Link-Quality Aware Path Selection in the Presence of Proactive Jamming in Fallible Wireless Sensor Networks

Prasenjit Bhavathankar, *Student Member, IEEE*, Subarna Chatterjee, *Student Member, IEEE*, and Sudip Misra, *Senior Member, IEEE*

***Abstract*— In this paper, we propose a mechanism to ensure the proper functioning of a wireless sensor network (WSN) in the presence of static and proactive jammer within the network. Existing research works have primarily focused on the detection of jammer node within the network and ameliorating its consequent effects on the network. However, these countermeasures to mitigate the effect of the jammer suffer from certain limitations as WSNs are primarily resource constrained and most of the countermeasures are computationally intensive. The objective of this paper is to prevent the disruption of the network in the presence of jamming by bypassing the jammed zone and setting up alternative paths. The alternative paths are chosen with the maximum link quality in order to maintain the quality of service of the network even after jamming. This paper proposes *Link-quality Aware Path SElection* (*LAPSE*) algorithm that chooses alternative paths based on the optimal link quality. LAPSE is based on *optimal decision rule* and its design considers the fallible nature of the nodes while choosing/rejecting a particular link. Finally, the performance of the proposed algorithm, LAPSE, is evaluated in terms of the network parameters—packet delivery rate, network throughput, transmission energy, node lifetime, and network lifetime. Results indicate that the performance of LAPSE is significantly better than the existing jamming avoidance algorithms.**

***Index Terms*— Jamming, wireless sensor network (WSN), routing, link quality, fallibility.**

I. Introduction

IN THE recent past, Wireless Sensor Networks (WSNs) have rapidly emerged and evolved because of their widespread and varied applicability across different domains [1], [2] such as target tracking [3], [4], military applications [5], [6], fuel management [7], health monitoring [8], robotics [9], and agriculture [10], [11]. However, WSNs are also vulnerable to several threats and attacks. Among these, *jamming* is a serious form of attack that disrupts and collapses a WSN very deeply. A jammer successfully prevents communication within the network by emitting radio signals in the same frequency as that of the nodes operating in the network. This, in turn, causes tremendous increase in the rate of packet drops and also results in very high number of unsuccessful packet re-transmissions. Also, as WSNs are heavily resource-constrained in nature, jamming in WSNs results in faster depletion of the residual energy level of the nodes and an eventual network failure.

Manuscript received January 10, 2017; revised June 8, 2017; accepted July 23, 2017. Date of publication August 7, 2017; date of current version April 16, 2018. The associate editor coordinating the review of this paper and approving it for publication was A. Nallanathan. *(Corresponding author: Sudip Misra.)*

The authors are with the Department of Computer Science & Engineering, IIT Kharagpur, Kharagpur 721302, India (e-mail: pbbhavathankar@gmail.com; chatterjeesubarna@yahoo.com; smisra@sit.iitkgp.ernet.in).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2017.2736550

In this work, we investigate the problem of avoiding the *jammer-affected* zone of a WSN and address the problem of re-establishing routing connectivity among the other non-jammed nodes of the network. We present the underlying motivation and contribution of this work in the following subsections.

A. Motivation

Recent research has already proposed several techniques to detect jammers [12], [13] and ameliorate the consequent effects [14]–[16]. However, in each of the countermeasure techniques, there are some difficulties while practically implementing them in a real-life situation involving a static WSN, in the presence of a proactive-jammer. As per the work of Mpitziopoulos *et al.* [17], the difficulties encountered with the proposed countermeasures are briefly discussed as follows:

- *Regulated Transmitted Power:* This technique requires a sensor node to increase the power of the transmitter as a resistant measure against the jammer. However, such nodes with the ability to regulate their transmission power is highly rare and vendor-specific, thereby questioning the generality of applicability of this solution.
- *Spread Spectrum Methods:* In Frequency-Hopping Spread Spectrum ((FHSS) transmission, the sensor node must possess compatible hardware to enable frequency switching and a very high bandwidth is required, compared to single frequency transmission. Another approach is the usage of the Direct Sequence Spread Spectrum (DSSS) method to detect jamming. As mentioned in the work of Spuhler *et al.* [12], the work focuses on the estimation of the packet delivery ratio. From the estimated value of the ratio, the work aims to detect the presence of jammers. The work targets to take the advantage of IEEE 802.15.4 standard by which it is possible to study the preamble for

signal synchronization, and generate apriori knowledge about the first few bits of the signals. However, the major drawback of DSSS transmission comes with reduced chip rate (2 Mchip/sec) and limited transmission power of the sensor nodes.

- *Directional Transmission:* The primary disadvantage of the use of this technique in WSNs is that in many cases, the nodes are required to multicast or broadcast data packets based on topological requirement. In such scenarios, directional transmission will not anti-jam the network. Azim *et al.* [18] focused on addressing the problem of controlling jammed zones in a WSN. The work determines the knowledge of the perimeter of the jammed zone and uses mapping routines within the zones. Eventually, the work determines the radius vector and calculates the point where the message notification process should terminate. As mentioned earlier, this approach would end up in flooding with too many broadcast messages within the jammed zone. This can lead to extreme erroneous results as the nodes within the jammed area become too noisy and it also exhausts the battery life of the nodes.
- *Ultra Wide Band Technology:* This technology allows a node to transmit short pulses within a large frequency spectrum, thereby disabling signal interception. Oppermann *et al.* focused on the architectural aspects of ultra wide band based sensor networks. However, such a technological approach has limitations related to increased power consumption and energy consumption.
- *Complex System Setup:* Some of the systems have an extremely complex setup and hardware dependencies that make such systems difficult to be incorporated in practical scenarios. For example, Sedehi *et al.* [15] focused on jamming detection and cancellation using airborne/spaceborne radar equipped systems. The characterization and the performance of the work depends highly on the degrees of freedom of the auxiliary beams used for detection of the jammer. The limitation of the work is multifold. Firstly, the radar based setup with multiple channels will have an increased complexity in practical systems requiring high power supplies. The number of auxiliary beans to be used largely depends on the the gain factor of the main antenna of the radar. Further, the selection of the degrees of freedom is significantly complex subjected to the intensity of the disturbance created by the jammer.

Thus, from the list of afore-mentioned limitations, it is evident that a holistic anti-jamming technique is yet to be designed and implemented. Further, when a jammer emits jamming signals, based on the strength of the emitted signal, a subset of nodes in the network becomes completely clogged. Therefore, data packets transmitted by these nodes are simply dropped. Also, packets destined for these jammed nodes cannot be delivered. In the latter scenario, sender nodes continuously engage themselves in repeated packet retransmissions, which eventually results in heavy depletion of energy resource of the nodes and reduction of the network lifetime. This eventually leads to the dysfunctioning of the network.

B. Contribution

This work focuses on ensuring the proper functioning of the WSN in the presence of jamming. The idea is to preserve the residual part of the network from collapsing when only a subset of the nodes is jammed. We consider a static WSN subjected to the attacks of a proactive jammer. Depending on the turbulence in the network or the intensity of jamming, we detect the jammed zone and create alternate routes for the other nodes of the network by bypassing the jammed zone. The work assumes the fallibile nature of the sensor nodes, thereby orienting the proposed problem to fit in well with the real-life scenarios and excluding the loss of generality.

The contributions of this work are briefly listed as follows:

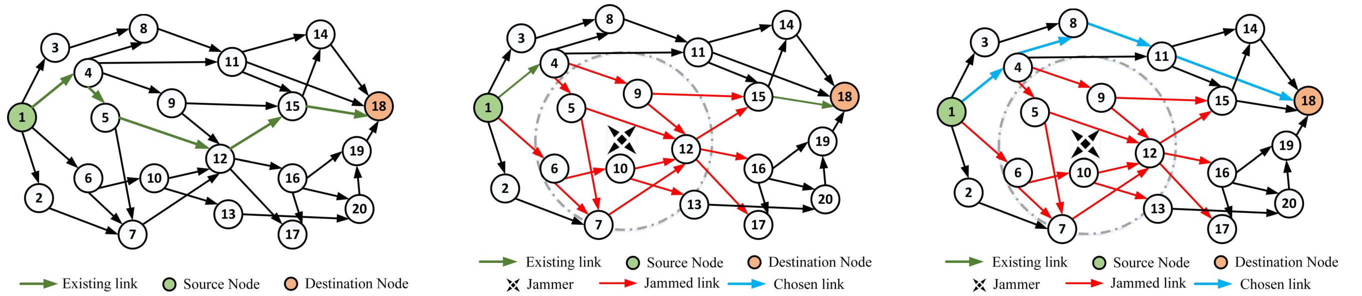
- The work proposes *Link-quality Aware Path SElection* (*LAPSE*) algorithm that focuses to choose an alternative path based on link quality. When an existing route between a source and a destination is partly or fully jammed, another path is chosen such that the component links of the path provide an optimal link quality.
- In order to select the optimal path, the work executes an algorithm that chooses an *Optimal Decision Rule* (*ODR*) [19]. The Rule maximizes the payoff in terms of the link quality, and hence, the path quality, and reduces the error incurred due to incorrect decision making.
- Finally, the performance of LAPSE is evaluated from both mathematical and network perspectives. In the former, the details of implementation of the ODR is thoroughly studied and analyzed, whereas, in the latter, the variation of the network metrics, viz. packet delivery rate, network throughput, transmission energy, node lifetime, and network lifetime are thoroughly analyzed.

C. Organization

The rest of the paper is organized as follows. Section II highlights the existing state-of-the-art. Section III illustrates a problem scenario of the proposed work with diagrammatic examples. In Section IV, we describe the system model and state the proposed formulation of the problem. The details of the proposed solution are described in Section V. The performance of the proposed solution is studied in Section VI. Finally, Section VII concludes the work and discusses the scope of future research.

II. Related Work

Jamming is a well explored area in sensor networks [18], [20], [21]. Large number of works have already investigated the problem of detecting jamming [22], [23]. Patel *et al.* [24] determined the type of geographically correlate links. The authors proposed ways to prevent network disruptions after jamming by modeling the jamming effects using adaptive energy threshold. Some works also focused on the interference caused in the presence of a jammer [25]–[28]. Yuan *et al.* [29] addressed the problem of channel direction information (CDI) in a cognitive radio system. The authors focused on designing a line of sight channel between the secondary transmitter and the primary receiver to resolve the issue. Similar to this, Noam *et al.* [30]



(a) Initial scenario (b) Jammer detected (c) Process of selection of alternative path

Fig. 1. Depiction of the problem scenario in phases.

proposed the technique based on null space learning in a two-user receiver-transmitter pair and Zhao *et al.* [31] proposed a relay-assisted method to obtain the cross-channel gain thereby reducing the interference.

Some works have addressed the problem of jamming-aware routing [32]–[35]. Tague *et al.* [36] proposed a scheme for jamming-aware traffic allocation by the source node using the portfolio selection theory. However, for the purpose of traffic allocation, initially, the impact of jamming is assessed—a problem which is computationally intensive and time-consuming. Further, Tague *et al.* [37] addressed the problem of determining the maximum network throughput in the presence of the jammer. They have introduced the probabilistic jamming into the network flow problem and used portfolio theory to provide a framework for throughput optimization under probabilistic jamming. Lee and Lim [38] analyzed how a routing protocol experiences degradation of throughput in the presence of a jammer. Parissidis *et al.* [39] proposed a model to analyze the effects of interference on data reception probability. The model estimates the probability of a packet to reach the receiver's end in the presence of interference. The work takes into account the node degree, transmission probability, radio propagation, and network card reception sensitivity. Sheikholeslami *et al.* [40] have studied the energy considerations in multi hop networks in the presence of jammer. Yoon and Ko [41] addressed the problem of reliable delivery of data in the presence of a jammer.

Synthesis: None of the works has further used the analytical information in canceling the effects of jamming or in designing an alternative route between a source-destination pair in the presence of jamming.

As per some of the prior works mentioned earlier, it is observed that Spuhler *et al.* [12] focused on the estimation of the packet delivery ratio for detection of jamming. The work targets to take the advantage of IEEE 802.15.4 standard during the signal synchronization phase, and generate apriori knowledge about the first few bits of the signals. Sedehi *et al.* [15] focused on jamming detection and cancellation using airborne/spaceborne radar equipped systems in which characterization and the performance of the work depends highly on the degrees of freedom of the auxiliary beams used for detection of the jammer. The limitation of the work is that the number of auxiliary beans to be used largely depends on the the gain factor of the main antenna of the radar. Further, the selection of the degrees of freedom is significantly complex subjected to the intensity of the disturbance created by the jammer. Azim *et al.* [18] addressed the problem of controlling jammed zones in a WSN. The work determines the knowledge of the perimeter of the jammed zone and uses mapping routines within the zones. Eventually, the work determines the radius vector and calculates the point where the message notification process should terminate. As mentioned earlier, this approach would end up in flooding with too many broadcast messages within the jammed zone. This can lead to extreme erroneous results as the nodes within the jammed area become too noisy and it also exhausts the battery life of the nodes.

Considering the limitations of the work done so far, this paper focuses to provide a software-based solution to control the effects of jamming in a WSN. In presence of jamming, the work aims to select an alternative path between a given source and destination based on the optimal link quality. This path can be used to bypass the jamming-affected zone thereby, preventing unnecessary transmission of broadcast messages and subsequent packet drops.

III. Problem Scenario

In this Section, we describe the problem scenario of the proposed work with an example. As shown in Figure 1, we illustrate the scenario as the different phases of the problem. Initially, let us assume that we have an underlying WSN, as shown in Figure 1(a). For the sake of exemplification, we consider a single source (node 1) and a single destination (node 18). The conventional route from node 1 to 18 is shown in the figure.

Now, after a certain time interval, let us assume that the network is intercepted by the presence of a jammer, as indicated in Figure 1(b). The jammer jams a subset of nodes in the network based on its power and radius of influence. Therefore, all the links involving these affected nodes break and these nodes become unreachable. Now, some the affected nodes are part of the path that connects nodes 1 and 18. Thus, the previous path that connected the source and the destination can not be used any more. In such a scenario, the source node, however, keeps re-transmitting packets and this results in heavy flooding of the network that eventually results in network disruption.

The proposed work addresses the afore-mentioned problem and focuses to select an alternative path between the source and the destination. The work is based on ODR that determines a decision rule that would help to choose that path with the optimum link quality as illustrated in Figure 1(c). During the jamming-affected time period, this path can be used to route and forward packets from node 1 to node 18. Thus, the objective of the proposed work can be visualized to essentially determine a particular decision rule that successfully chooses the best path best on link-quality.

IV. System Model

In this Section, we thoroughly discuss the proposed system model. Table I is a notation table that illustrates the significant functions and variables used in the proposed system.

We consider a WSN comprising of a set of n nodes or vertices, $V = \{v_1, v_2, \cdots, v_n\}$, and a set of edges, E. For any pair of vertices, (v_i, v_j), $1 \le i, j \le n, i \neq j$, an edge, if exists, is indicated as $v_i \to v_j$. Also, $v_i \to v_j \not\Leftrightarrow v_j \to v_i$, i.e., the edges are directed.

A. Assumptions of the Model

(i) The underlying WSN is static in nature.

(ii) The jammer is static in nature, and the absolute coordinates of the jammer, (x_J, y_J), are known a priori.*

(iii) Every node has its own decision making ability which may be imperfect on a temporal basis.

(iv) It is more probable for node v_i to approve a good path than that of disapproving it, and disapprove a bad path than that of approving it.

From the existing work of Boano *et al.* [45], a link quality metric, $Q_{i,j}$, is obtained for every link $v_i \to v_j \in E$, using the *Triangle Metric*, as,

$$Q_{i,j} = \sqrt{\overline{SNR}_{i,j}^2 + \overline{RSS}_{i,j}^2} \tag{1}$$

where $\overline{SNR}_{i,j}$ and $\overline{RSS}_{i,j}$ are the mean Signal-to-Noise-Ratio (SNR) and the mean Received Signal Strength (RSS) of link $v_i \to v_j$, respectively. The values of $\overline{SNR}_{i,j}$ and $\overline{RSS}_{i,j}$ are computed as,

$$\overline{SNR}_{i,j} = \frac{\sum_{s=1}^{b} snr_{i,j}^{s}}{a} \tag{2}$$

$$\overline{RSS}_{i,j} = \frac{\sum_{s=1}^{b} rss_{i,j}^{s,v_j}}{a}, \quad \text{where, } rss_{i,j}^{s,v_j} = \psi_s \frac{P_s^{tr}}{\xi(v_i, v_j)^a} \tag{3}$$

where $snr_{i,j}^{s}$ is the SNR of the link $v_i \to v_j$ while transmitting the s^{th} packet and b out of a packets have been successfully transmitted over link $v_i \to v_j$ [45].† $rss_{i,j}^{s,v_j}$ is the RSS at node v_j for reception of the s^{th} data packet [48], [49]. P_s^{tr} is the transmitted power, ψ_s comprises of all the other factors affecting RSS of the s^{th} packet such as the antenna gain and antenna height, ξ computes the Euclidean metric between v_i and v_j, and a denotes the propagation constant. It is to be additionally noted that, both $\overline{SNR}_{i,j}$ and $\overline{RSS}_{i,j}$ are expressed in dB. A traversal path, P, starting at vertex v_x and ending at vertex v_y, with one or more intermediate vertices in between, is expressed as $P : (v_x, \cdots, v_y)$.

Definition 1: If $Q_{i,j}$ is the quality of a link $v_i \to v_j$, for any $k-$vertex path $P : (v_{\epsilon_1}, v_{\epsilon_2}, \cdots, v_{\epsilon_k})$, the path quality of P, Q_P, is obtained as the summation of the quality of the component links of P. Q_P is expressed as,

$$Q_P = \sum_{i=1}^{k-1} Q_{\epsilon_i, \epsilon_{i+1}} \tag{4}$$

B. Problem Formulation

A pictorial demonstration of problem scenario is depicted in Figure 1. The WSN is subjected to the presence of a static and proactive jammer, J, because of which a subset of edges of the network are affected. Given a source vertex, v_s, and a destination vertex, v_d, the problem is to select the optimal path, $\hat{P} : (v_s, \cdots, v_d)$, from v_s to v_d, in presence of J, so that the path quality achieved through $\hat{P}$, $Q_{\hat{P}}$, is maximized. Let $P_{s,d}$ be the set of p possible paths between v_s and v_d obtained through conventional path exploration techniques [50], [51]. Path $P_i \in P_{s,d}$ comprises of k_i number of intermediate vertices, $1 \le i \le p$. Mathematically, we have,

$$\begin{aligned} P_{s,d} = \Big\{ & P_1 : (v_s, v_{\epsilon_{1,1}}, v_{\epsilon_{1,2}}, \cdots, v_{\epsilon_{1,k_1}}, v_d), \\ & P_2 : (v_s, v_{\epsilon_{2,1}}, v_{\epsilon_{2,2}}, \cdots, v_{\epsilon_{2,k_2}}, v_d), \ldots, \\ & P_p : (v_s, v_{\epsilon_{p,1}}, v_{\epsilon_{p,2}}, \cdots, v_{\epsilon_{p,k_p}}, v_d) \Big\} \end{aligned} \tag{5}$$

Using Equation (4), the path quality P_i is obtained as,

$$Q_{P_i} = Q_{s,\epsilon_{i,1}} + \sum_{l=1}^{k_i - 1} Q_{\epsilon_{i,l}, \epsilon_{i,l+1}} + Q_{\epsilon_{i,k_i}, d} \tag{6}$$

As the goal of the work is to select the path with the maximum quality, the objective function is denoted as $f : P_{s,d} \to \hat{P}$, such that,

$$Q_{\hat{P}} = \arg\max \left\{ Q_{P_i} \right\}, 1 \le i \le p \tag{7}$$

Having described the formal problem statement of the proposed work, we discuss the system model and the approach followed to obtain the solution.

*Regarding the assumption of the a priori knowledge of the coordinates of the jammer, we would like to mention that practically, it is difficult to simply know the coordinates of the jammer. However, as per the current state-of-the-art, there are a lot of works that focus on the localization strategies of one or more jammers [42]–[44]. The proposed work implements one of these strategies [42] before executing the proposed algorithm LAPSE to get the knowledge of the coordinates of the jammer. Based on this knowledge, LAPSE is executed to selected the optimal link-quality aware alternative path between a given source and a destination.

†As far as the probability distribution of the SNR values are concerned, it is very challenging to determine the exact Cumulative Distribution Function (CDF) of the link SNR values. However, from the range of the magnitude of the estimated link SNR values obtained using Equation (2), the probability distribution can be assumed to fit the Pearson System of Approximation. As indicated by the results of the works of Song *et al.* [46], [47], it can be observed that the probability distribution function of the SNR values obtained through Pearson Approximation tends very closely to that when computed using the Triangle Metric mentioned in the work of Boano *et al.* [45].

TABLE I
TABLE OF NOTATION

Parameters	**Values**
n	Number of nodes in the WSN
v_i	A single vertex i
$SNR_{i,j}$	Signal-to-Noise Ratio (SNR) of the link $v_i \rightarrow v_j$ for transmitting the s^{th} packet
$RSS_{i,j}$	Mean Received Signal Strength (RSS) of the link $v_i \rightarrow v_j$ for transmitting the s^{th} packet
$\overline{SNR_{i,j}}$	Mean SNR of link $v_i \rightarrow v_j$
$\overline{RSS_{i,j}}$	Mean RSS of link $v_i \rightarrow v_j$
P^s_{tr}	Power with which the s^{th} packet was transmitted
$\xi(v_i, v_j)$	Computes the Euclidean metric between v_i and v_j
$P : (v_x, \cdots, v_y)$	Path from v_x to v_y
$\mathcal{Q}_{i,j}$	Quality of link $v_i \rightarrow v_j$
$\mathcal{Q}_P$	Quality of path P
J	Jammer node
$P_{s,d}$	Set of possible paths between source v_s and destination v_d
P_{nom}	Set of nominated paths, $P_{nom} \subset P_{s,d}$
$\mathcal{C}$	Committee of decision makers of LAPSE
$\mathcal{P}(1:1)$	Payoff associated with approval of a good path
$\mathcal{P}(-1:-1)$	Payoff associated with disapproval of a bad path
$d^{x,y}_i$	Decision of node v_i for the link $v_x \rightarrow v_y$
$d^{P_l}_i$	Decision of node v_i for the path P_l
$\mathcal{D}_{P_l}$	Decision profile for path P_l
$\mathcal{M}$	Set of all decision profiles
f	Decision rule
F	Set of decision rules
W^1_{i,P_l}	Event of approving or disapproving path P_l by node v_i
$W^2_{P_l}$	Event of path P_l being “good” or “bad”
λ^+_{i,P_l}	Probability of approving a good path
λ^-_{i,P_l}	Probability of disapproving a bad path
$\lambda^{-'}_{i,P_l}$	Type I error
$\lambda^{+'}_{i,P_l}$	Type II error
$\delta_{a,b}(t)$	Packet delivery rate of the link $v_a \rightarrow v_b$ at time t
$\mathcal{G}^{s,d}_{a,b}$	Goodness of link $v_a \rightarrow v_b$ for source vertex v_s and destination vertex v_d
$\mathcal{G}^{s,d}_{P_l}$	Goodness of path P_l for source vertex v_s and destination vertex v_d
$\bar{\mathcal{G}}^{s,d}_{a,b}$	Badness of link $v_a \rightarrow v_b$ for source vertex v_s and destination vertex v_d
$\bar{\mathcal{G}}^{s,d}_{P_l}$	Badness of path P_l for source vertex v_s and destination vertex v_d
$P(W^1_{i,v_a \rightarrow v_b} = 1)$	Probability of approving link $v_a \rightarrow v_b$ by v_i
$P(W^1_{i,v_a \rightarrow v_b} = -1)$	Probability of disapproving link $v_a \rightarrow v_b$ by v_i
$\mathcal{Y}^{f+}_{P_l}$	Partition of decision profiles over which the outcome of the decision rule f is positive
$\mathcal{Y}^{f-}_{P_l}$	Partition of decision profiles over which the outcome of the decision rule f
$P^{P_l f+}_{\mathcal{C}}$	Probability with which $\mathcal{C}$ approves P_l under f
$P^{P_l f-}_{\mathcal{C}}$	Probability with which $\mathcal{C}$ disapproves P_l under f
$\mathcal{Q}_{\mathcal{C}}$	Final profit of the committee in terms of path quality
α	Proportion of good paths
$\zeta(\mathcal{D}_{P_l} : 1)$	Probability of P_l to be approved using $\mathcal{D}_{P_l}$
$\zeta(\mathcal{D}_{P_l} : -1)$	Probability of P_l to be disapproved using $\mathcal{D}_{P_l}$

V. Proposed Solution

Motivated by the ODR [19] as proposed by Ben-Yashar and Nitzan, we consider the *general pairwise choice framework* and apply it to the underlying WSN in presence of the jammer.

A. Optimal Group Decision Rule

The general pairwise choice framework is utilized in economic and financial organizations, in which human fallibility is considered. The framework considers that while making a decision, the decision makers may commit mistakes subjected to the variable fallibility of human behavior. Consequently, the decision incurs a profit or a loss based on the alternative chosen. For example, if a project is to be accepted (or rejected) by a committee of *n* members, there can be four “alternative-states of nature” [19] associated with the acceptance (or rejection) of a good (or bad) project. The ODR takes into account the different probabilistic possibilities of a decision thereby, formulating the expected payoff of the committee. Eventually, the decision rule that maximizes the expected payoff is selected among all the alternatives. Such a rule is termed as a *optimal decision rule* (ODR).

In this work, the ODR is analogously used in the proposed algorithm *Link-quality Aware Path SElection* (*LAPSE*). LAPSE selects the optimal link quality-aware path between a pair of nodes within a WSN in the presence of a jammer.

B. Outline of the Solution Approach

In this subsection, we would present a brief outline of the ODR used in the proposed work. As mentioned earlier, the goal of the proposed LAPSE algorithm is to select an alternative path based on optimal link-quality in a jammer-affected scenario. LAPSE is thoroughly based on ODR in which a subset of the underlying nodes of the WSN comprise the committee of electors and a reduced subset of the set of all potential paths from a source to the destination comprise the set of candidates that are being voted. Every member of the committee votes for every candidate. The votes obtained from every committee member are eventually aggregated to select the path with the optimal link-quality.

The following subsection discusses the detailed mathematical model of LAPSE. The first phase comprises of the selection of the committee of voters. Followed by this, the general pairwise choice framework of the ODR is presented. It specifies the internal details of modeling the payoffs, the decision making skills of every node, and the rationale behind the decision taken by every node. Every committee member votes for each link of a nominated path. The votes of the component links of a nominated path are combined to determine the vote of the path for each committee member. These votes are outcomes of the probabilistic decision making skills of every node as mentioned in Definitions 2 and 3. The path quality is mathematically computed for every path thereby forming the set of nominated paths, i.e., the set of candidates to be voted. Also, for every nominated path, a metric of "goodness" and "badness" are defined in Definitions 4 and 5 to quantitatively indicate how decisive it is to included the path as the alternative path between a source and a destination. Eventually, the ODR is modeled that aggregates all the votes for all the nominated paths to selection of a single path. This path, between a given source and destination, is the alternative path that is selected for routing and data forwarding in a jammer-affected scenario.

C. Mathematical Model

We discuss the detailed mathematical model of the proposed work and illustrate the stepwise formation of the optimal decision rule that selects a path with the maximum path quality, as per Equation (7). We envision a subset of nodes, $\mathcal{C}$, of the WSN to constitute a committee where each node approves or disapproves a route $P \in P_{s,d}$, between v_s and v_d, based on its decision making ability.

1) Formation of the Committee: In the proposed algorithm LAPSE, the committee of decision makers is chosen from those nodes that are present within one or more potential routes from v_s to v_d. Therefore, $\mathcal{C}$ is mathematically represented as,

$$\mathcal{C} = \{v_x : v_x \in P_y, P_y \in P_{s,d}\} \tag{8}$$

Thus, every such node, which is a component of a potential route between the source and the destination, is an element of the committee, $\mathcal{C}$. $\mathcal{C}$ is the set of m nodes out of the total nodes.

2) General Pairwise Choice Framework: As per the ODR, for every path $P_l \in P_{s,d}$, there are two potential states of nature – good (+1) or bad (-1). A payoff is incurred by approving or disapproving a good or a bad route. The payoff associated with the approval of a good path by node v_i is denoted by $\mathcal{P}(1 : 1)$ and that with the disapproval of a bad route is denoted by $\mathcal{P}(-1 : -1)$. As the framework of LAPSE considers all possible types of asymmetry, the payoffs associated with approving a bad route and disapproving a good route are also taken into account and are denoted by $\mathcal{P}(1 : -1)$ and $\mathcal{P}(-1 : 1)$, respectively. Having obtained the set of possible paths, $P_{s,d}$ from v_s to v_d, we compute the mean path quality, $\hat{Q}$, over $P_{s,d}$, as:

$$\hat{Q} = \frac{1}{p}\sum_{i=1}^{p} Q_{P_i} = \frac{1}{p}\sum_{i=1}^{p}\left[Q_{s,\epsilon_{i,1}} + \sum_{l=1}^{k_i-1} Q_{\epsilon_{i,l},\epsilon_{i,l+1}} + Q_{\epsilon_{i,k_i},d}\right] \tag{9}$$

Based on the magnitude of $\hat{Q}$, the set of nominated paths P_{nom}, where, $P_{nom} \subset P_{s,d}$, is formed using the conventional path selection techniques [52], [53]. All such paths whose quality is equal to or greater than the mean path quality, constitute the set P_{nom}. Hence, we have,

$$P_{nom} = \{P_k : Q_{P_k} \geq \hat{Q}, P_k \in P_{s,d}\} \tag{10}$$

The rationale to build the set P_{nom} is to reduce the cardinality of set $P_{s,d}$, so that the number of potential candidates of concern, significantly reduces. This also improves the computation time and efficiency.

Every node has its own decision making skill and the decision of a node $v_i \in \mathcal{C}$ is denoted by d_i. $d_i = \{+1, -1\}$ based on its approval or disapproval of a path. Initially, v_i examines every component link $v_x \to v_y$ of a path P_l and assigns a value of $d_i^{x,y} = \{+1, -1\}$ to the link based on the decision criteria:

(a) v_i votes a link $v_x \to v_y$ with -1, if, packet delivery rate, $\delta_{i,y}$, (in packets per second) of the link $v_i \to v_y$, is extremely low or tends to zero, i.e., v_i judges the performance of node v_y, hence link $v_x \to v_y$, from its past experience of data transmission over link $v_i \to v_y$.

(b) If $\delta_{i,y} > 0$, which means v_i has a past history of successful data transmission to v_y, the current Euclidean distance (in meter) of v_y is computed from the jammer, J. Node v_i senses the position v_y and if v_y is found to lie within a threshold distance ξ_{th} from J, $v_x \to v_y$ is voted with -1.

(c) If conditions (a) and (b) fail, $v_x \to v_y$ is voted by v_i with $+1$.

Therefore, we have,

$$d_i^{x,y} = \begin{cases} -1, & \delta_{i,y} \to 0, \quad \text{or } \xi(v_y, J) \leq \xi_{th} \\ +1, & \text{otherwise} \end{cases} \tag{11}$$

In this study, v_i obtains $d_i^{x,y}$ for all component links of P_l and votes positive for P_l, if the sum of the votes for all the links is positive. Otherwise, P_l is negatively voted by v_i. Mathematically,

$$d_i^{P_l} = \begin{cases} -1, & \sum_{\forall v_x \to v_y \in P_l} d_i^{x,y} \leq 0 \\ +1, & \text{otherwise} \end{cases} \tag{12}$$

After obtaining the individual decisions $\forall v_i \in \mathcal{C}$ on path P_l, a decision profile for P_l is constructed, and expressed as,

$$\mathcal{D}^{P_l} = \{d_x^{P_l} : v_x \in \mathcal{C}\}, \mathcal{D}^{P_l} \in \mathcal{M} \tag{13}$$

where $\mathcal{M}$ is the set of all possible decision profiles, $\mathcal{M} = \{1, -1\}^m$.

The proposed system comprises of two specific events, as follows:

1. $W^1_{i,P_l} = \{1, -1\}$: Event of approving or disapproving a path by node v_i
2. $W^2_{P_l} = \{1, -1\}$: Event of path P_l being "good" or "bad"

As per our assumptions, every node is fallible in terms of making a decision. A decision is "correct", if and only if a good path is approved or a bad path is disapproved.

Definition 2: The probability of making a correct decision by node v_i for path P_l is expressed as,

$$\begin{aligned}\Lambda^+_{i,P_l} &= P(W^1_{i,P_l} = 1 \mid W^2_{P_l} = 1) = P(1:1),\\ \Lambda^-_{i,P_l} &= P(W^1_{i,P_l} = -1 \mid W^2_{P_l} = -1) = P(-1:-1)\end{aligned} \quad (14)$$

where Λ^+_i and Λ^-_i are the respective probabilities of approving a good path and disapproving a bad path.

Definition 3: The Type I and Type II errors corresponding to the probabilities of making an incorrect decision due to disapproval of a good path ($\Lambda^{+'}_i$) and approval of a bad path ($\Lambda^{-'}_i$), by node v_i, is expressed:

$$\begin{aligned}\Lambda^{+'}_{i,P_l} &= P(W^1_{i,P_l} = -1 \mid W^2_{P_l} = 1) = P(-1:1),\\ \Lambda^{-'}_{i,P_l} &= P(W^1_{i,P_l} = 1 \mid W^2_{P_l} = -1) = P(1:-1)\end{aligned} \quad (15)$$

The likelihood of approving a good path is higher that disapproving it, i.e., $\Lambda^+_i > \Lambda^{+'}_i$. Similarly, $\Lambda^-_i > \Lambda^{-'}_i$. A decision rule $f()$ accepts a decision profile and outputs $+1$ or -1, based on aggregation. Mathematically, we have, $f : \mathcal{M} \rightarrow \{1, -1\}$. It is imperative to identify whether a path is "good" or "bad" and quantify its "goodness" and "badness".

Definition 4: The "goodness" of a link $v_a \rightarrow v_b$, at time t, with respect to the source node v_s and destination node v_d, is denoted by $\mathcal{G}^{s,d}_{a,b}$, and is defined as the mean of the packet delivery rates of the link for the last h time instants and the mean of Euclidean distance of v_a and v_b from J. Therefore, $\mathcal{G}^{s,d}_{a,b}$ is expressed as,

$$\mathcal{G}^{s,d}_{a,b}(t) = \frac{gp\sum_{t=1}^{h}\delta_{a,b}(t)}{h} \times \frac{\xi(v_a, J) + \xi(v_b, J)}{2}{*} \quad (16)$$

where, $\delta_{a,b}(t)$ is the packet delivery rate of the link $v_a \rightarrow v_b$, at time t, p is the size of each packet (in bits), and g is the normalization constant with unit second meter^{-1} bit^{-1}. Also, $0 \leq \mathcal{G}^{s,d}_{a,b} \leq 1$.

Definition 5: The "goodness" of a path P_l at time t, $\mathcal{G}^{s,d}_{P_l}$, with respect to the source node v_s and destination node v_d, is defined as the product of the goodness of its component links. Therefore, $\mathcal{G}^{s,d}_{P_l}$ is mathematically expressed as,

$$\mathcal{G}^{s,d}_{P_l}(t) = \prod_{\forall v_a \rightarrow v_b \in P_l} \mathcal{G}^{s,d}_{a,b}(t) \quad (17)$$

where, $0 \leq \mathcal{G}^{s,d}_{P_l}(t) \leq 1$.

*In absence of jammer, the values of $\xi(v_a, J)$ and $\xi(v_b, J)$ are considered to be very large to ensure the goodness of every node due to lack of proximity from the jammer.

Analogous to "goodness" of a link, "badness" is complimentary to the "goodness" metric. The "badness" of a link ($\overline{\mathcal{G}}^{s,d}_{a,b}$) is expressed as, $\overline{\mathcal{G}}^{s,d}_{a,b}(t) = 1 - \mathcal{G}^{s,d}_{a,b}(t)$. "Badness" of a path is obtained as, $\overline{\mathcal{G}}^{s,d}_{P_l}(t) = \prod_{\forall v_a \rightarrow v_b \in P_l} \overline{\mathcal{G}}^{s,d}_{a,b}(t)$. However, based on the fallibility of decision making of a node, the probabilistic values of approving or disapproving a path may vary. The probability of approving a path, $P(W^1_{i,P_l} = 1)$, depends on the probability of approving every component link of the path. The probability of approving a link by a node v_i, $v_i \in \mathcal{C}$, is obtained as the ratio of the number of times it approved the link to the total number of times. Therefore, based on the last h time instants, the probability ($P(W^1_{i,v_a \rightarrow v_b} = 1)$) of approving link $v_a \rightarrow v_b$ by v_i, is given by,

$$P(W^1_{i,v_a \rightarrow v_b} = 1) = \frac{\sum_{t=1}^{h}\left(d^{a,b}_i(t) + 1\right)! - 1}{h} \quad (18)$$

where,

$$\left(d^{a,b}_i(t) + 1\right)! - 1 = \begin{cases} 1, & \text{if } d^{a,b}_i(t) = +1 \\ 0, & \text{otherwise} \end{cases} \quad (19)$$

$d^{a,b}_i(t)$ is the decision value given by node v_i for link $v_a \rightarrow v_b$ at time t. Hence, the total probability of approving a path is obtained as,

$$P(W^1_{i,P_l} = 1) = \prod_{\forall v_a \rightarrow v_b \in P_l} P(W^1_{i,v_a \rightarrow v_b} = 1) \quad (20)$$

Following Equations (18) and (20), we directly obtain,

$$\begin{aligned}P(W^1_{i,v_a \rightarrow v_b} = -1) &= 1 - P(W^1_{i,v_a \rightarrow v_b} = 1)\\ &= 1 - \frac{\sum_{t=1}^{h}\left(d^{a,b}_i(t) + 1\right)! - 1}{h}\end{aligned} \quad (21)$$

$$P(W^1_{i,P_l} = -1) = \prod_{\forall v_a \rightarrow v_b \in P_l} P(W^1_{i,v_a \rightarrow v_b} = -1) \quad (22)$$

Using the approach of Bayesian classification for conditional probability [54], [55], we get,

$$\begin{aligned}&\Lambda^+_{i,P_l}\\ &= P\left(\frac{W^1_{i,P_l} = 1}{W^2_{P_l} = 1}\right)\\ &= \frac{P(W^1_{i,P_l} = 1)P\left(\frac{W^2_{P_l}=1}{W^1_{i,P_l}=1}\right)}{P(W^1_{i,P_l}=1)P\left(\frac{W^2_{P_l}=1}{W^1_{i,P_l}=1}\right) + P(W^1_{i,P_l} = -1)P\left(\frac{W^2_{P_l}=1}{W^1_{i,P_l}=-1}\right)}\end{aligned} \quad (23)$$

$$\begin{aligned}&\Lambda^-_{i,P_l}\\ &= P\left(\frac{W^1_{i,P_l} = -1}{W^2_{P_l} = -1}\right)\\ &= \frac{P(W^1_{i,P_l} = -1)P\left(\frac{W^2_{P_l}=-1}{W^1_{i,P_l}=-1}\right)}{P(W^1_{i,P_l}=-1)P\left(\frac{W^2_{P_l}=-1}{W^1_{i,P_l}=-1}\right) + P(W^1_{i,P_l} = 1)P\left(\frac{W^2_{P_l}=-1}{W^1_{i,P_l}=1}\right)}\end{aligned} \quad (24)$$

The Type I and Type II errors corresponding to Equations (23) and (24) are obtained as,

$$\Lambda^{+'}_{i,P_l} = 1 - \Lambda^{+}_{i,P_l}, \quad \Lambda^{-'}_{i,P_l} = 1 - \Lambda^{-}_{i,P_l} \tag{25}$$

Having obtained the conditional probabilities of approving or disapproving a path by a node, it is imperative to select the decision rule that maximizes the payoff of the committee. Initially, we partition the set of all possible decision profiles for path P_l as, $\mathcal{Y}^{f+}_{P_l}$ and $\mathcal{Y}^{f-}_{P_l}$, such that, $\mathcal{Y}^{f+}_{P_l}$ and $\mathcal{Y}^{f-}_{P_l}$ are the sets of those profiles over which the outcome of the decision rule f is positive, and negative, respectively. Thus,

$$\mathcal{Y}^{f+}_{P_l} = \{u \in \mathcal{M} : f(u) = 1\}, \quad \mathcal{Y}^{f-}_{P_l} = \{u \in \mathcal{M} : f(u) = -1\} \tag{26}$$

Let $P^{P_l f+}_{C}$ and $P^{P_l f-}_{C}$ be the respective probabilities with which $\mathcal{C}$ approves or disapproves path P_l under decision rule f. Therefore,

$$P^{P_l f+}_{C} = P(u \in \mathcal{Y}^{f+}_{P_l}), \quad P^{P_l f-}_{C} = P(u \in \mathcal{Y}^{f-}_{P_l}) \tag{27}$$

Therefore, the probability that a decision profile belongs to $\mathcal{Y}^{f+}_{P_l}$ and still gets disapproved is given as $1 - P^{P_l f+}_{C}$ and the probability of a decision profile in $\mathcal{Y}^{f-}_{P_l}$ being approved is $1 - P^{P_l f-}_{C}$. Contextually, it is important to note that the payoff to be maximized is Q_{P_l}, as per Equation (7). The focus of this work is, for a decision rule $f \in F$,

$$\max_{f \in F} Q_{\mathcal{C}} \tag{28}$$

where, $Q_{\mathcal{C}}$ is the final profit of the committee, $\mathcal{C}$. $Q_{\mathcal{C}}$ is expressed as,

$$\begin{aligned} Q_{\mathcal{C}} = \alpha\Big[&\mathcal{P}(1:1)P^{P_l f+}_{C} + \mathcal{P}(-1:1)\big(1 - P^{P_l f+}_{C}\big)\Big](1-\alpha) \\ &\times \Big[\mathcal{P}(-1:-1)P^{P_l f-}_{C} + \mathcal{P}(1:-1)\big(1 - P^{P_l f-}_{C}\big)\Big] \end{aligned} \tag{29}$$

where, α is the proportion of good paths. The magnitude of α is time-variant and can be evaluated based on history. At time instant $h+1$, the magnitude of α is computed as,

$$\alpha(h+1) = \frac{1}{h}\sum_{t=1}^{h} \frac{\sum_{\forall P_k \in P_{nom}} \eta_{P_k}(t)}{\mid P_{nom} \mid} \tag{30}$$

where $\eta_{P_k}(t)$ is the "goodness" indicator of path P_k at time t. $\eta_{P_k}(t)$ is designed as,

$$\eta_{P_k}(t) = \begin{cases} 1, & \text{if } \mathcal{G}^{s,d}_{P_k} \geq \overline{\mathcal{G}}^{s,d}_{P_k} \\ 0, & \text{otherwise} \end{cases} \tag{31}$$

Considering $\mathcal{P}(1) = \mathcal{P}(1:1) - \mathcal{P}(-1:1)$ and $\mathcal{P}(-1) = \mathcal{P}(-1:-1) - \mathcal{P}(1:-1)$ as the respective effective profits due to the approval of a good path and disapproval of a bad path, Equation (29) can be simplified as,

$$\begin{aligned} Q_{\mathcal{C}} = \alpha\mathcal{P}(1)P^{P_l f+}_{C} + (1-\alpha)\mathcal{P}(-1)P^{P_l f-}_{C} + \alpha\mathcal{P}(-1:1) \\ + (1-\alpha)\mathcal{P}(1:-1) \end{aligned} \tag{32}$$

Every decision profile for path P_l is partitioned into two disjoint sets, $\mathcal{A}(\mathcal{D}_{P_l})$ and $\mathcal{R}(\mathcal{D}_{P_l})$, such that,

$$\mathcal{A}(\mathcal{D}_{P_l}) = \{v_x : d^{P_l}_x = 1\}, \quad \mathcal{R}(\mathcal{D}_{P_l}) = \{v_x : d^{P_l}_x = -1\} \tag{33}$$

Given that path P_l is "good", the probability of the path to be approved by the decision profile $\mathcal{D}_{P_l}$ is expressed as,

$$\begin{aligned} \zeta(\mathcal{D}_{P_l}:1) &= \prod_{v_x \in \mathcal{A}(\mathcal{D}_{P_l})} \Lambda^{+}_{x,P_l} \prod_{v_x \in \mathcal{R}(\mathcal{D}_{P_l})} \big(1 - \Lambda^{+}_{x,P_l}\big), \\ \zeta(\mathcal{D}_{P_l}:-1) &= \prod_{v_x \in \mathcal{R}(\mathcal{D}_{P_l})} \Lambda^{-}_{x,P_l} \prod_{v_x \in \mathcal{A}(\mathcal{D}_{P_l})} \big(1 - \Lambda^{-}_{x,P_l}\big) \end{aligned} \tag{34}$$

For a particular decision rule f, we have,

$$\begin{aligned} P^{P_l f+}_{C} &= \sum_{\forall \mathcal{D}_{P_l} \in \mathcal{Y}^{f+}_{P_l}} \zeta(\mathcal{D}_{P_l}:1), \\ P^{P_l f-}_{C} &= \sum_{\forall \mathcal{D}_{P_l} \in \mathcal{Y}^{f-}_{P_l}} \zeta(\mathcal{D}_{P_l}:-1) \end{aligned} \tag{35}$$

Referring to Equation (32), it can be observed that the solution of LAPSE, in turn, maximizes the following:

$$\begin{aligned} \max_{f \in F} \mathcal{P}'_C &= \alpha\mathcal{P}(1)P^{P_l f+}_{C} + (1-\alpha)\mathcal{P}(-1)P^{P_l f-}_{C} \\ &= \alpha\mathcal{P}(1)\sum_{\forall \mathcal{D}_{P_l} \in \mathcal{Y}^{f+}_{P_l}} \zeta(\mathcal{D}_{P_l}:1) + (1-\alpha)\mathcal{P}(-1) \\ &\quad \times \sum_{\forall \mathcal{D}_{P_l} \in \mathcal{Y}^{f-}_{P_l}} \zeta(\mathcal{D}_{P_l}:-1) \end{aligned} \tag{36}$$

Theorem 1: The optimal decision rule $\hat{f}$ of our problem is denoted as:

$$\hat{f} = \sigma\big(\theta + \omega + \gamma + \Psi\big) \tag{37}$$

where,

$$\theta = \ln\frac{\alpha}{1-\alpha}, \quad \omega = \ln\frac{\mathcal{P}(1)}{\mathcal{P}(-1)} \tag{38}$$

$$\begin{aligned} \gamma &= \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^{+}_{x,P_l}}{\big(1-\Lambda^{-}_{x,P_l}\big)}\Big(d^{P_l}_x + 1\Big)! \\ &\qquad - \ln\frac{\Lambda^{-}_{x,P_l}}{\big(1-\Lambda^{+}_{x,P_l}\big)}\Big(1 - d^{P_l}_x\Big)!\Bigg], \end{aligned}$$

$$\Psi_x = \ln\frac{\Lambda^{-}_{x,P_l}\big(1-\Lambda^{-}_{x,P_l}\big)}{\Lambda^{+}_{x,P_l}\big(1-\Lambda^{+}_{x,P_l}\big)}, \ \Psi = \sum_{x=1}^{m}\Psi_x \tag{39}$$

$$\sigma(a) = \begin{cases} 1, & \text{if } a > 0 \\ 0, & \text{otherwise} \end{cases} \tag{40}$$

Proof: The proof is illustrated in Appendix. ■

Finally, the algorithmic representation of LAPSE is also indicated through Algorithm 1.

VI. PERFORMANCE EVALUATION

In this Section, we discuss the performance evaluation of the proposed algorithm LAPSE. The study is performed under

Algorithm 1 LAPSE: Link-Quality Aware Path SElection

Input: Source node: υ_s,
Destination node: υ_d,
Absolute coordinates of the jammer: (x_J, y_J),
Set of p possible paths between υ_s and υ_d: $P_{s,d}$
Output: Optimal decision rule: $\hat{f}$

Form the committee $\mathcal{C}$, using Equation (8)
for $P_k \in P_{s,d}$ **do**
  Compute Q_{P_k}
Compute $\hat{Q}$
Build P_{nom} using Equation (10)
for $P_l \in P_{nom}$ **do**
  for $\upsilon_i \in \mathcal{C}$ **do**
    for $\upsilon_x \rightarrow \upsilon_y \in P_l$ **do**
      Compute $d_i^{x,y}$
    Compute $d_i^{P_l}$
    Compute Λ^+_{i,P_l}, Λ^-_{i,P_l}, $\Lambda^{+'}_{i,P_l}$, $\Lambda^{-'}_{i,P_l}$
  Build $\mathcal{D}_{P_l}$
for $P_l \in P_{nom}$ **do**
  for $\upsilon_a \rightarrow \upsilon_b \in P_l$ **do**
    Compute $\mathcal{G}^{s,d}_{a,b}(t)$
  Compute $\mathcal{G}^{s,d}_{P_l}(t)$ and $\hat{\mathcal{G}}^{s,d}_{P_l}(t)$
  Compute $P_C^{P_l f+}$ and $P_C^{P_l f-}$
Compute $\hat{f}$ as per Equation (37)

three distinct subsections. In the first subsection, we analyze the proposed scheme from a mathematical perspective and justify the correctness of the applicability of ODR in this regard. In the second subsection, we study and discuss the performance of the algorithm in terms of the network parameters. In the third subsection, we thoroughly present an asymptotic analysis of the time complexity of the algorithm.

Experimental Setup

For the purpose of experimentation, we consider a uniform random deployment of 100 wireless sensor nodes over an area of 1000 m $\times$1000 m. Each node is assumed to communicate over Zigbee protocol (IEEE 802.15.4) within a communication range varying from 50 to 100 meter. The energy expended due to transmission and computation is considered as 7 nJ/bit and 5 nJ/sec, respectively [49]. The size of every packet transmitted and received is considered to be 128 byte. Using Network Simulator, such a network is simulated for 100 time units. The jamming effect is considered to be randomly initiated between the 30^{th} and the 60^{th} time instant. We also take into into account white Gaussian noise with unit variance. For computing the coordinates of the jammer, we chose three existing schemes on jammer localization [42]–[44] and then compare the accuracy of the estimation of the coordinates as shown in Tables III and IV. After a thorough analysis, the work of Liu *et al.* [42] is chosen as it has the closest estimation of the jammer localization. The experimental setup is also provided in a tabular format in Table II followed by a detailed analysis the subsequent subsections.

TABLE II
EXPERIMENTAL SETUP

Parameters	Values
Deployment Area	1000 m $\times$ 1000 m
Deployment	Uniform, random
Number of nodes	100
Communication range	$[50, 100]$ m
Channel overhead	$[1, 5]\%$
Transmission energy	7 nJ/bit [49]
Computation energy	5 nJ/sec [49]
Packet Size	128 byte

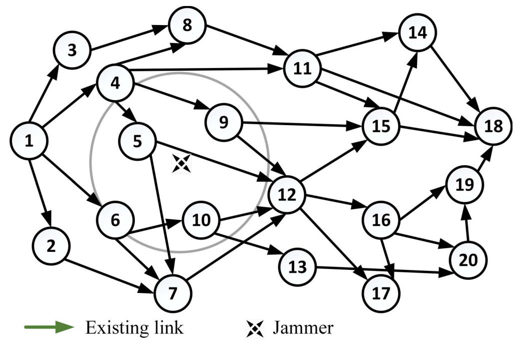


Fig. 2. Sample graph for analysis.

A. Mathematical Perspective (A Case Study)

In this subsection, we analyze the implementation of the ODR and the process of selecting a path, eventually. For the purpose of the case study, we consider a connected graph, as shown in Figure 2 comprising of 20 vertices and 34 edges, and the position of the jammer as indicated. The source and the destination node for packet transmission is considered to be 1 and 18, respectively. Initially, the route between the nodes 1 and 18 is $1 \rightarrow 4 \rightarrow 9 \rightarrow 15 \rightarrow 18$. However, in the presence of jammer, using Equation (10), we consider the set of nominated paths as $P_{nom} = \{1 \rightarrow 3 \rightarrow 8 \rightarrow 11 \rightarrow 14 \rightarrow 18, 1 \rightarrow 4 \rightarrow 11 \rightarrow 14 \rightarrow 18, 1 \rightarrow 4 \rightarrow 8 \rightarrow 11 \rightarrow 14 \rightarrow 18, 1 \rightarrow 2 \rightarrow 7 \rightarrow 12 \rightarrow 15 \rightarrow 18, 1 \rightarrow 2 \rightarrow 7 \rightarrow 12 \rightarrow 16 \rightarrow 19 \rightarrow 18\}$.

Before executing the ODR, we evaluate the link parameters as shown in Figure 3 using Equations (1) through (3). For every nominated path, the intermediate SNR, intermediate RSS, and intermediate link quality were determined using the definitions as follows:

Definition 6: For a path $P_i : \upsilon_{\epsilon_1}, \upsilon_{\epsilon_2}, \cdots, \upsilon_{\epsilon_k}$, the intermediate SNR ($\overline{SNR}'_j$) at link $\upsilon_{\epsilon_{j-1}} \rightarrow \upsilon_{\epsilon_j}$, is computed as the summation of the mean SNR of all the links preceding and including $\upsilon_{\epsilon_{j-1}} \rightarrow \upsilon_{\epsilon_j}$ of P_i. Mathematically,

$$\overline{SNR}'_j = \sum_{\forall \upsilon_{\epsilon_x} \in \{\upsilon_{\epsilon_1}, \cdots, \upsilon_{\epsilon_{j-1}}\}} \overline{SNR}_{\epsilon_x, \epsilon_{x+1}}$$

TABLE III
ESTIMATION OF ABSCISSA OF THE JAMMER

	Original value of abscissa	Values estimated		
		Liu et al. [42]	Cheng et al. [43]	Wang et al. [44]
X_1	40.23	40.18	41.44	40.02
X_2	100.876	100.867	101.991	100.202
X_3	512.674	512.422	510.644	512.999
X_4	874.335	874.110	875.906	875.432
X_5	899.901	899.967	898.112	899.457

TABLE IV
ESTIMATION OF ORDINATE OF THE JAMMER

	Original value of ordinate	Values estimated		
		Liu et al. [42]	Cheng et al. [43]	Wang et al. [44]
Y_1	16.561	16.143	17.943	17.412
Y_2	93.176	93.897	91.866	94.992
Y_3	533.984	534.102	532.423	534.739
Y_4	751.941	752.110	750.766	751.102
Y_5	957.017	956.857	958.202	958.987

and

$$\overline{RSS}'_j = \sum_{\forall v_{\epsilon_x} \in \{v_{\epsilon_1}, \cdots, v_{\epsilon_{j-1}}\}} \overline{RSS}_{\epsilon_x, \epsilon_{x+1}} \tag{41}$$

$$\overline{Q}'_j = \sum_{\forall v_{\epsilon_x} \in \{v_{\epsilon_1}, v_{\epsilon_2}, \cdots, v_{\epsilon_{j-1}}\}} Q_{\epsilon_x, \epsilon_{x+1}} \tag{42}$$

Using Equations (41) and (42), we compute the intermediate metric values of all the nominated paths 1 through 5, as illustrated in Figures 3(a) through 3(e), respectively. Now, having obtained the SNR and the RSS values of the all the links of the different nominated paths, the decision rule is evaluated using Equation (37). Once the decision rule is obtained, the rule is applied over all the paths and the inequality condition is checked as illustrated in Equations (50) and (50). After validation of the condition of the decision rule on the paths, path 5 was observed to get through the condition and hence, is selected as the path with the optimal quality. This is also indicated through Figure 3(e), where we observe that the link quality for the last link is above 7 dB unlike the links of other paths. Thus, the decision rule that selects path 5 is optimal and hence selected.

It may be observed that path 5 comprises of 6 links, whereas the other paths consist of 4 to 5 links. Therefore, cumulation of the metrics might seem to be obvious for enhancement of performance for path 5. For the purpose of further validation of the decision rule, the mean SNR and RSS values of the nominated paths were minutely studied for 50 time instants. In Figure 4(a), it is observed that, path 5 possesses a significantly high SNR and RSS, compared to paths 1, 2, 3, and 4 with 95% confidence. The path quality is also analyzed over the 50 time instants, as shown in Figure 4(b). It is observed that although the 95% confidence interval of the link quality is the widest for path 5 ([0.96, 1.101]), the mean link quality is higher in case of path 5 compared to the other nominated paths. The study of the implementation of the ODR was further extended by investigating the effects of the packet delivery rate of the paths on the overall link quality of the optimal path. Figure 4(c) depicts the variation of the mean packet delivery rate, δ, on the path quality, which is plotted along the secondary axis. We observe that with the increase in the mean packet delivery rate, the mean link quality also increases. Thus, the packet delivery rate directly influenced the selection of the optimal path.

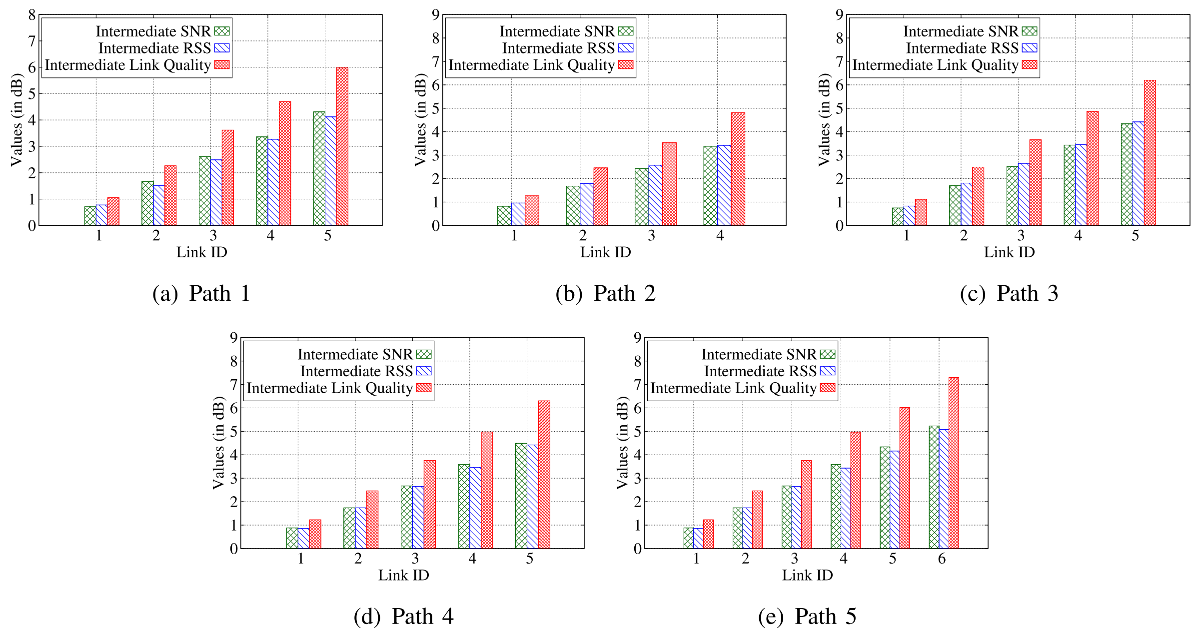
B. Network Perspective

In this subsection we study the performance of the proposed scheme from a network perspective. We compare the proposed algorithm with two different benchmark approaches. In the first approach [21], once jamming occurs, the affected nodes get simply clogged and this results in heavy packet drops and eventual network failure. Here, we compare our proposed technique with the existing scheme and discuss the performance that is achieved. In the second approach [56], the authors focus on alternative path selection strategy based on the link outage probabilities. We also take into account this approach and compare to analyze the better path selection algorithm. For both the benchmark approaches, Figure 5 indicates the variation of the network parameters over time and Figure 6 depicts the percentage of fall or rise in the magnitude of the parameters in comparison to the existing schemes.

Performance Metrics

The metrics used for network performance analysis are the following:

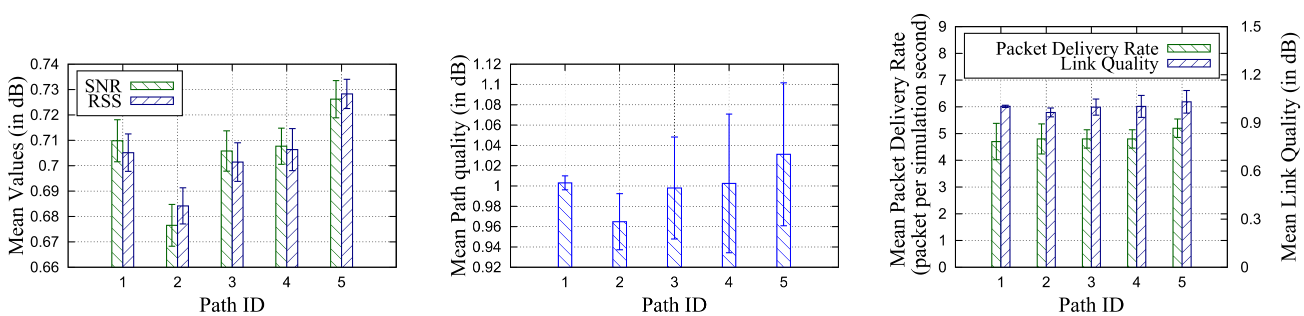
- *Packet Delivery Rate:* The packet delivery rate, δ_t, of the network at time t is computed as the total number of successful packet transmissions between any pair of nodes per unit time. The cumulative packet delivery rate is computed as $\delta^c = \sum_{t=1}^{100} \delta_t$.



(a) Path 1 (b) Path 2 (c) Path 3

(d) Path 4 (e) Path 5

Fig. 3. Analysis of the SNR, RSS, and the Link Quality for the set of the nominated paths.



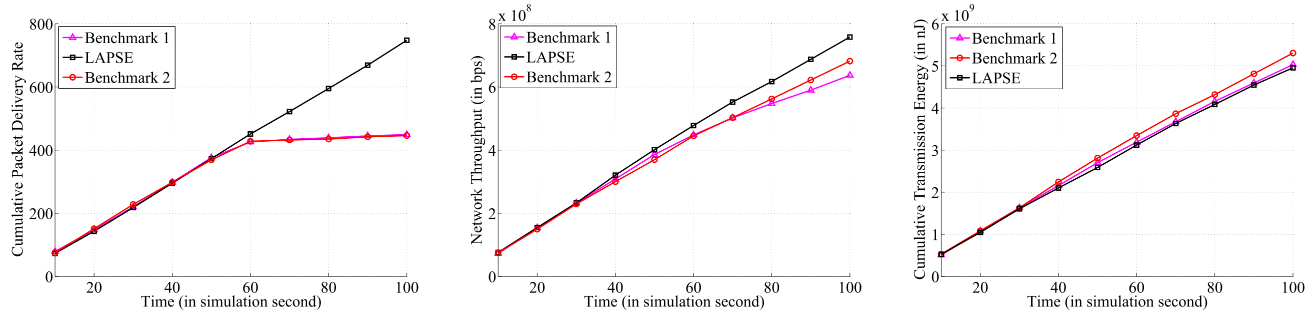
(a) Mean SNR and mean RSS (b) Mean Path Quality (c) Variation of the mean Packet Delivery Rate (δ) and the mean Path Quality

Fig. 4. Study of the mean SNR, mean RSS, mean Path Quality, and variation of the mean Packet Delivery Rate and the mean Path Quality of the nominated paths over 50 time instants.

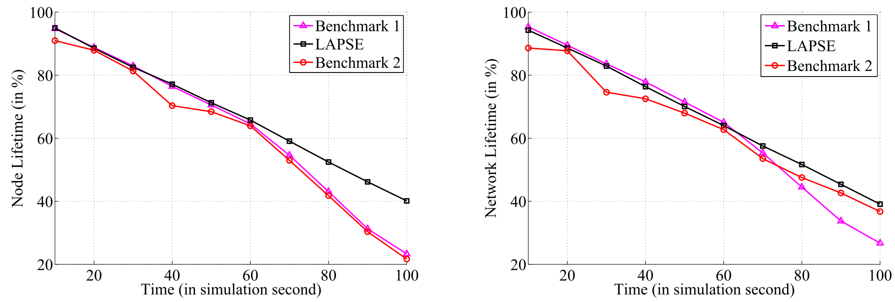
- *Network Throughput:* The throughput of the network at time t, $\mathcal{N}_t$, is directly obtained from the packet delivery rate when converted to bits per second. Therefore, $\mathcal{N}_t = \sum_{i=1}^{n} \delta_{i,t} \times p$, $\mathcal{N}^c = \sum_{t=1}^{100} \mathcal{N}_t$, where p is the packet size, which is considered as 128 bytes, n is the number of nodes in the network, $\delta_{i,t}$ is the packet transmission rate of node i at time t, and $\mathcal{N}^c$ is the cumulative network throughput over time.
- *Transmission Energy:* For evaluation of the transmission energy, $E_{tr\,t}$, at time t, we consider both the transmission and re-transmission attempts of the nodes in the network. Thus, we have, $E_{tr\,t} = \mathcal{N}_t \times E_p$, where E_p the transmission energy per bit. In our work, we considered $E_p = 7$ nJ/bit.
- *Node Lifetime:* The lifetime of a node v_x, at time t, $\mathcal{L}_{v_x\,t}$, is expressed as the ratio of the residual energy (E_t) to the initial energy content of the node (E_{init}) and is expressed as a percentage value. $\mathcal{L}_{v_x\,t} = \frac{E_t}{E_{init}} \times 100\%$
- *Network Lifetime:* The network lifetime, $\mathcal{L}_{N\,t}$, is defined as the cumulation of the lifetime of every nodes, and is expressed as, $\mathcal{L}_{N\,t} = \frac{\sum_{i=1}^{n} \mathcal{L}_{v_i\,t}}{nE_{init}} \times 100\%$.

Performance Analysis

As shown in Figure 5(a), we observe that, in our simulated scenario, the jammer intervention occurs at the 59^{th} time instant after which the packet delivery rate was observed to be negligible for both of the benchmark algorithms and hence, the residual cumulative packet delivery rate remains almost constant over time. On the other hand, using the proposed technique, LAPSE, even after the intervention of the jammer, routes are altered and packets channelized so that the delivery rate is maintained. The consistency of the packet delivery rate under the proposed scheme can also be observed by the rising trend of the cumulative packet delivery rate in Figure 5(a). The corresponding increase of the packet



(a) Comparative analysis of Packet Delivery Rate (b) Comparative analysis of Network Throughput (c) Comparative analysis of Cumulative Transmission Energy



(d) Comparative analysis of Node Lifetime (e) Comparative analysis of Network Lifetime

Fig. 5. Comparative analysis of network parameters for the existing and the proposed scheme.

delivery rate is also reflected in Figure 6(a) which shows the percentage of improvement of the packet delivery rate achieved using the proposed scheme, compared to the benchmark approaches.

In Figure 5(b), it can be observed that the network throughput initially remains almost the same for all the three solutions. After the intervention of the jammer, the throughput considerably falls with the first approach and is slightly better with the second approach as there is a reduced packet delivery rate for the jammer-affected nodes. However, using the proposed technique, as alternative routing paths are established and the packet delivery rates are maintained, the network throughput comparatively increases and achieves a maximum increment by more than 15% as shown in Figure 6(b).

The effects, as shown in Figure 5(b), has a direct influence on the cumulative transmission energy that is reflected in Figure 5(c). It can be observed that the transmission energy is almost the same till the jammer intervention after which the energy expenditure increases with the second benchmark approach. This is mainly because of the repeated transmission and re-transmission attempts of the jammer-affected nodes. Therefore, the variation of the magnitude of the transmission energy under all the three schemes is initially insignificant, as shown in Figure 5(c). 5(c). However, after jamming, a consistent reduction of the transmission energy was observed for benchmark LAPSE, compared to benchmark 2. The percentage of reduction of the cumulative transmission energy is also reflected in Figure 6(c).

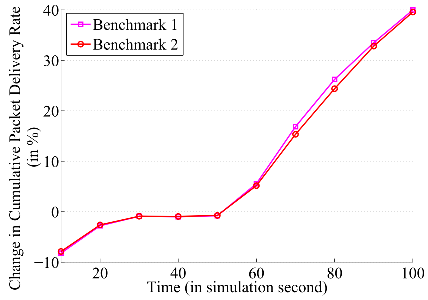
Using the formula as mentioned before in the subsection for performance metrics, the node lifetime was computed and analyzed in Figure 5(d). Because of repeated transmission attempts, a jammer-affected node easily drains out of its energy, which results in significant reduction in lifetime as indicated in Figure 5(d). Using the proposed scheme, the lifetime is significantly increased, which is also depicted in Figure 6(d). Finally, the network lifetime is depicted in Figure 5(e). As in the case of node lifetime, the network lifetime also significantly improved with the proposed scheme. The variation of the magnitude of the network lifetime is shown in Figure 6(e), and is close to that in Figure 6(d).

C. Asymptotic Computational Complexity Analysis

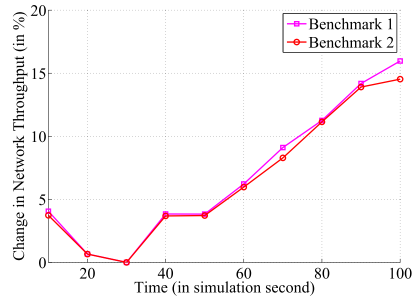
In this subsection, we perform and analyze the asymptotic computational complexity of the proposed LAPSE algorithm. For the purpose of determining the asymptotic expression for computational complexity, we would refer to Algorithm 1, as described in Section IV. The time complexity for computation of line i in Algorithm 1 is denoted by $T(i)$.

As we observe from the algorithm of LAPSE, the first step involves the formation of the committee as per Equation (8). Now, for a given source υ_s, and a destination υ_d, $P_{s,d}$ is the set of all the paths from υ_s to υ_d. Let the cardinality of the set $P_{s,d}$ be denoted by $\eta(P_{s,d})$. Therefore, if $\eta(P_{s,d}) = k$, then it can be inferred that there can be a maximum of k distinct paths from υ_s to υ_d. As per Equation (8), all the vertices involved in all of the paths of $P_{s,d}$ comprise the committee $\mathcal{C}$.

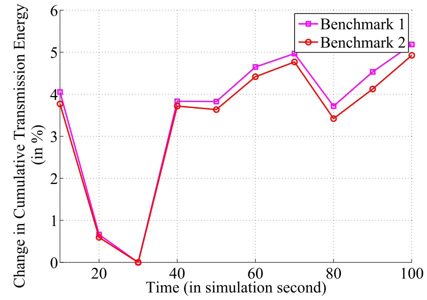
1) Case 1 (With a Single Intermediate Vertex): In that case, it is obvious this the cardinality of the committee is the minimum if every path has the minimum number of vertices



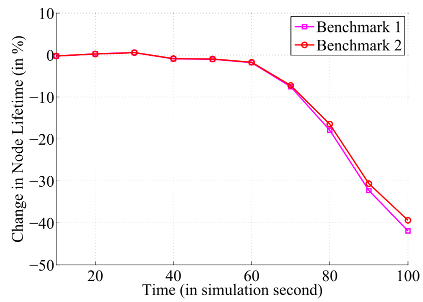
(a) Packet Delivery Rate



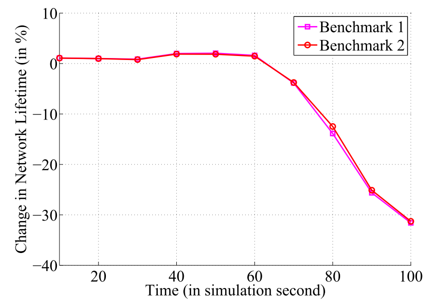
(b) Network Throughput



(c) Cumulative Transmission Energy



(d) Node Lifetime



(e) Network Lifetime

Fig. 6. Comparative analysis of network parameters for the existing and the proposed scheme.

that stand distinct compared to the other $k-1$ paths. A trivial example of this case is when the number of intermediate vertices in each path less than or equal to 1. In that case, if $\eta_{max}(\mathcal{C})$ denotes the maximum cardinality of the committee, then the structure of each path is as follows. Referring to Equation (5), we have,

$$P_{s,d} = \left\{P_i : (v_s, v_{\epsilon_{i,1}}, v_d), \right\}, \quad \forall 1 \leq i \leq k \tag{43}$$

Therefore, we have, $\eta_{max}(\mathcal{C}) = k+2$, where all the k intermediate vertices in the k paths are distinct. It is to be noted that, the minimum cardinality of the committee, $\eta_{min}(\mathcal{C})$, is always less than or equal to k. The rationale behind the determination of $\eta_{min}(\mathcal{C})$ is that, if only k' out of the k paths have a distinct intermediate vertex, where $1 \leq k' \leq k$, there is no effective contribution on cardinality by the other $k'-k$ paths. Therefore, $\eta_{min}(\mathcal{C}) \leq k$.

2) Case 2 (With Multiple Intermediate Vertices): In this case, every path in $P_{s,d}$ has more than one intermediate vertices. Here, the magnitude of $\eta_{max}(\mathcal{C})$ can be large. The magnitude is maximum if every path possesses h distinct intermediate vertices. Thus, again referring to Equation (5), we have,

$$P_{s,d} = \left\{P_i : (v_s, v_{\epsilon_{i,1}}, v_{\epsilon_{i,2}}, \cdots, v_{\epsilon_{i,h}}, v_d), \right\}, \quad \forall 1 \leq i \leq k \tag{44}$$

Therefore, $\eta_{max}(\mathcal{C}) \approx O(kh)$ where, an experimental magnitude of h ranges from 11 to 20 with the hop length varying between $200-400$ meters [57], [58].

Having computed the cardnality of the committee, the computation of Q_{P_k} and $\hat{Q}$ (as per lines $2-4$ of Algorithm 1) over all the links of all paths is asymptotically equivalent to $O(kh)$. Again, it is to be noted that, if there are overlapping links within different paths, the link-quality is calculated only once and subsequently re-used. Therefore, in a practical scenario, the time taken to compute $\hat{Q}$, $T(\hat{Q})$, can be judiciously assumed to be less thank kh. At line 5 we have, $T(5) \approx O(k)$ as the computation is done over all k paths. For computation of lines $6-12$, the complexity can be modeled as $T(6-12) \approx O(kh)$ based on parallel execution of lines 6 and 8 within every node in the committee. Again, $T(13-18) \approx O(k)$.[‡]

From the above discussion, we may conclude that, for a jammer-affected zone comprising of k h-hop paths from the source to the destination, the computation time complexity of LAPSE id $O(kh)$. As the magnitude of h may be fairly low ranging from 10 to 20 nodes, the complexity may be further considered to have a tighter upper bound of $O(k)$.

VII. Conclusion

This work focuses on mitigating the effects of static and proactive jamming in WSNs. In the presence of a jammer, several nodes undergo repeated transmissions, which results in rapid drainage of energy resource. To prevent the network from the aforementioned problem, this work proposes a link-quality aware bypassing mechanism to detour the jamming

[‡]While implementing LAPSE, it is to be noted that a single link can be a part of multiple paths. However, while calculating the "goodness" of a link for the first time, we use an approach similar to the one used in dynamic programming. Whenever the "goodness" value of a link is computed for the first time, it is stored in a memoized table and for any subsequent reference to these links, the values are fetched from the memoized table and reused. This approach optimizes the computational complexity and eventually reduces the overall time to compute the "goodness" values of all the paths.

affected zone. The work propounds an alternative path selection scheme between every source-destination pair of the network. This scheme is aware of the link quality and is based on the theory of ODR. The objective of this work was to determine the alternative path that has the optimal link quality. Results indicated that the network efficiency significantly increases in terms of packet delivery rate, network throughput, transmission energy, node lifetime, and network lifetime.

In the future, this problem may be revisited and investigated in a real-sensor network platform. Further, the problem may be extended under a mobile WSN scenario. Incorporation of a reactive jammer also induces research interest.

Appendix
Proof of Theorem 1

Based on Equation (36), it can be observed that [19], $\hat{f}(\mathcal{D}_{P_l}) = 1$, *iff*, $\alpha\mathcal{P}(1)\zeta(\mathcal{D}_{P_l} : 1) > (1-\alpha)\mathcal{P}(-1)\zeta(\mathcal{D}_{P_l} : -1)$. Therefore, $\hat{f}(\mathcal{D}_{P_l}) = -1$, *iff* $\alpha\mathcal{P}(1)\zeta(\mathcal{D}_{P_l} : 1) < (1-\alpha)\mathcal{P}(-1)\zeta(\mathcal{D}_{P_l} : -1)$. Therefore, for $\hat{f}$ to be optimal, partitioning should be such that,

$$\mathcal{Y}_{P_l}^{f+} = \{\mathcal{D}_{P_l} \in \mathcal{M} : \hat{f}(\mathcal{D}_{P_l}) = 1\} \tag{45}$$

$$= \Big\{\mathcal{D}_{P_l} : \mathcal{D}_{P_l} \in \mathcal{M} \text{ and, } \alpha\mathcal{P}(1)\zeta(\mathcal{D}_{P_l} : 1) > (1-\alpha)\mathcal{P}(-1)\zeta(\mathcal{D}_{P_l} : -1)\Big\} \tag{46}$$

$$= \Bigg\{\mathcal{D}_{P_l} : \mathcal{D}_{P_l} \in \mathcal{M} \text{ and, } \frac{\alpha}{1-\alpha}\frac{\mathcal{P}(1)}{\mathcal{P}(-1)} \times \prod_{\upsilon_x \in \mathcal{A}(\mathcal{D}_{P_l})} \Lambda^+_{x,P_l} \prod_{\upsilon_x \in \mathcal{R}(\mathcal{D}_{P_l})} \left(1-\Lambda^+_{x,P_l}\right) > \prod_{\upsilon_x \in \mathcal{R}(\mathcal{D}_{P_l})} \Lambda^-_{x,P_l} \prod_{\upsilon_x \in \mathcal{A}(\mathcal{D}_{P_l})} \left(1-\Lambda^-_{x,P_l}\right)\Bigg\} \tag{47}$$

$$= \Bigg\{\mathcal{D}_{P_l} : \mathcal{D}_{P_l} \in \mathcal{M} \text{ and, } \ln\frac{\alpha}{1-\alpha} + \ln\frac{\mathcal{P}(1)}{\mathcal{P}(-1)} + \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^+_{x,P_l}}{\left(1-\Lambda^-_{x,P_l}\right)}\left(d_x^{P_l}+1\right)! - \ln\frac{\Lambda^-_{x,P_l}}{\left(1-\Lambda^+_{x,P_l}\right)}\left(1-d_x^{P_l}\right)!\Bigg] + \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^-_{x,P_l}}{\left(1-\Lambda^+_{x,P_l}\right)} - \ln\frac{\Lambda^+_{x,P_l}}{\left(1-\Lambda^-_{x,P_l}\right)}\Bigg] > 0\Bigg\} \tag{48}$$

$$= \Bigg\{\mathcal{D}_{P_l} : \mathcal{D}_{P_l} \in \mathcal{M} \text{ and, } \ln\frac{\alpha}{1-\alpha} + \ln\frac{\mathcal{P}(1)}{\mathcal{P}(-1)} + \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^+_{x,P_l}}{\left(1-\Lambda^-_{x,P_l}\right)}\left(d_x^{P_l}+1\right)! - \ln\frac{\Lambda^-_{x,P_l}}{\left(1-\Lambda^+_{x,P_l}\right)}\left(1-d_x^{P_l}\right)!\Bigg] + \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^-_{x,P_l}\left(1-\Lambda^-_{x,P_l}\right)}{\Lambda^+_{x,P_l}\left(1-\Lambda^+_{x,P_l}\right)}\Bigg] > 0\Bigg\} \tag{49}$$

Therefore, we obtain that,

$$\mathcal{Y}_{P_l}^{\hat{f}+} = \Bigg\{\mathcal{D}_{P_l} : \mathcal{D}_{P_l} \in \mathcal{M} \text{ and, } \ln\frac{\alpha}{1-\alpha} + \ln\frac{\mathcal{P}(1)}{\mathcal{P}(-1)} + \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^+_{x,P_l}}{\left(1-\Lambda^-_{x,P_l}\right)}\left(d_x^{P_l}+1\right)! - \ln\frac{\Lambda^-_{x,P_l}}{\left(1-\Lambda^+_{x,P_l}\right)}\left(1-d_x^{P_l}\right)!\Bigg] + \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^-_{x,P_l}\left(1-\Lambda^-_{x,P_l}\right)}{\Lambda^+_{x,P_l}\left(1-\Lambda^+_{x,P_l}\right)}\Bigg] > 0\Bigg\} \tag{50}$$

and,

$$\mathcal{Y}_{P_l}^{\hat{f}+} = \Bigg\{\mathcal{D}_{P_l} : \mathcal{D}_{P_l} \in \mathcal{M} \text{ and, } \ln\frac{\alpha}{1-\alpha} + \ln\frac{\mathcal{P}(1)}{\mathcal{P}(-1)} + \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^+_{x,P_l}}{\left(1-\Lambda^-_{x,P_l}\right)}\left(d_x^{P_l}+1\right)! - \ln\frac{\Lambda^-_{x,P_l}}{\left(1-\Lambda^+_{x,P_l}\right)}\left(1-d_x^{P_l}\right)!\Bigg] + \sum_{x=1}^{m}\Bigg[\ln\frac{\Lambda^-_{x,P_l}\left(1-\Lambda^-_{x,P_l}\right)}{\Lambda^+_{x,P_l}\left(1-\Lambda^+_{x,P_l}\right)}\Bigg] \leq 0\Bigg\} \tag{51}$$

Hence, $\hat{f} = \sigma\left(\theta + \omega + \gamma + \Psi\right)$. This concludes the proof.

References

[1] T.-Y. Wang, L.-Y. Chang, and P.-Y. Chen, "A collaborative sensor-fault detection scheme for robust distributed estimation in sensor networks," *IEEE Trans. Commun.*, vol. 57, no. 10, pp. 3045–3058, Oct. 2009.

[2] J. Barros and M. Tüchler, "Scalable decoding on factor trees: A practical solution for wireless sensor networks," *IEEE Trans. Commun.*, vol. 54, no. 2, pp. 284–294, Feb. 2006.

[3] S. Chatterjee and S. Misra, "Target tracking using sensor-cloud: Sensor-target mapping in presence of overlapping coverage," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1435–1438, Aug. 2014.

[4] S. Aeron, V. Saligrama, and D. A. Castanon, "Efficient sensor management policies for distributed target tracking in multihop sensor networks," *IEEE Trans. Signal Process.*, vol. 56, no. 6, pp. 2562–2574, Jun. 2008.

[5] J. Oetting, "An analysis of meteor burst communications for military applications," *IEEE Trans. Commun.*, vol. 28, no. 9, pp. 1591–1601, Sep. 1980.

[6] R. J. Kenefic, "Performance of an FMCW radar sensor," *IEEE Trans. Commun.*, vol. 40, no. 11, pp. 1675–1678, Nov. 1992.

[7] K.-H. Ahn, A. G. Stefanopoulou, and M. Jankovic, "AFR-based fuel ethanol content estimation in flex-fuel engines tolerant to MAF sensor drifts," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 3, pp. 590–603, May 2013.

[8] S. Misra and S. Chatterjee, "Social choice considerations in cloud-assisted WBAN architecture for post-disaster healthcare: Data aggregation and channelization," *Inf. Sci.*, vol. 284, pp. 95–117, Nov. 2014.

[9] D. Kruse, J. T. Wen, and R. J. Radke, "A sensor-based dual-arm tele-robotic system," *IEEE Trans. Autom. Sci. Eng.*, vol. 12, no. 1, pp. 4–18, Jan. 2015.

[10] C. T. Kone, A. Hafid, and M. Boushaba, "Performance management of IEEE 802.15.4 wireless sensor network for precision agriculture," *IEEE Sensors J.*, vol. 15, no. 10, pp. 5734–5747, Oct. 2015.

[11] T. Wark *et al.*, "Transforming agriculture through pervasive wireless sensor networks," *IEEE Pervasive Comput.*, vol. 6, no. 2, pp. 50–57, Apr. 2007.

[12] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1593–1603, Mar. 2014.

[13] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1746–1759, Aug. 2014.

[14] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[15] M. Sedehi, F. Colone, D. Cristallini, and P. Lombardo, "Reduced order jammer cancellation scheme based on double adaptivity," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 46, no. 4, pp. 1762–1781, Oct. 2010.

[16] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN," *IEEE Trans. Mobile Comput.*, vol. 11, no. 5, pp. 793–806, May 2012.

[17] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart., 2009.

[18] A. Azim, S. Mahiba, T. A. K. Sabbir, and S. Ahmad, "Efficient jammed area mapping in wireless sensor networks," *IEEE Embedded Syst. Lett.*, vol. 6, no. 4, pp. 93–96, Dec. 2014.

[19] R. C. Ben-Yashar and S. I. Nitzan, "The optimal decision rule for fixed-size committees in dichotomous choice situations: The general result," *Int. Econ. Rev.*, vol. 38, no. 1, pp. 175–186, 1997.

[20] S. Misra, R. Singh, and S. V. R. Mohan, "Geomorphic zonalisation of wireless sensor networks based on prevalent jamming effects," *IET Commun.*, vol. 5, no. 12, pp. 1732–1743, Aug. 2011.

[21] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 8, pp. 1119–1133, Aug. 2010.

[22] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: A jammed-area mapping service for sensor networks," in *Proc. 24th IEEE Real-Time Syst. Symp.*, Dec. 2003, pp. 286–297.

[23] H.-M. Sun, S.-P. Hsu, and C.-M. Chen, "Mobile jamming attack and its countermeasure in wireless sensor networks," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops*, vol. 1. May 2007, pp. 457–462.

[24] U. Patel, T. Biswas, and R. Dutta, "A routing approach to jamming mitigation in wireless multihop networks," in *Proc. 18th IEEE Workshop Local Metropolitan Area Netw. (LANMAN)*, Oct. 2011, pp. 1–6.

[25] Z. Bidai and M. Maimour, "Interference-aware multipath routing protocol for video transmission over ZigBee wireless sensor networks," in *Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS)*, Apr. 2014, pp. 837–842.

[26] I. Nikseresht, H. Yousefi, A. Movaghar, and M. Khansari, "Interference-aware multipath routing for video delivery in wireless multimedia sensor networks," in *Proc. 32nd Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Jun. 2012, pp. 216–221.

[27] M. Kodialam and T. V. Lakshman, "Minimum interference routing with applications to MPLS traffic engineering," in *Proc. IEEE 19th Annu. Joint Conf. IEEE Comput. Commun. Soc.*, vol. 2. Mar. 2000, pp. 884–893.

[28] I. Bahceci and A. K. Khandani, "Linear estimation of correlated data in wireless sensor networks with optimum power allocation and analog modulation," *IEEE Trans. Commun.*, vol. 56, no. 7, pp. 1146–1156, Jul. 2008.

[29] F. Yuan, G. P. Villardi, F. Kojima, and H. Yano, "Channel direction information probing for multi-antenna cognitive radio system," *EURASIP J. Adv. Signal Process.*, vol. 2015, no. 1, pp. 1–13, Aug. 2015.

[30] Y. Noam, A. Manolakos, and A. J. Goldsmith, "Null space learning with interference feedback for spatial division multiple access," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5699–5715, Oct. 2014.

[31] G. Zhao, B. Huang, L. Li, and X. Zhou, "Relay-assisted cross-channel gain estimation for spectrum sharing," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 973–986, Mar. 2016.

[32] A. Fida, N. T. Jaidi, and T. D. Ngo, "Link quality aware route selection in heterogeneous wireless sensor networks," in *Proc. 11th Int. Conf. Ubiquitous Robots Ambient Intell. (URAI)*, Nov. 2014, pp. 279–284.

[33] H. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, "Jamming-resilient multipath routing," *IEEE Trans. Depend. Sec. Comput.*, vol. 9, no. 6, pp. 852–864, Nov. 2012.

[34] M. B. Pursley and H. B. Russell, "Routing in frequency-hop packet radio networks with partial-band jamming," *IEEE Trans. Commun.*, vol. 41, no. 7, pp. 1117–1124, Jul. 1993.

[35] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1433–1448, Jul. 2015.

[36] P. Tague, S. Nabar, J. A. Ritcey, and R. Poovendran, "Jamming-aware traffic allocation for multiple-path routing using portfolio selection," *IEEE/ACM Trans. Netw.*, vol. 19, no. 1, pp. 184–194, Feb. 2011.

[37] P. Tague, S. Nabar, J. A. Ritcey, D. Slater, and R. Poovendran, "Throughput optimization for multipath unicast routing under probabilistic jamming," in *Proc. IEEE 19th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2008, pp. 1–5.

[38] J.-J. Lee and J. Lim, "Effective and efficient jamming based on routing in wireless ad hoc networks," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1903–1906, Nov. 2012.

[39] G. Parissidis, M. Karaliopoulos, T. Spyropoulos, and B. Plattner, "Interference-aware routing in wireless multihop networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 5, pp. 716–733, May 2011.

[40] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Jamming-aware minimum energy routing in wireless networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 2313–2318.

[41] S.-J. Yoon and Y.-B. Ko, "JRGP: Jamming resilient geocasting protocol for mobile tactical ad hoc networks," in *Proc. Int. Conf. Inf. Commun. Technol. Converg.*, Nov. 2010, pp. 437–442.

[42] Z. Liu, H. Liu, W. Xu, and Y. Chen, "An error-minimizing framework for localizing jammers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 508–517, Feb. 2014.

[43] T. Cheng, P. Li, and S. Zhu, "An algorithm for jammer localization in wireless sensor networks," in *Proc. IEEE 26th Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2012, pp. 724–731.

[44] Q. Wang, X. Wei, J. Fan, T. Wang, and Q. Sun, "A step further of PDR-based jammer localization through dynamic power adaptation," in *Proc. 11th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2015, pp. 1–6.

[45] C. A. Boano, M. A. Zuniga, T. Voigt, A. Willig, and K. Romer, "The triangle metric: Fast link quality estimation for mobile wireless sensor networks," in *Proc. 19th Int. Conf. Comput. Commun. Netw.*, Aug. 2010, pp. 1–7.

[46] H. Song, R. Kwan, and J. Zhang, "Approximations of EESM effective SNR distribution," *IEEE Trans. Commun.*, vol. 59, no. 2, pp. 603–612, Feb. 2011.

[47] H. Song, R. Kwan, and J. Zhang, "Analytical approximations of EESM effective SNR distribution using pearson system," in *Proc. IEEE 73rd Veh. Technol. Conf. (VTC Spring)*, May 2011, pp. 1–5.

[48] K. W. Cheung, H. C. So, W.-K. Ma, and Y. T. Chan, "Received signal strength based mobile positioning via constrained weighted least squares," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, vol. 5. Apr. 2003, pp. V-137–V-140.

[49] S. Chatterjee, R. Ladia, and S. Misra, "Dynamic optimal pricing for heterogeneous service-oriented architecture of sensor-cloud infrastructure," *IEEE Trans. Serv. Comput.*, vol. 10, no. 2, pp. 203–216, Mar./Apr. 2015.

[50] F. Cadger, K. Curran, J. Santos, and S. Moffett, "A survey of geographical routing in wireless ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 621–653, 2nd Quart., 2013.

[51] L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, "A survey of multicast routing protocols for mobile ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 78–91, 1st Quart., 2009.

[52] H. Salarian, K.-W. Chin, and F. Naghdy, "An energy-efficient mobile-sink path selection strategy for wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2407–2419, Jun. 2014.

[53] S.-R. Hu, S. Peeta, and H.-T. Liou, "Integrated determination of network origin–destination trip matrix and heterogeneous sensor selection and location strategy," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 1, pp. 195–205, Jan. 2016.

[54] Y. Zheng, O. Ozdemir, R. Niu, and P. K. Varshney, "New conditional posterior Cramér–Rao lower bounds for nonlinear sequential Bayesian estimation," *IEEE Trans. Signal Process.*, vol. 60, no. 10, pp. 5549–5556, Oct. 2012.

[55] M. Neil, X. Chen, and N. Fenton, "Optimizing the calculation of conditional probability tables in hybrid Bayesian networks using binary factorization," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 7, pp. 1306–1312, Jul. 2012.

[56] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Energy-efficient routing in wireless networks in the presence of jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6828–6842, Oct. 2016.

[57] M. Kheireddine and R. Abdellatif, "Analysis of hops length in wireless sensor networks," *Wireless Sens. Netw.*, vol. 6, no. 6, pp. 109–117, 2014.

[58] O. Jerew and K. Blackmore, "Estimation of hop count in multi-hop wireless sensor networks with arbitrary node density," *Int. J. Wireless Mobile Comput.*, vol. 7, no. 3, pp. 207–216, May 2014.

Prasenjit Bhavathankar received the B.E. degree in computer engineerig from Shivaji University, India, in 1998, and the M.Tech. degree in computer engineering from Mumbai University, India, in 2007. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, IIT Kharagpur, Kharagpur, India. His current research interests are wireless ad-hoc and sensor networks.

Subarna Chatterjee received the B.Tech. degree in computer science and technology from the West Bengal University of Technology, India, in 2012. She is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, IIT Kharagpur, Kharagpur, India. Her current research interests include networking and communication aspects of cloud computing in wireless sensor networks.

Sudip Misra received the bachelor's degree from IIT Kharagpur, Kharagpur, India, the master's degree from the University of New Brunswick, Fredericton, Canada, and the Ph.D. degree in computer science from Carleton University, Ottawa, Canada. He has several years of experience with the academia, government, and the private sectors in research, teaching, consulting, project management, architecture, software design, and product engineering roles. He was associated with Cornell University, USA, Yale University, USA, Nortel Networks, Canada, and the Government of Ontario, Canada. He is currently an Associate Professor with the Department of Computer Science and Engineering, IIT Kharagpur. He is the author of over 200 scholarly research papers, including 90 journal papers. His current research interests include algorithm design for emerging communication networks. He has received eight research paper awards in different conferences. He received the IEEE ComSoc Asia Pacific Outstanding Young Researcher Award at the IEEE GLOBECOM 2012, Anaheim, CA, USA. He was also a recipient of several academic awards and fellowships, such as the Young Scientist Award (National Academy of Sciences, India), the Young Systems Scientist Award (Systems Society of India), the Young Engineers Award (Institution of Engineers, India), the (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 received the Canadian Governments prestigious NSERC Post-Doctoral Fellowship and the Humboldt Research Fellowship in Germany. He is the Editor-in-Chief of the *International Journal of Communication Networks and Distributed Systems* (U.K.: Inderscience). He has also been serving as the Associate Editor of the *Telecommunication Systems* Journal (Springer), the *Security and Communication Networks* Journal (Wiley), the *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).