cumulative energy consumption of the network is studied to be increased by 3.36 times and 5.29 times when the jammer is operating in f_α and f_β frequencies, respectively, compared to that when the jammer is



(a) Effect of jammer on both frequencies (b) Jammer operating in f_α frequency (c) Jammer operating in f_β frequency

Fig. 5. Analysis of route energy consumption vs route ID.



(a) Effect of jammer on both frequencies (b) Jammer operating in f_α frequency (c) Jammer operating in f_β frequency

Fig. 6. Analysis of network energy consumption vs time.

non-existent. The repeated frame-drops caused by the influence of the jammer, which results in multiple re-transmissions of the same data frames, trigger a surge in the energy consumption of the network, as a whole.

However, comparing the results shown in Fig. 6(b) with that of Fig. 6(a), we notice an improvement of 53.10% in the cumulative energy dissipation of the network. Application of the optimal decision rule in a jammer-affected scenario is observed to diminish the overall network energy consumption to only 1.57% of that of the ideal scenario. Similar results are obtained as we study the results plotted in Fig. 6(c). The energy dissipation of the network is observed to be improved by 73.74%, mitigating it to only 1.44 times of that when the jammer is absent from the network. It is noteworthy that even after the application of the optimal decision rule on the network when it is affected by the jammer's presence, the network energy consumption never gets close to its ideal value. This is because not all communication routes are altered successfully through application of the decision rule as routes with either the source or the destination nodes (or both) placed within the jammer's communication region may not take part in the decision making processing, and thus, are unable to switch frequencies.

5.2.3. Network-level analysis with variable frame size

Having analyzed the variation of the network energy with time, we now analyze the effects of variable frame size on the energy consumed by the network as a whole in Fig. 7. As mention in Table 1, the frame header size in the IEEE 802.11 communication standard is 34 bytes inclusive of the 4 bytes for frame check sequence (FCS), whereas the frame payload size may vary between 0 – 2034 bytes. We observe in Fig. 7(a), with the variation of the frame size, the network energy consumption increases by a steady but slow rate in absence of the jammer. However, when the jammer starts to operate in the f_α frequency, the energy consumption of the network is noticed to increase by approximately 3.36 times and close to 5.47 times when the jammer operates in the f_β frequency.

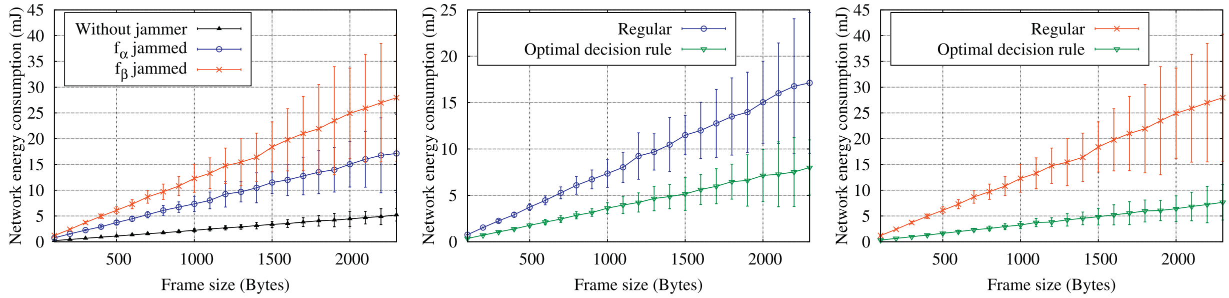
Fig. 7(b), however, depicts that application of the optimal decision rule vastly improves the condition and the overall energy consumption of the network is reduced by 53.18% as all the members nodes of the society decides to switch their frequencies. Similar patterns are observed in Fig. 7(c), where we notice a sharp decrease in the network's energy consumption by 73.29% as the optimal decision rule is put into application. However, once again, in neither of the cases, the energy dissipation of the network is diminished enough to be close to the ideal state, i.e., the energy dissipation of the network in absence of the jammer as route in which the source or destination node (or both) are positioned within the jammer-impacted region may not take part in the decision making procedure, and hence, may not be able to act accordingly to avoid the jammer's interception.

Finally, in Fig. 8, we plot the amount of energy salvaged by the application of the optimal decision rule. Fig. 8(a) shows the amount of cumulative energy recovered over time as the optimal decision making was put into play. Similarly, in Fig. 8(b), the amount of energy saved is plotted against the frame size. Through this we establish the suitability of the optimal decision rule, and thus, justify its application in the jamming avoidance.

5.3. Synthesis

Finally, based on the results obtained, we summarize the key-takeaways from the experiments performed. The observations are presented as follows:

- Application of the optimal decision rule for ex-ante frequency hopping effectively diminishes the PDR and consequently the energy consumption of the overall network.
- In our case study, for route R_3 the destination node (node v_{18}) is within the jammer-affected region. The same holds true for



(a) Effect of jammer on both frequencies (b) Jammer operating in f_α frequency (c) Jammer operating in f_β frequency

Fig. 7. Analysis of network energy consumption vs frame size.

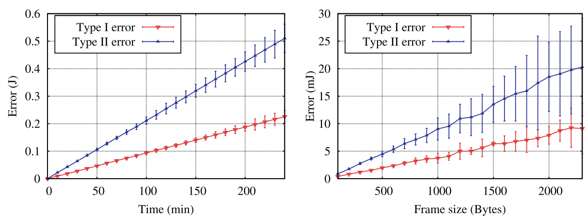


Fig. 8. Analysis of Type I and Type II errors.

the source node (node v_8) for route R_7. Therefore, even after application of the optimal decision rule, the performance of neither of these routes is improved.

- The network payoff, i.e., the overall network energy consumption, however, is observed to be highly improved in case of the proposed solution approach. This comes as a direct consequence of reduced frame transmission as compared to a jammer-afflicted sub-network. Note that, the proposed solution aims to achieve a globally optimal solution considering the entire network condition than a region-specific local solution to the jamming.

6. Conclusion

This work addresses the problem of jamming avoidance using frequency hopping technique. We consider the situation with a static WSN affected by a constant static jammer, which is capable of switching frequencies. We assume that the nodes in the network and the jammer are able to switch between two different frequencies. The objective of this work is to determine the optimal decision rule for frequency-hopping with a larger goal of maximizing the overall network throughput. We observe that, in the presence of a jammer, the route packet delivery ratio as well as the network packet delivery ratio are affected adversely by a significant extent. Results confirm that application of the optimal decision rule in such situations improves the network throughput and minimizes the energy consumption by a notable margin.

In future, we plan to extend our solution approach for situations with large number of operating frequencies. Also, we plan to investigate the utility of the proposed mechanism in the context of mobile WSNs and mobile jammers.

References

[1] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM, 2005, pp. 46–57.
[2] A. Wood, J. Stankovic, S. Son, JAM: a jammed-area mapping service for sensor networks, in: Proceedings of the 24th IEEE Real-Time Systems Symposium, 2003, pp. 286–297.
[3] S. Vadlamani, B. Eksioglu, H. Medal, A. Nandi, Jamming attacks on wireless networks: a taxonomic survey, Int. J. Prod. Econ. 172 (2016) 76–94.
[4] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. Pantziou, A survey on jamming attacks and countermeasures in WSNs, IEEE Commun. Surv. Tutorials 11 (4) (2009) 42–56.
[5] L. Tytgat, O. Yaron, S. Pollin, I. Moerman, P. Demeester, Analysis and experimental verification of frequency-based interference avoidance mechanisms in IEEE 802.15.4, IEEE/ACM Trans. Networking 23 (2) (2015) 369–382.
[6] G. Chen, Y. Li, L. Xiao, L. Huang, Collaborative anti-jamming broadcast with uncoordinated frequency hopping over USRP, in: Proceedings of the IEEE 81st Vehicular Technology Conference, 2015, pp. 1–6.
[7] M. Yu, Y. Wang, G. Wang, A novel ICA-based frequency hopping receiver with correlated jamming suppression, in: Proceedings of the International Conference on Wireless Communications Signal Processing, 2012, pp. 1–5.
[8] C. Popper, M. Strasser, S. Capkun, Anti-jamming broadcast communication using uncoordinated spread spectrum techniques, IEEE J. Sel. Areas Commun. 28 (5) (2010) 703–715.
[9] O.D. Incel, A survey on multi-channel communication in wireless sensor networks, Comput. Netw. 55 (13) (2011) 3081–3099.
[10] M.-A.E. Houssaini, A. Aaroud, A.E. Hore, J. Ben-Othman, Detection of jamming attacks in mobile ad hoc networks using statistical process control, Procedia Comput. Sci. 83 (2016) 26–33.
[11] S. Misra, S.K. Dhurandher, A. Rayankula, D. Agrawal, Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks, Comput. Electr. Eng. 36 (2) (2010) 367–382. Wireless ad hoc, Sensor and Mesh Networks
[12] S. Misra, S. Dash, M. Khatua, A.V. Vasilakos, M.S. Obaidat, Jamming in underwater sensor networks: detection and mitigation, IET Commun. 6 (14) (2012) 2178–2188.
[13] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Comput. Netw. 38 (4) (2002) 393–422.
[14] S. Misra, S. Sarkar, Priority-based time-slot allocation in wireless body area networks during medical emergency situations: an evolutionary game-theoretic perspective, IEEE J. Biomed. Health Inform. 19 (2) (2015) 541–548.
[15] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Netw. 52 (12) (2008) 2292–2330.
[16] S. Chatterjee, S. Sarkar, S. Misra, Quantification of node misbehavior in wireless sensor networks: a social choice-based approach, in: IEEE International Conference on Communication Workshop, Institute of Electrical and Electronics Engineers (IEEE), 2015, pp. 1479–1484.
[17] S. Sarkar, S. Misra, From micro to nano: the evolution of wireless sensor-based health care, IEEE Pulse 7 (1) (2016) 21–25, doi:10.1109/mpul.2015.2498498.
[18] V. Potdar, A. Sharif, E. Chang, Wireless sensor networks: a survey, in: International Conference on Advanced Information Networking and Applications Workshops, Institute of Electrical and Electronics Engineers (IEEE), 2009.
[19] A. Spyropoulos, C. Raghavendra, Energy efficient communications in ad hoc networks using directional antennas, in: Proceedings of the IEEE 21st Annual Joint Conference of the IEEE Computer and Communications Societies, 1, 2002, pp. 220–228.
[20] G.-Y. Chang, J.-F. Huang, Z.-H. Wu, A frequency hopping algorithm against jamming attacks under asynchronous environments, in: Proceedings of the IEEE International conference on Global Communications, 2014, pp. 324–329.
[21] E. Achuthan, R. Kishore, A novel anti jamming technique for wireless sensor networks, in: Proceedings of the International Conference on Communications and Signal Processing, 2014, pp. 920–924.
[22] L. Zhang, H. Wang, T. Li, Anti-jamming message-driven frequency hopping x2014;part I: system design, IEEE Trans. Wireless Commun. 12 (1) (2013) 70–79.
[23] I. Mansour, G. Chalhoub, A. Quilliot, Security architecture for wireless sensor networks using frequency hopping and public key management, in: Proceedings of the IEEE International Conference on Networking, Sensing and Control, 2011, pp. 526–531.
[24] R. Pickholtz, D. Schilling, L. Milstein, Theory of spread-spectrum communications–a tutorial, IEEE Trans. Commun. 30 (5) (1982) 855–884.
[25] H. Quan, H. Zhao, P. Cui, Anti-jamming frequency hopping system using multiple hopping patterns, Wireless Pers. Commun. 81 (3) (2015) 1159–1176.

[26] Y. Desmedt, R. Safavi-Naini, H. Wang, L. Batten, C. Charnes, J. Pieprzyk, Broadcast anti-jamming systems, Comput. Netw. 35 (2–3) (2001) 223–236.
[27] L. Xiao, H. Dai, P. Ning, Jamming-resistant collaborative broadcast using uncoordinated frequency hopping, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 297–309.
[28] Q. Wang, P. Xu, K. Ren, X.-Y. Li, Towards optimal adaptive UFH-based anti-Jamming wireless communication, IEEE J. Sel. Areas Commun. 30 (1) (2012) 16–30.
[29] M. Strasser, C. Pöpper, S. Čapkun, Efficient uncoordinated FHSS anti-jamming communication, in: Proceedings of the 10th ACM International Symposium on Mobile Ad Hoc Networking and Computing, in: MobiHoc '09, ACM, 2009, pp. 207–218.
[30] C. Pöpper, M. Strasser, S. Čapkun, Jamming-resistant broadcast communication without shared keys, in: Proceedings of the 18th Conference on USENIX Security Symposium, in: SSYM'09, USENIX Association, 2009, pp. 231–248.
[31] S. Bag, B. Roy, Two channel hopping schemes for jamming resistant wireless communication, in: Proceedings of the 9th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2013, pp. 659–666.
[32] A. Alagil, M. Alotaibi, Y. Liu, Randomized positioning DSSS for anti-jamming wireless communications, in: Proceedings of the International Conference on Computing, Networking and Communications, 2016, pp. 1–6.
[33] M. Li, I. Koutsopoulos, R. Poovendran, Optimal jamming attack strategies and network defense policies in wireless sensor networks, IEEE Trans. Mobile Comput. 9 (8) (2010) 1119–1133.
[34] Y. Zhang, Y. Shen, J. Zhu, X. Jiang, Eavesdropper-tolerance capability in two-Hop wireless networks via cooperative jamming, Ad Hoc Sens. Wireless Netw. 29 (2015) 113–131.
[35] N. Rouissi, H. Gharsellaoui, S. Bouamama, A hybrid DS-FH-THSS approach anti–jamming in wireless sensor networks, in: Proceedings of the 14th International Conference on Software Engineering Research, Management and Applications, 2016, pp. 133–139.
[36] P. Du, G. Roussos, Adaptive time slotted channel hopping for wireless sensor networks, in: Proceedings of the 4th Computer Science and Electronic Engineering Conference, 2012, pp. 29–34.
[37] J. Mahapatro, S. Misra, M. Manjunatha, N. Islam, Interference-aware channel switching for use in WBAN with human-sensor interface, in: Proceedings of the 4th International Conference on Intelligent Human Computer Interaction, 2012, pp. 1–5.
[38] S. Misra, R. Singh, S.V.R. Mohan, Geomorphic zonalisation of wireless sensor networks based on prevalent jamming effects, IET Commun. 5 (12) (2011) 1732–1743, doi:10.1049/iet-com.2010.0512.
[39] S. Misra, R. Singh, S.V.R. Mohan, Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system, Sensors 10 (4) (2010) 3444, doi:10.3390/s100403444.
[40] C.F. Shih, A.E. Xhafa, J. Zhou, Practical frequency hopping sequence design for interference avoidance in 802.15.4e TSCH networks, in: Proceedings of the IEEE International Conference on Communications, 2015, pp. 6494–6499.
[41] R.C. Ben-Yashar, S.I. Nitzan, The optimal decision rule for fixed-size committees in dichotomous choice situations: the general result, Int. Econ. Rev. 38 (1) (1997) 175–186.
[42] S. Chatterjee, S. Sarkar, S. Misra, Energy-efficient data transmission in sensor–cloud, in: Proceedings of the Applications and Innovations in Mobile Computing, 2015, pp. 68–73.
[43] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, in: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000. 10 pp

Prasenjit Bhavathankar received his M.Tech. degree in Computer Engineering from Mumbai University, India in 2007 and B.E. in Computer Engineering from Shivaji University, India . He is presently pursuing his Ph.D. from the Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur. His current research interests are wireless ad-hoc and sensor networks.

Subhadeep Sarkar is presently pursuing his Ph.D. from the School of Medical Science and Technology, Indian Institute of Technology Kharagpur, India. He has also worked as a Junior Research Fellow (2013–'14) and as a Senior Research Fellow (2014–'15) at School of Information Technology, Indian Institute of Technology Kharagpur in a project funded by Department of Electronics and Information Technology (DEITY), Government of India. He received his B. Tech. degree in Computer Science and Engineering from West Bengal University of Technology, India in 2012. Subhadeep was selected as one of the Most Qualified Young Scientists to attend the 4th Heidelberg Laureate Forum (HLF), 2016 held at Heidelberg, Germany. He was the awarded the second best Ph.D. thesis awarded at the 5th IDRBT Doctoral Colloquium, 2015 held at Hyderabad, India organized by Institute for Development and Research in Banking Technology (IDRBT) in collaboration with Reserve Bank of India (RBI). His current research interests include networking and communication aspects of Wireless Body Area Networks (WBANs), Cloud Computing, and Fog Computing.

Sudip Misra is an Associate Professor in the Department of Computer Science and Engineering at the Indian Institute of Technology Kharagpur. Prior to this he was associated with Cornell University (USA), Yale University (USA), Nortel Networks (Canada) and the Government of Ontario (Canada). He received his Ph.D. degree in Computer Science from Carleton University, in Ottawa, Canada, and the masters and bachelors degrees respectively from the University of New Brunswick, Fredericton, Canada, and the Indian Institute of Technology, Kharagpur, India. Dr. Misra has several years of experience working in the academia, government, and the private sectors in research, teaching, consulting, project management, architecture, software design and product engineering roles. His current research interests include algorithm design for emerging communication networks. Dr. Misra is the author of over 180 scholarly research papers (including 90 journal papers). He has won eight research paper awards in different conferences. He was awarded the IEEE ComSoc Asia Pacific Outstanding Young Researcher Award at IEEE GLOBECOM 2012, Anaheim, California, USA. He was also the recipient of several academic awards and fellowships such as the Young Scientist Award (National Academy of Sciences, India), Young Systems Scientist Award (Systems Society of India), Young Engineers Award (Institution of Engineers, India), (Canadian) Governor Generals Academic Gold Medal at Carleton University, the University Outstanding Graduate Student Award in the Doctoral level at Carleton University and the National Academy of Sciences, India Swarna Jayanti Puraskar (Golden Jubilee Award). He was also awarded the Canadian Governments prestigious NSERC Post Doctoral Fellowship and the Humboldt Research Fellowship in Germany. Dr. Misra is the Editor-in-Chief of the International Journal of Communication Networks and Distributed Systems (IJCNDS), Inderscience, U.K.. He has also been serving as the Associate Editor of the Telecommunication Systems Journal (Springer), Security and Communication Networks Journal (Wiley), International Journal of Communication Systems (Wiley), and the EURASIP Journal of Wireless Communications and Networking. He is also an Editor/Editorial Board Member/Editorial Review Board Member of the IET Communications Journal, IET Wireless Sensor Systems, and Computers and Electrical Engineering Journal (Elsevier). Dr. Misra has edited 6 books in the areas of wireless ad hoc networks, wireless sensor networks, wireless mesh networks, communication networks and distributed systems, network reliability and fault tolerance, and information and coding theory, published by reputed publishers such as Springer, Wiley, and World Scientific. He was invited to chair several international conference/workshop programs and sessions. He served in the program committees of several international conferences. Dr. Misra was also invited to deliver keynote/invited lectures in over 20 international conferences in USA, Canada, Europe, Asia and Africa.