PLOS ONE

RESEARCH ARTICLE

Enhancement of the performance of wireless sensor networks using the multihop multiantenna power beacon path selection method in intelligent structures

Ahmed Hammad[1]*, **M. A. Mohamed**[1], **Heba M. Abdel-Atty**[2]

1 Department of Electronics and Communications Engineering, Mansoura University, Mansoura, Egypt, **2** Department of Electrical Engineering, Port Said University, Port Said, Egypt

* ahmed_khairt@std.mans.edu.eg

Citation: Hammad A, Mohamed MA, Abdel-Atty HM (2022) Enhancement of the performance of wireless sensor networks using the multihop multiantenna power beacon path selection method in intelligent structures. PLoS ONE 17(11): e0276940. https://doi.org/10.1371/journal.pone.0276940

Editor: Kapil Kumar Nagwanshi, Guru Ghasidas Vishwavidyalaya: Guru Ghasidas University, INDIA

Received: August 12, 2022

Accepted: October 17, 2022

Published: November 7, 2022

Peer Review History: PLOS recognizes the benefits of transparency in the peer review process; therefore, we enable the publication of all of the content of peer review and author responses alongside final, published articles. The editorial history of this article is available here: https://doi.org/10.1371/journal.pone.0276940

Data Availability Statement: All relevant data are within the paper and its Supporting information files.

Abstract

Sensor nodes are the building blocks of wireless sensor networks (WSNs), which may gather, analyze, and transmit various types of information to a certain destination. Data collection and transmission to the destination are the main responsibilities of sensor nodes at specified time intervals. However, one of the biggest issues with WSNs is the creation of energy-efficient wireless network algorithms. In this paper, a multi-hop multi-antenna power beacon path selection (MMPS) protocol is proposed. The proposed approach consists of a source, a destination, relays, power beacons generating radio frequency (RF) signals for energy harvesting, and eavesdroppers. We used physical layer security associated with energy harvesting to protect data from eavesdroppers without requiring higher layer data encryption and enhance the energy consumption of wireless networks. The signal's broadcast strength must be high enough to allow for energy harvesting while being low enough to prevent eavesdropping. The process continues until the data reaches the destination. Comparing the performance of MMPS with those of conventional methods, MMPS enhanced the wireless network outage probability (OP) up to 99.7%, life time, energy consumption, protection from eavesdroppers, and more resistant to hardware impairments which increased the immunity up to 95%.

Introduction

Several routing strategies have been proposed to save energy and enhance network performance. In this respect, wireless sensor networks (WSNs) have dynamic architectures, making energy-aware routing between wireless sensor nodes one of their main issues. previously [1], some authors proposed a centralized genetic-based clustering (CGC) protocol using a new concept called the onion approach, where cluster heads are elected on the basis of a genetic algorithm with three criteria. Their simulation results proved that the CGC protocol significantly extends network lifetime, decreases network energy consumption, and is capable of

Funding: The author(s) received no specific funding for this work.

Competing interests: The authors have declared that no competing interests exist.

considerably enhancing packet delivery and keeping nodes operational for longer times. However, these networks lack a specific infrastructure and are formed in inaccessible areas. Thus, constant control over these networks is not practicable. Consequently, they frequently come under attack. Meanwhile, Hatamian et al. [2] proposed a fuzzy rate controller with a congestion-aware routing technique that prioritizes data packets. On the basis of the data value, they proposed a queuing model for determining packet priority. Fuzzy logic and a greedy method were used to reduce packet loss and average energy consumption in nodes. They also proposed a method for enhancing the time, energy, and packet loss limitations while increasing the system quality of service. In a distributed environment, the latency of more upstream traffic must be tested. For instance, wireless nodes are in charge of gathering physiological data from patients and keeping track of their routine medical examinations. WSNs can also be used for interior monitoring in the business sector [3]. The application of WSNs in the military and medical areas emphasizes the significance of data transmission security in these networks. In WSNs, key management is one of the techniques used to secure information transfer between network components. In a previous study [4], sensor nodes were arranged into a binary tree, and the aggregation requests were validated using a shared key, according to the authors' discussion of a dependable tree-based data aggregation approach. Only after an acknowledgment does the request become aggregated. Meanwhile, a collaborative signal processing framework gathers data from the monitoring region. Heavy calculation and assessment are required for surveillance systems, which leads to the implementation of realistically feasible solutions. In another study [5], the proposed method's encryption procedures were built in three phases with three keys that may be changed as needed to increase secrecy and security. In the proposed scheme, the network was split into several zones controlled by area managers, which were stronger nodes with extra processing and memory. The proposed approach had better scalability, flexibility, efficiency, and lower power usage. In Alimoradi et al. [6], zones were used to describe a network. The network was organized into non-overlapping hexagonal zones. There were several sensor nodes in each zone. The two forms of communication defined by the proposed approach were intra-zone and inter-zone communication. The proposed method outperformed comparable protocols in terms of attack resistance, energy usage, alive nodes, and communication overhead. Nilsaz Dezfuli and Barati [7] presented a system where the network region was split into several square grids based on a geographical foundation to increase the lifespan and coverage of WSNs. The sensor node in each grid with the highest energy was chosen as a cluster head. The residual part of the zone may then be determined thereafter. The power used for sensing is generally insignificant when compared with the power used for reporting. Thus, creative energy-efficient reporting systems for WSNs are the focus of most research efforts. In a smart environment, various sensors are used to perform or control processes using various approaches. When Internet of things (IoT) systems and smart environments are combined, smart objects perform much better. For instance, Ghorbani Dehkordi and Barati [8] used two-phase clustering and routing as a solution for the multiobjective problem, but the division of the network environment affected the performance. Intelligent sensors deployed in target places and jointly function as a system called WSNs inspect physically dynamic quantities that are also time-sensitive and delay-tolerant or real-time and non-real-time operations. Because of the power-restricted nature of these nodes, the conventional routing protocol does not take data heterogeneity into account while establishing routing pathways. Instead, it focuses on energy-efficient routing to extend the lifetime of the system [9]. Thus, a framework was created in [10] to operate with several sensor nodes, including border, common, and gateway nodes, which conduct sensing under various workloads. One of the critical elements of the applications of sensors is the energy and power modeling of WSNs, a technique for data gathering and hierarchical network management. Thus, creating

an independent and effective network among sensor nodes is crucial to providing long network lifetimes and regulated energy consumption of networks [11].

Motivations and related work

Physical layer security (PLS) [12] has been considered a low-cost alternative to upper-layer encryption for securing data during transmission. Secrecy performance is measured in PLS using secrecy capacity, defined as the variation between the data link channel and eavesdropping link channel capacities. Various algorithms [13–15] aimed to optimize the data rate to optimize the effectiveness of secured communication methods for data links. Security improvement strategies in underlay cognitive networks (CNs) have been suggested previously [6, 16]. The transmitters in CNs must alter their broadcast energy to meet interference limits imposed by main users. Cao et al. [17] examined the security and reliability of CNs by determining the intercept probability (IP) during the existence of an external observer and the outage probability (OP) at certified recipients. According to previous studies [18, 19], transmitting wireless sensors on the route path, such as source and relays, could decrease their transmission power to avoid IP at an active eavesdropper. Ayatollahitafti et al. [20] presented chaotic compressive sensing to handle energy efficiency and security challenges simultaneously. Wireless equipment with limited battery power must gather energy from the environment to keep going, which recently popularized energy harvesting (EH) from radio frequency (RF) in mobile ad-hoc networks [21], cognitive radio ad-hoc networks [22], and WSNs [23]. This is why noninfrastructure networks [24] have received a lot of attention as an effective approach for energy-constrained wireless networks. The EH from RF approach enables nodes to harvest their energies from RF signals. In this regard, several authors suggested secure communication algorithms using RF and EH methods in [25, 26]. The secrecy OP of simultaneous wireless communication and power transmission network comprising one base station, one required data receiver, multiple main subscribers, and several EH receivers in UCR platforms was explored in [26]. Meanwhile, Hieu et al. [27] generated formulations of OP for the proposed methods over the Rayleigh fading channel by considering that EH receivers might function as eavesdroppers. They presented the shortest path selection (SPS) protocol, random path selection (RPS) protocol, and best path selection (BPS) protocol as three unique path selection techniques, but their method has only one beacon. A rechargeable helpful jammer with a rechargeable supply was used to prevent eavesdropping in [28]. Other previous studies [29–31] presented various viable receiver architectures for simultaneous wireless information and power transfer. In [32], cooperative communication algorithms were used to minimize error rates, enhance system coverage, and improve network lifetime. Other authors investigated the wireless system performance of underlay multihop cognitive radio networks in [33, 34], where secondary users harvest energy from a beacon or a main transmitter. Previously, practically most published works considered wireless equipment hardware transceivers as ideal. However, frequency noises, amplifier amplitude nonlinearity, and I/Q imbalance were common problems in low-cost wireless nodes' physical transceivers that decrease the performance of wireless networks [35–37]. Power beacons (PBs), depending on the time switching model, were described in [38] for attaining great energy consumption and increasing the range of wireless transmission in large-scale wireless communication networks. PBs were incorporated or deployed separately from the base station [39]. In [40], the main network used several primary transmitters that acted as PBs to power the secondary network's source and relay. The EH CNs throughput performance and OP were examined and evaluated. The big modeling approach with some primary transmitters expanding to infinity was also addressed. Many investigators have lately focused on multi-hop cooperative relays to enhance network performance and

increase radio coverage (e.g., [41–43]). Compared with conventional method connection, the transmitter in multi-hop networks reduces energy consumption for data transfer. Consequently, it may be found in various applications in the real world, such as WSNs, cellular networks, IoT, vehicle or people roadside, and tracking services [44–46].

Problem definition and contributions

According to the above literature, effective energy use with secure routing is a significant area of study interest. However, most current solutions cannot modify routing performance in response to the changing environment and constrained WSN capabilities. Furthermore, contemporary work cannot choose the next hop based on the best choice, and such methods affect the performance of routing across the whole network. Additionally, routing pathways are frequently reorganized during data relay, adding redundancy in terms of both time and communication costs. The continuous transmission of routing and management messages in the setup phase is the cause of this overhead. Consequently, investigating the field of energy efficiency with a lightweight solution to extend the lifetime of the network is necessary. All of the cited previous studies provided helpful information on the performance of EH regarding PLS, allowing system designers to make more precise recommendations. However, most of them focused on dual-hop relaying systems rather than multi-hop relaying systems. Thus, we presented one novel protocol to improve the outage performance for multi-hop multi-path decode-and-forward ultra-dense networks. There are numerous pathways between a secondary source and a secondary destination in the proposed method. One of these is chosen to transmit the source information to the receiver [36]. For packet forwarding, the source and relays on the selected channel must gather energy from the environment beacon RF waves [47, 48]. These transmitting wireless sensors must alter their signal strength in eavesdropper (V) presence to fulfill an interference limitation.

We therefore propose a multi-hop multi-antenna PB path selection (MMPS) approach to increase the e2e simultaneous channel capacity. We provide accurate and asymptotic closed-form formulations of e2e OP for the proposed scheme over the Rayleigh fading channel to measure performance. Simulations using the Monte Carlo approach are then used to confirm our conclusions.

The following are the significant contributions of this paper:

- The MMPS approach, which picks the path with the maximum end-to-end channel capacity, is proposed as a path selection method using an H number of beacons to achieve the best outage performance.
- We investigate a real-world WSN application where all hardware transmitters and receivers suffer from limitations.
- The source and relay nodes use the RF method to avoid eavesdroppers from aggregating source-collected data across several hops. Furthermore, by adjusting their transmitter power, these approved transmitters can restrict the channel capacity gained on the eavesdropping lines.
- We use a non-cooperative eavesdropping scenario, where eavesdroppers work individually.
- Over a Rayleigh fading channel, we construct closed-form equations for OP. The results of Monte Carlo simulations are provided to confirm our conclusions.

The following is an overview of the paper's structure. The system model utilized in this work is described in Section IV. Section V provides an overview of three traditional protocols.

Section VI contains the proposed protocol. Section VII presents the performance evaluation and the simulation outcomes. Finally, section VIII concludes the article.

System model

In Fig 1, the proposed protocol is expressed by a system model, where S is the source connected with the destination D in a multi-hop approach. Further, there are N possible pathways between S and D, but just one is chosen to serve the communication between them.

Let us call the count of relays Y_k (denoted by $R_{k,1}, R_{k,2}, \ldots, R_{k,Y_k}$) on the kth path, where $k = 1, 2, \ldots, N$ and $Y_k \geq 1$. Furthermore, active V eavesdroppers are denoted by $V_1, V_2, \ldots, V_u$ attempting to eavesdrop on the data sent by the source and wireless relay nodes. The RF approach in [49] is used at each hop on the specified path to stop eavesdroppers from using a maximum ratio combiner to integrate the incoming data. We assume that S and the relays, as well as all transmitters, are power-limited. Thus, they must collect the network beacon's RF energy (identified by $PB_1, PB_2, \ldots, PB_H$) for data transfer. All the connections are also expected to be low-cost wireless sensor nodes with one antenna operating in half-duplex mode. Consequently, data are sent over orthogonal periods using time division multiple access. Suppose that the transmission of data is divided into orthogonal time slots and that the kth route is chosen. Specifically, in the $(i + 1)^{th}$ time slot, the relay $R_{k,i}$ sends the Z data from the source to the relay $R_{k,i+1}$, where $i = 0, 1, 2, \ldots, Y_k$.

We should add that $R_{k,0} \equiv S$ and $R_{k,Y_k+1} \equiv D$ for all k. Because there are problems with the hardware, the received signal of the broadcast $R_{k,i} \rightarrow R_{k,i+1}$ and $R_{k,i} \rightarrow V_u$ can be respectively

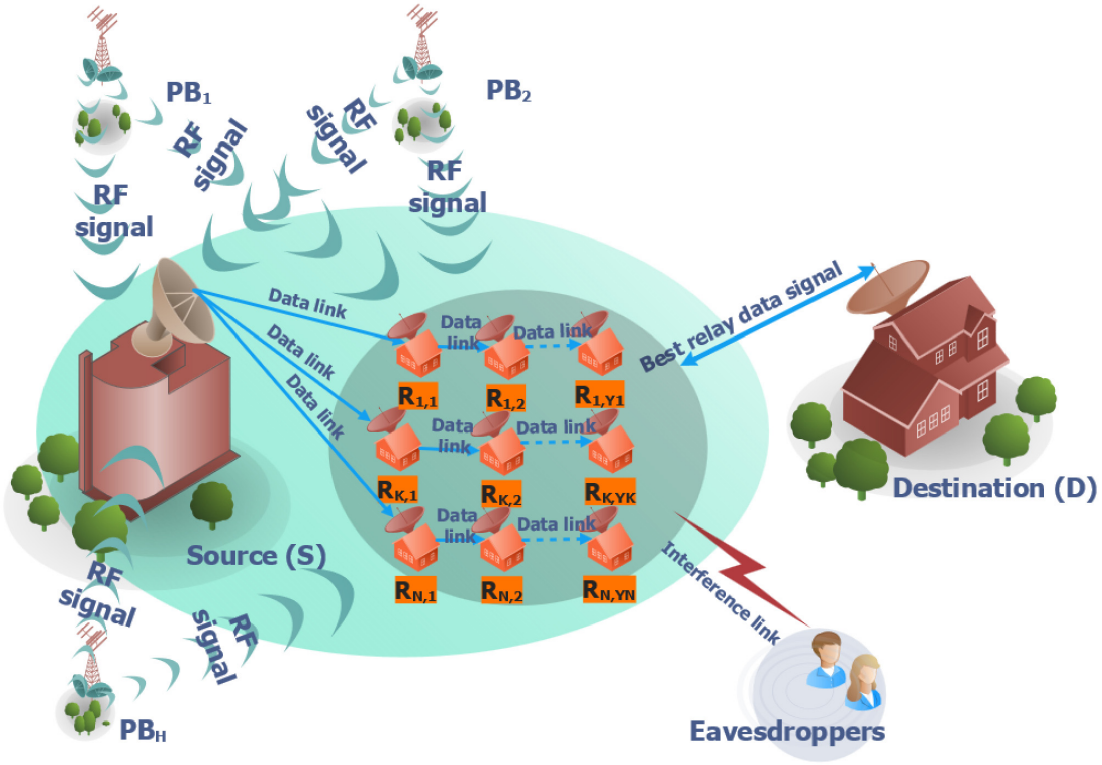

Fig 1. System model of PB-assisted relaying protocols with relay selection methods.

https://doi.org/10.1371/journal.pone.0276940.g001

described in the following ways:

$$y_{R_{k,i},R_{k,i+1}} = \sqrt{P_{R_{k,i}}} h_{R_{k,i}R_{k,i+1}} (Z + \eta_{R_{k,i}R_{k,i+1}}) + \mu_{R_{k,i}R_{k,i+1}} + v_{R_{k,i}R_{k,i+1}}, \quad (1)$$

$$y_{R_{k,i}V_u} = \sqrt{P_{R_{k,i}}} h_{R_{k,i}V_u} (Z + \eta_{R_{k,i}V_u}) + \mu_{R_{k,i}V_u} + v_{R_{k,i}V_u}, \quad (2)$$

where $P_{R_{k,i}}$ represents the transmitter's transmission power $R_{k,i}$,h_{AB} is the coefficient of transmission channel from A to B link, where $A, B \in \{R_{k,i}, R_{k,i+1}, V_u\}$, η_{AB} and μ_{AB} represent the noise made by hardware malfunctions at the transmitter A and receiver B, respectively, and v_{AB} are Additive White Gaussian noises represented as random Gaussian variables with variance N_0 and zero mean.

Assuming the Rayleigh fading channel and the channel gain as $\gamma_{AB} = |h_{AB}|^2$, where γ_{AB} is an exponential random variable, the cumulative distribution function (CDF) and probability density function (PDF) are given, respectively, as

$$F_{\gamma_{AB}}(x) = 1 - \exp((-\lambda_{AB})x), \quad (3)$$

$$f_{\gamma_{AB}}(x) = \lambda_{AB}\exp((-\lambda_{AB})x), \quad (4)$$

where λ_{AB} is γ_{AB} a parameter and equal to $1/\varepsilon\{\gamma_{AB}\}$ and an predicted operator is $\varepsilon\{.\}$. is formulated as in [50] to calculate the path loss:

$$\lambda_{AB} = d_{AB}^{\beta}, \quad (5)$$

where d_{AB} is the distance between A and B,where the path loss scale β is $(2 \geq \beta \leq 6)$ as in [35, 51, 52]. The distortion noises can be represented by η_{AB} and μ_{AB}, as a complex with a circular symmetry Zero-mean and variance Gaussian distribution $(\sigma_{AB}^t)^2 P_A$, and $(\sigma_{AB}^r)^2 P_A \gamma_{AB}$.

All nodes are considered to have used the same design, with the same rates of hardware limitations (i.e., $(\sigma_{AB}^t)^2 = \sigma_a^2, \sigma_{AB}^r = \sigma_b^2$.

Consequently, the instantaneous signal-to-noise ratio (SNR) of $R_{k,i} \rightarrow R_{k,i+1}$ and $R_{k,i} \rightarrow V_u$ able to implement this links is

$$SNR_{R_{k,i}R_{k,i+1}} = \frac{P_{R_{k,i}} \gamma_{R_{k,i}R_{k,i+1}}}{\kappa P_{R_{k,i}} \gamma_{R_{k,i}R_{k,i+1}} + N_0}, \quad (6)$$

$$SNR_{R_{k,i}V_u} = \frac{P_{R_{k,i}} \gamma_{R_{k,i}V_u}}{\kappa P_{R_{k,i}} \gamma_{R_{k,i}V_u} + N_0}, \quad (7)$$

where $k = \sigma_a^2 + \sigma_b^2$.

We assumed D as a block duration and the $(i + 1)th$ data transmission time slot for the kth path with time duration $\tau_k = D/(Y_k + 1)$. Time switching was used in this time slot, where the relay $R_{k,i}$ harvested its energy from beacon PB at the time $\alpha\tau_k$, where $\alpha \in (0 < \alpha < 1)$ as shown in [33]. The energy harvested by $R_{k,i}$ can be formulated as

$$EH_{R_{k,i}} = \eta\alpha\tau_k P \sum_{h=1}^{H} \gamma_{R_{k,i},PB_h}, \quad (8)$$

where η represents the EH efficiency $0 < \eta < 1$, P is the transmission power of PB, and $\gamma_{P_B R_{k,i}}$ describes the channel gain of the $P_B \rightarrow R_{k,i}$ channel. We additionally supposed that the

connection between P_B and $\gamma_{P_B R_{k,i}}$ is a Rayleigh fading channel, and the PDF and CDF of $\gamma_{P_B R_{k,i}}$ were formulated as in (3) and (4).

The data were sent using the time duration $(1-\alpha)\tau_k$; thus, the power transmitted by the relay $R_{k,i}$ was formulated from energy conservation as

$$\mathrm{P}_{\mathrm{R_{k,i}}}^{\max} \leq \frac{EH_{R_{k,i}}}{(1-\alpha)\tau_k} \triangleq Z_{P_B R_{k,i}}, \tag{9}$$

where $Z_{P_B R_{k,i}} = zP\sum_{h=1}^{H}\gamma_{R_{k,i},PB_h}$ with $z = \eta\alpha/(1-\alpha)$. The frequency ranges utilized for data transmission and EH were diverse to minimize interference. Furthermore, at each time slot, all of the nodes spent the same amount of time $\alpha\tau_k$ harvesting energy before using it to transmit data.

Assuming the transmitter $R_{k,i}$ can get the eavesdropping channel state information (CSI) of connections $R_{k,i} \rightarrow V_u$ because the eavesdroppers are active, it can decrease the quality of these links by adjusting the transmission power. Let us call $P_{R_{k,i}}^{V}$ the transmit power of $R_{k,i}$, which is modified to account for eavesdropping CSIs. The capacity of the channel between $R_{k,i}$ and V_u is determined as follows:

$$\mathrm{C}_{\mathrm{R_{k,i}V_u}} = (1-\alpha)\tau_k \log_2\left(1 + \frac{P_{R_{k,i}}^{V}\gamma_{R_{k,i}V_u}}{kP_{R_{k,i}}^{V}\gamma_{R_{k,i}V_u} + N_0}\right), \tag{10}$$

Assuming that the eavesdroppers work individually, the channel capacity of the finest eavesdropper is used to calculate the eavesdropping information bit rate at the kth time slot (see [53])

$$\mathrm{C}_{\mathrm{R_{k,i}V_u}}^{\mathrm{tot}} = \max_{u=1,2,\ldots,U}(\mathrm{C}_{R_{k,i}Vu}), \tag{11}$$

$$\mathrm{C}_{\mathrm{R_{k,i}V_u}}^{\mathrm{tot}} = (1-\alpha)\tau_k \log_2\left(1 + \frac{P_{R_{k,i}}^{V}\varphi_{R_{k,i}max}}{kP_{R_{k,i}}^{V}\varphi_{R_{k,i}max} + N_0}\right), \tag{12}$$

where

$$\varphi_{\mathrm{R_{k,i}max}} = \max_{u=1,2,\ldots,U}(\gamma_{R_{k,i}Vu}), \tag{13}$$

The probability of an outage (OP) is the foundation of the maximum throughput received at the receiver side and is less than the desired rate (as indicated by $C_t h$).

We already have a set of criteria to prevent eavesdroppers from successfully decoding:

$$\mathrm{C}_{\mathrm{R_{k,i}V_u}}^{\mathrm{tot}} \leqslant C_{th}, \tag{14}$$

$$\mathrm{P}_{\mathrm{R_{k,i}}}^{\mathrm{V}} \leqslant \frac{\rho_k N_0}{\varphi_{R_{k,i}max}(1-\kappa\rho_k)}, (\kappa < 1/\rho_k) \tag{15}$$

where

$$\rho_{\mathrm{k}} = 2^{c_{th}/(1+\alpha)\tau_k} - 1, \tag{16}$$

The max transmitting power of the relay $R_{k,i}$ can be formulated as (see (9) and (15))

$$P_{R_{k,i}}^{max} = \begin{cases} Z_{P_B R_{k,i}} & \text{if } \kappa \leq 1/\rho_k. \\ \min\left(Z_{P_B R_{k,i}}, \dfrac{\rho_k N_0}{\varphi_{R_{k,i}max}(1-\kappa\rho_k)}\right), & \text{otherwise.} \end{cases} \tag{17}$$

Consequently,the link $R_{k,i} \rightarrow R_{k,i+1}$ channel capacity can be formulated as

$$C_{R_{k,i}R_{k,i+1}} = \begin{cases} (1-\alpha)\tau_k \log\left(1 + \dfrac{\Delta_{1,k,i}}{\kappa\Delta_{1,k,i} + N_0}\right) & \text{if } \kappa > 1/\rho_k. \\ (1-\alpha)\tau_k \log\left(1 + \dfrac{\Delta_{2,k,i}}{\kappa\Delta_{2,k,i} + N_0}\right), & \text{otherwise.} \end{cases} \tag{18}$$

where

$$\Delta_{1,\mathrm{k,i}} = Z_{P_B R_{k,i}} \gamma_{R_{k,i}R_{k,i+1}}, \tag{19}$$

$$\Delta_{2,\mathrm{k,i}} = min\left(Z_{P_B R_{k,i}}, \frac{\rho_k N_0}{\varphi_{R_{k,i}max}(1-\kappa\rho_k)}\right), \tag{20}$$

Thereafter, we can formulate the e2e channel capacity of the kth path as

$$\mathrm{C}_{\mathrm{k}}^{\mathrm{e2e}} = \min_{i=1,2,\ldots,Y_k+1}(C_{R_{k,i}R_{k,i+1}}), \tag{21}$$

Traditional protocols

This section describes three multihop harvest-to-transmit WSNs with path selection methods. Hieu et al. [27] proposed three novel route selection techniques, namely, the SPS, RPS, and BPS protocols, to examine the effect of EH and hardware cognitive problems on the effectiveness of cooperative multihop WSNs during outages. They used a method to harvest energy similar to that in [33]. As a result, BPS is more resistant to hardware failure than RPS and SPS, and it can overcome the Rayleigh block fading on devices with poor hardware quality. The source randomly chooses one of the possible pathways in the first protocol, known as RPS, to send data to the destination. The e2e OP in this protocol may be expressed as

$$\mathrm{OP}_{\mathrm{RPS}} = 1/N\sum_{k=1}^{N}\Pr(C_a^{e2e} < C_{th}), \tag{22}$$

where $(a)\in\{1, 2, \ldots, N\}$

Although the RPS method is straightforward to construct, it may not give good outage performance because of the random selection. Because of the delay limitation, minimizing the number of hops on the chosen route enhances the e2e data rate. Thus, we suggest the SPS protocol as the second protocol. The SPS technique selects the route with the fewest hops number. Thus, the protocol's e2e OP is written as

$$\mathrm{OP}_{\mathrm{SPS}} = \Pr(C_b^{e2e} < C_{th}), \tag{23}$$

where $(b)\in\{1, 2, \ldots, N\}$

Finally, BPS selects the way that offers the most end-to-end channel capacity to maximize system performance. Mathematically, the OP of this protocol can be written as

$$\mathrm{OP}_{\mathrm{BPS}} = \Pr(C_c^{e2e} < C_{th}), \tag{24}$$

where $(c)\in\{1, 2, \ldots, N\}$

The e2e channel capacity of the kth path is formulated as follows:

$$C_k^{e2e} = \begin{cases} (1-\alpha)\tau_k \log_2\left(1 + \min_{i=1,2,\ldots,Y_k+1} \dfrac{\Delta_{1,k,i}}{\kappa\Delta_{1,k,i} + N_0}\right) & \text{if } \kappa > 1/\rho_k. \\ (1-\alpha)\tau_k \log_2\left(1 + \min_{i=1,2,\ldots,Y_k+1} \dfrac{\Delta_{2,k,i}}{\kappa\Delta_{2,k,i} + N_0}\right), & \text{otherwise.} \end{cases} \tag{25}$$

Proposed MMPS protocol

We propose a new path selection method for intelligent structures based on the EH technique to extend the lifetime of the network and for suitability for WSNs or ad-hoc networks. The flowchart of the proposed protocol scheme is shown in Fig 2.

First, we evaluated the performance of MMPS, and the path with the maximum e2e channel capacity was picked. Second, we used the SNR to calculate the e2e OP and generate a throughput expression.

$$\mathrm{C}_{\mathrm{q}}^{\mathrm{e2e}} = \max_{m=1,2,\ldots,N} (C_k^{e2e}), \tag{26}$$

where $(q)\in\{1, 2, \ldots, N\}$, and the e2e OP for MMPS can be formulated as

$$\mathrm{OP}_{\mathrm{MM}}^{\mathrm{e2e}} = \Pr(C_q^{e2e} < C_{th}) = \prod_{k=1}^{N} Pr(C_k^{e2e} < C_{th}), \tag{27}$$

$$\Pr(C_q^{e2e} < C_{th}) = \begin{cases} \Pr\left(\min_{i=1,2,\ldots,Y_k+1} \log_2\left(\dfrac{\Delta_{1,q,i}}{\kappa\Delta_{1,q,i} + N_0}\right) < \rho_q\right) & \text{if } \kappa \geqslant 1/\rho_k. \\ \Pr\left(\min_{i=1,2,\ldots,Y_k+1} \log_2\left(\dfrac{\Delta_{2,q,i}}{\kappa\Delta_{2,q,i} + N_0}\right) < \rho_q\right) & \text{otherwise} \end{cases} \tag{28}$$

where OP_{MM}^{e2e} is expressed from OP at the most direct route, and the exact form of OP can be given as

$$OP = \begin{cases} \Pr\left(\dfrac{\Delta_{1,a,i}}{\kappa\Delta_{1,a,i} + N_0}\right) < \rho_a) & \text{if } \kappa \geqslant 1/\rho_a. \\ \Pr\left(\dfrac{\Delta_{2,a,i}}{\kappa\Delta_{2,a,i} + N_0}\right) < \rho_a) & \text{otherwise} \end{cases} \tag{29}$$

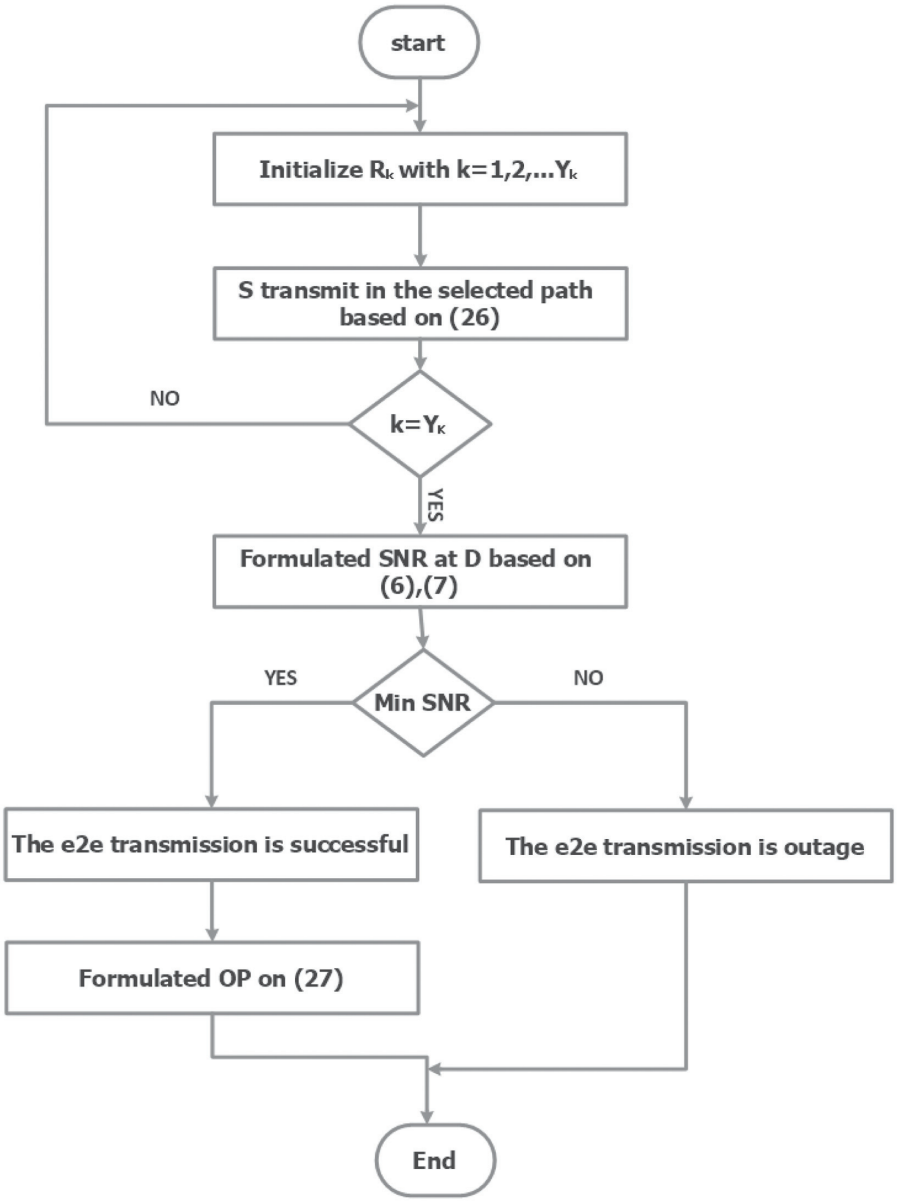

Fig 2. The flow chart for the data transmission of (MMPS) scheme.

https://doi.org/10.1371/journal.pone.0276940.g002

Performance evaluation

We used Monte Carlo simulations in this part to evaluate the theoretical formulas and compare our results with SPS, RPS, and BPS [27]. A matrix research facility was used to generate the simulation outcomes (MATLAB R2020a). We executed separate trials to get the e2e OP for the MMPS protocol compared with the other described protocols. In each session, we built Rayleigh channel coefficients for every link. Table 1 shows a two-dimensional grid where each coordinate is displayed. We used markers, solid lines, and dashed lines for all scenarios to represent simulation outcomes, precise theoretical results, and asymptotic theoretical findings, respectively.

Table 1. Coordinates of network component.

Component	Coordinates
Source	$S \rightarrow (0, 0)$
Relays	$R \rightarrow \left(\frac{i}{Y_K+1}, 0\right)$
Destination	$D \rightarrow (1, 0)$
Beacon	$PB \rightarrow (x_{PB}, y_{PB})$
Eavesdroppers	$V \rightarrow (x_V, y_V)$

https://doi.org/10.1371/journal.pone.0276940.t001

As shown in Fig 3, we studied the effect of beacon P's transmission power (dB) on the magnitude of OP in the scenario when the eavesdroppers work individually by setting the components as shown in Table 2. As shown, there is an inverse relationship between the power of the beacon and OP, and the theoretical and simulation findings agree well. When P (dB) is low, for example, when the power in the figure is equal to −5 dB, we can detect that OP approaches 1; when the power of the beacon grows, the OP numbers decline. Thus, boosting the transmission power can help protect the physical layer versus eavesdropping assaults. In addition, when comparing the three traditional protocols, the BPS protocol clearly gets the highest OP. However, when we used the proposed MMPS protocol and added more PBs to the network by setting $H = 2$, the MMPS protocol very clearly achieves the highest OP among RPS, SPS and BPS protocols by 99.6%, 99.7% and 49.3% respectively. Furthermore, raising the transmission power of the proposed method can improve its outage performance.

Fig 4 shows the scenarios where eavesdroppers do not cooperate with the OP as a function of the number of impairments at two distinct broadcast powers of beacon P = 15 dB and the

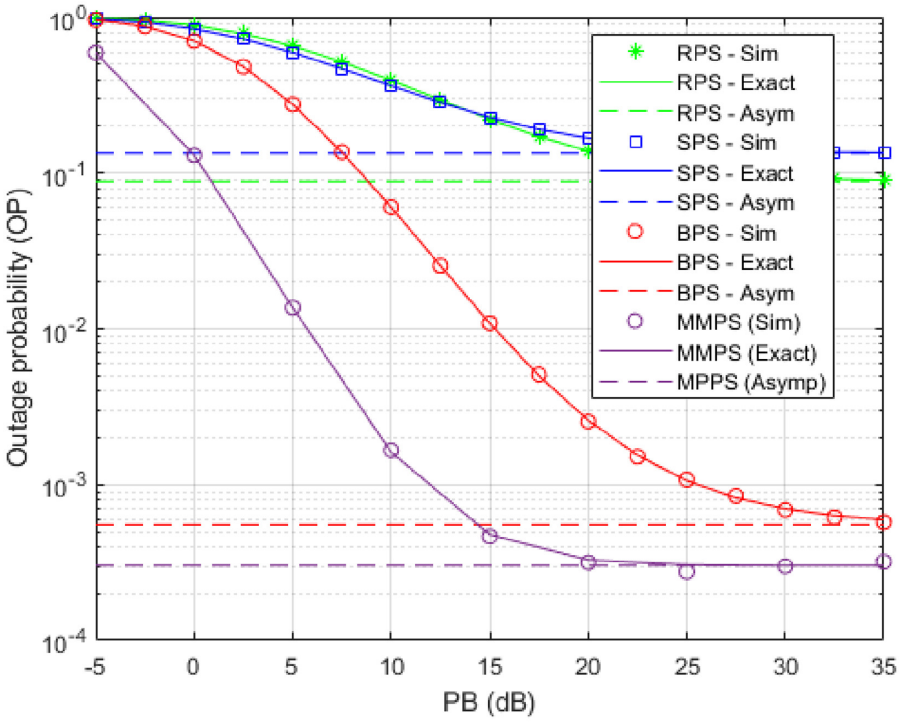

Fig 3. OP as a function of transmitting power P in (db).

https://doi.org/10.1371/journal.pone.0276940.g003

Table 2. Simulation conditions for each figure.

Component	Fig 3	Fig 4	Fig 5	Fig 6	Fig 7
Y	[2, 3, 4]	[2, 3, 4]	[2, 3, 4]	[2, 3, 4]	[2, 3, 4]
R	0.5	0.5	0.5	0.5	0.5
u	2	2	2	2	2
(x_{PB}, y_{PB})	(0.5,0.1)	(0.5,0.1)	(—,0.1)	(0.5,0.1)	(0.5,0.1)
(x_V, y_V)	(0.5,1)	(0.5,1)	(0.5,1)	(0.5,—)	(0.5,1)
η	0.1	0.1	0.1	0.1	0.1
α	0.1	0.1	0.1	0.1	-
H	2	4	4	4	4
κ	0.1	-	0.1	0.1	0.1

The mark (—) means that a certain component is variable.

https://doi.org/10.1371/journal.pone.0276940.t002

wireless network is adjusted by the components shown in Table 2. The OP numbers of MMPS, BPS, RPS, and SPS rose as κ grew, as can be seen in this graph. The MMPS still beat RPS, SPS, and BPS at all curve points. Furthermore, in high areas, the OP of all algorithms converged toward 1, specifically at $\kappa \geq 0.55$, which is consistent with the preceding section's findings. The figure also illustrates that the MMPS algorithm is much more resistant to hardware failure than RPS, SPS, and BPS by 99.5%, 99.6%, 87.7% respectively, allowing it to function efficiently on devices with poor hardware quality.

The probability of an outage is presented as a function of x_{PB} in Fig 5 upon simulation by the components shown in Table 2. Apparently, when x_{PB} grows to around 0.4, the outage

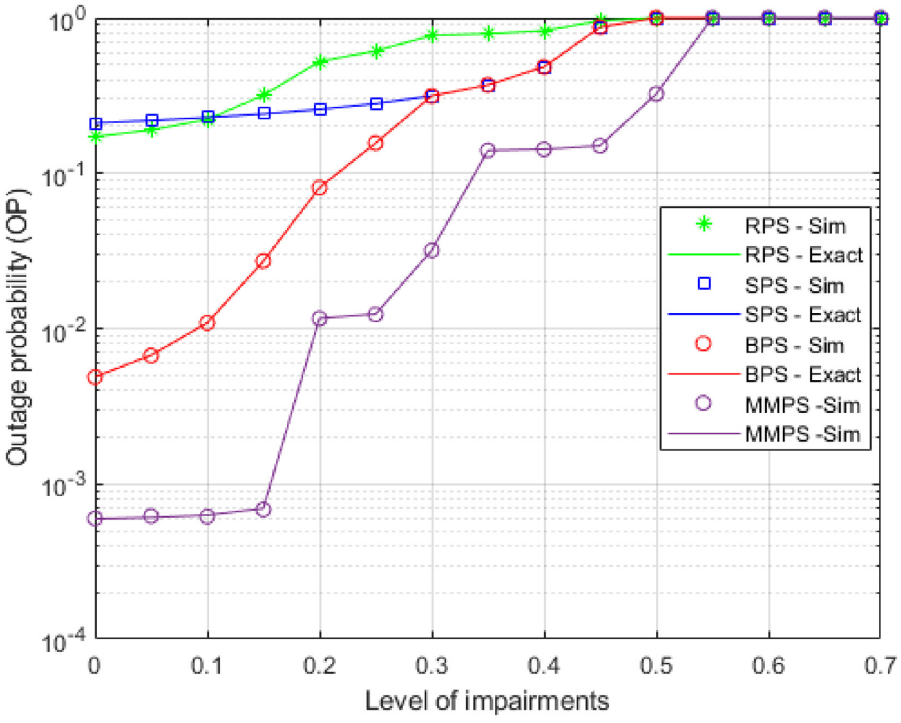

Fig 4. OP as a function of κ.

https://doi.org/10.1371/journal.pone.0276940.g004

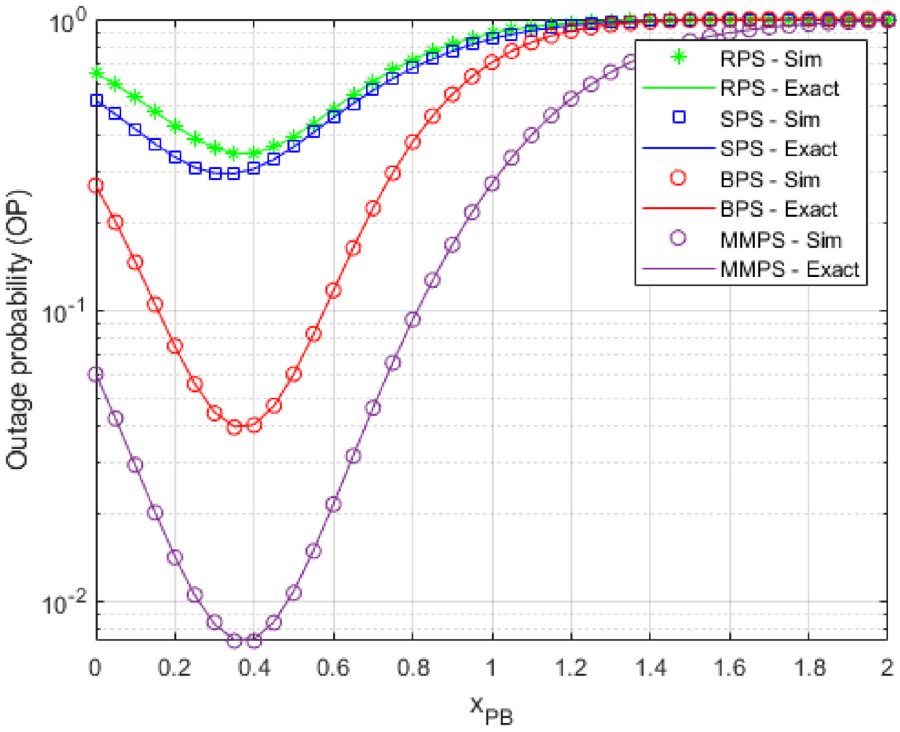

Fig 5. OP as a function of x_{PB}.

https://doi.org/10.1371/journal.pone.0276940.g005

performances of the proposed algorithms improve until they reach an optimal value, beyond which they fall. Using this model, we can identify the location of the beacon where the OP achieves the ideal value. That is, once x_{PB} is around 0.4, the OP of MMPS is minimized; when it is about 0.3 or 0.35, the OP values of RPS, SPS, and BPS are minimized.

In Fig 6, we investigated the impact of y_V on OP upon simulation by the components shown Table 2 and set $x_{PB} = 0.4$ as the optimal value. As can be observed from the figure, OP rises when the eavesdroppers move far from the data path. Thus, when $y_V = 0$, OP has the worst effects as the connection between V_u and S or $R_{k,i}$ is the smallest.

In Fig 7, using the simulation components shown in Table 2 the OP is shown as a function of the EH ratio α when the eavesdroppers work individually. Because it affects the received power at the ideal relay path and the transmission power of the source and relay nodes, as shown in the figure, the EH ratio α is significant in this situation. These graphs show the ideal value during which the OP can be decreased. Accordingly, the more energy that can be extracted from the beacon, the higher the value of α. Consequently, relay nodes can utilize more energy to transmit data from S to D. The higher the value of α, the less the amount of time necessary for communication $(1 - \alpha)\tau_k$ between $S \rightarrow R$ or $R \rightarrow R$. Thus, we can get the optimum outage performance when α reaches its optimal value. For example, the best value for MMPS equals 0.3, as shown in Fig 7.

Conclusion

We examined the effects of hardware limitations besides EH on the throughput performance of multi-hop multi-path collaborative WSNs by presenting a unique path selection approach called the MMPS. Furthermore, we computed the proposed protocol's OP accurately and

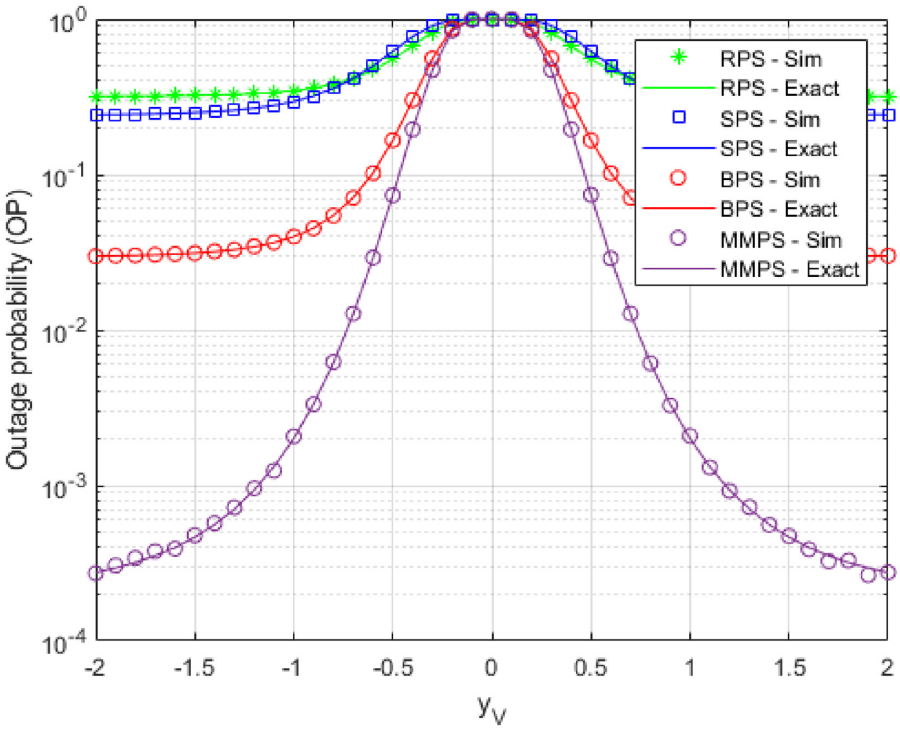

Fig 6. OP as a function of y_V.

https://doi.org/10.1371/journal.pone.0276940.g006

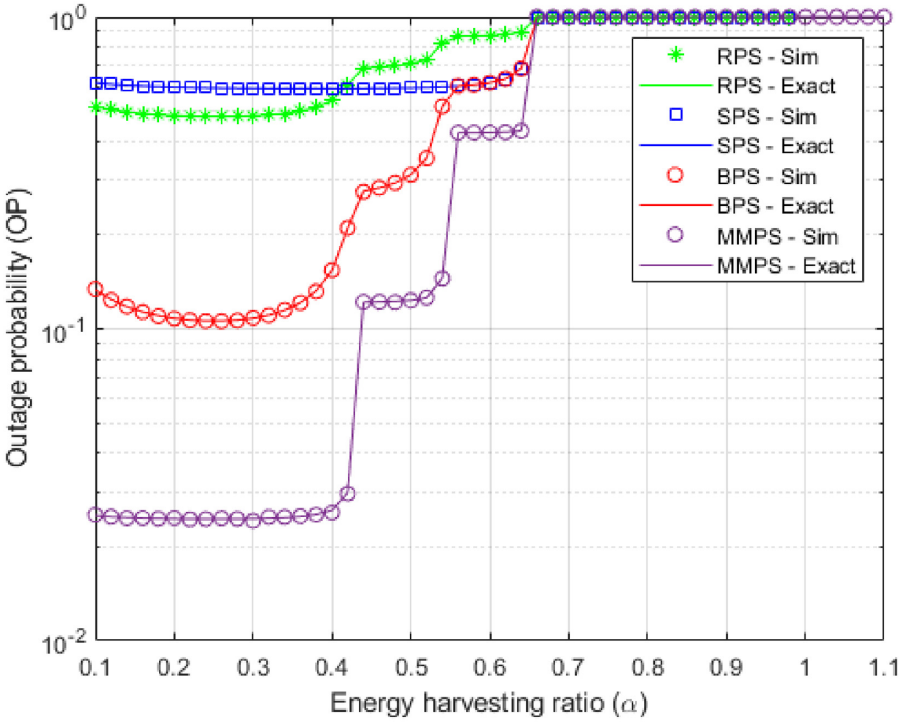

Fig 7. OP as a function of α.

https://doi.org/10.1371/journal.pone.0276940.g007

asymptotically in the context of several beacons, several eavesdropping assaults, and Rayleigh block fading, where the source S and wireless relay sensors can collect the beacon's RF signals. The considered EH and hardware limitation system performed securely according to simulation findings. MMPS was resistant to hardware issues, allowing it to work better with devices with poor hardware quality. Finally, the performance may be enhanced by positioning the beacon in the proper location and selecting an appropriate EH ratio α.

Supporting information

S1 File.
(DOCX)

Author Contributions

Conceptualization: M. A. Mohamed, Heba M. Abdel-Atty.

Data curation: Ahmed Hammad, M. A. Mohamed, Heba M. Abdel-Atty.

Formal analysis: Ahmed Hammad, M. A. Mohamed.

Funding acquisition: Ahmed Hammad, Heba M. Abdel-Atty.

Investigation: Ahmed Hammad.

Methodology: M. A. Mohamed, Heba M. Abdel-Atty.

Project administration: M. A. Mohamed.

Resources: M. A. Mohamed.

Software: Ahmed Hammad.

Supervision: Ahmed Hammad, Heba M. Abdel-Atty.

Validation: M. A. Mohamed, Heba M. Abdel-Atty.

Visualization: Ahmed Hammad, M. A. Mohamed.

Writing – original draft: Ahmed Hammad, Heba M. Abdel-Atty.

Writing – review & editing: Ahmed Hammad, Heba M. Abdel-Atty.

References

1. Hatamian M, Barati H, Movaghar A, Naghizadeh A. CGC: centralized genetic-based clustering protocol for wireless sensor networks using onion approach. Telecommun Syst. 2016; 62: 657–674. https://doi.org/10.1007/s11235-015-0102-x
2. Hatamian M, Almasi Bardmil M, Asadboland M, Hatamian M, Barati H. Congestion-Aware Routing and Fuzzy-based Rate Controller for Wireless Sensor Networks. Radioengineering. 2016; 25: 114–123. https://doi.org/10.13164/re.2016.0114
3. Hamid Barati, Ali Movaghar, Ali Barati,Arash azizi mazreah. A review of coverage and routing for wireless sensor networks. International Journal of Electronics and Communication Engineering. 2008; 2: 67–73.
4. Hasheminejad E, Barati H. A reliable tree-based data aggregation method in wireless sensor networks. Peer Peer Netw Appl. 2021; 14: 873–887. https://doi.org/10.1007/s12083-020-01025-x
5. Havashemi rezaeipour K, Barati H. A hierarchical key management method for wireless sensor networks. Microprocess Microsyst. 2022; 90: 104489. https://doi.org/10.1016/j.micpro.2022.104489
6. Alimoradi P, Barati A, Barati H. A hierarchical key management and authentication method for wireless sensor networks. International Journal of Communication Systems. 2022; 35. https://doi.org/10.1002/dac.5076

7. Nilsaz Dezfuli N, Barati H. Distributed energy efficient algorithm for ensuring coverage of wireless sensor networks. IET Communications. 2019; 13: 578–584. https://doi.org/10.1049/iet-com.2018.5329
8. Ghorbani Dehkordi E, Barati H. Cluster based routing method using mobile sinks in wireless sensor network. International Journal of Electronics. 2022; 1–13. https://doi.org/10.1080/00207217.2021.2025451
9. Hajipour Z, Barati H. EELRP: energy efficient layered routing protocol in wireless sensor networks. Computing. 2021; 103: 2789–2809. https://doi.org/10.1007/s00607-021-00996-w
10. Sharifi SS, Barati H. A method for routing and data aggregating in cluster-based wireless sensor networks. International Journal of Communication Systems. 2021; 34. https://doi.org/10.1002/dac.4754
11. Nilsaz Dezfouli N, Barati H. A distributed energy-efficient approach for hole repair in wireless sensor networks. Wireless Networks. 2020; 26: 1839–1855. https://doi.org/10.1007/s11276-018-1867-0
12. Zhu F, Yao M. Improving Physical-Layer Security for CRNs Using SINR-Based Cooperative Beamforming. IEEE Trans Veh Technol. 2016; 65: 1835–1841. https://doi.org/10.1109/TVT.2015.2412152
13. Luo J, Hu J, Wu D, Li R. Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks. IEEE Trans Industr Inform. 2015; 11: 112–121. https://doi.org/10.1109/TII.2014.2374071
14. Khan A, Khan M, Ahmed S, Abd Rahman MA, Khan M. Energy harvesting based routing protocol for underwater sensor networks. PLoS One. 2019; 14: e0219459. https://doi.org/10.1371/journal.pone.0219459 PMID: 31314772
15. Zhang T, Cai Y, Huang Y, Duong TQ, Yang W. Secure Full-Duplex Spectrum-Sharing Wiretap Networks with Different Antenna Reception Schemes. IEEE Transactions on Communications. 2016; 1–1. https://doi.org/10.1109/TCOMM.2016.2625257
16. Cao Z, Ji X, Wang J, Zhang S, Ji Y, Wang J. Security-Reliability Tradeoff Analysis for Underlay Cognitive Two-Way Relay Networks. IEEE Trans Wirel Commun. 2019; 18: 6030–6042. https://doi.org/10.1109/TWC.2019.2941944
17. Adnan AI, Hanapi ZM, Othman M, Zukarnain ZA. A Secure Region-Based Geographic Routing Protocol (SRBGR) for Wireless Sensor Networks. PLoS One. 2017; 12: e0170273. https://doi.org/10.1371/journal.pone.0170273 PMID: 28121992
18. Tran Tin P, The Hung D, Nguyen T, Duy T, Voznak M. Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-Hop Transmission with and without Presence of Hardware Impairments. Entropy. 2019; 21: 217. https://doi.org/10.3390/e21020217 PMID: 33266932
19. Dinh Tran H, Trung Tran D, Choi SG. Secrecy performance of a generalized partial relay selection protocol in underlay cognitive networks. International Journal of Communication Systems. 2018; 31: e3806. https://doi.org/10.1002/dac.3806
20. Ayatollahitafti V, Ngadi MA, Mohamad Sharif J bin, Abdullahi M. An Efficient Next Hop Selection Algorithm for Multi-Hop Body Area Networks. PLoS One. 2016; 11: e0146464. https://doi.org/10.1371/journal.pone.0146464 PMID: 26771586
21. Bhardwaj A, El-Ocla H. Multipath Routing Protocol Using Genetic Algorithm in Mobile Ad Hoc Networks. IEEE Access. 2020; 8: 177534–177548. https://doi.org/10.1109/ACCESS.2020.3027043
22. Wang D, Song Y. ECCO: A Novel End-to-End Congestion Control Scheme in Multi-Hop Cognitive Radio Ad Hoc Networks. IEEE Trans Cogn Commun Netw. 2019; 5: 93–102. https://doi.org/10.1109/TCCN.2018.2889337
23. Hao S, Hong Y, He Y. An Energy-Efficient Routing Algorithm Based on Greedy Strategy for Energy Harvesting Wireless Sensor Networks. Sensors. 2022; 22: 1645. https://doi.org/10.3390/s22041645 PMID: 35214547
24. Lu X, Wang P, Niyato D, Kim DI, Han Z. Wireless networks with rf energy harvesting: A contemporary survey. IEEE Communications Surveys and Tutorials. 2015; 17: 757–789. https://doi.org/10.1109/COMST.2014.2368999
25. Singh A, Bhatnagar MR, Mallik RK. Secrecy Outage Performance of SWIPT Cognitive Radio Network With Imperfect CSI. IEEE Access. 2020; 8: 3911–3919. https://doi.org/10.1109/ACCESS.2019.2962382
26. Singh A, Bhatnagar MR, Mallik RK. Secrecy Outage of a Simultaneous Wireless Information and Power Transfer Cognitive Radio System. IEEE Wireless Communications Letters. 2016; 5: 288–291. https://doi.org/10.1109/LWC.2016.2544828
27. Hieu TD, Duy TT, Kim B-S. Performance Enhancement for Multihop Harvest-to-Transmit WSNs With Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises. IEEE Sens J. 2018; 18: 5173–5186. https://doi.org/10.1109/JSEN.2018.2829145
28. el Shafie A, Niyato D, Al-Dhahir N. Security of Rechargeable Energy-Harvesting Transmitters in Wireless Networks. IEEE Wireless Communications Letters. 2016; 5: 384–387. https://doi.org/10.1109/LWC.2016.2565466

29. Wu F, Xiao L, Yang D, Cuthbert L, Liu X. Simultaneous Wireless Information and Power Transfer Mechanism in Interference Alignment Relay Networks. Mobile Information Systems. 2016; 2016: 1–9. https://doi.org/10.1155/2016/1685054

30. Zhang R, Ho CK. MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer. IEEE Trans Wirel Commun. 2013; 12: 1989–2001. https://doi.org/10.1109/TWC.2013.031813.120224

31. Huang G, Tu W. On Opportunistic Energy Harvesting and Information Relaying in Wireless-Powered Communication Networks. IEEE Access. 2018; 6: 55220–55233. https://doi.org/10.1109/ACCESS.2018.2872757

32. Mansourkiaie F, Ahmed MH. Cooperative routing in wireless networks: A comprehensive survey. IEEE Communications Surveys and Tutorials. 2015; 17: 604–626. https://doi.org/10.1109/COMST.2014.2386799

33. Xu C, Zheng M, Liang W, Yu H, Liang Y-C. Outage Performance of Underlay Multihop Cognitive Relay Networks With Energy Harvesting. IEEE Communications Letters. 2016; 20: 1148–1151. https://doi.org/10.1109/LCOMM.2016.2547985

34. Xu C, Zheng M, Liang W, Yu H, Liang Y-C. End-to-End Throughput Maximization for Underlay Multi-Hop Cognitive Radio Networks With RF Energy Harvesting. IEEE Trans Wirel Commun. 2017; 16: 3561–3572. https://doi.org/10.1109/TWC.2017.2684125

35. Duy TT, Duong TQ, da Costa DB, Bao VNQ, Elkashlan M. Proactive Relay Selection With Joint Impact of Hardware Impairment and Co-Channel Interference. IEEE Transactions on Communications. 2015; 63: 1594–1606. https://doi.org/10.1109/TCOMM.2015.2396517

36. Solanki S, Singh V, Upadhyay PK. RF Energy Harvesting in Hybrid Two-Way Relaying Systems With Hardware Impairments. IEEE Trans Veh Technol. 2019; 68: 11792–11805. https://doi.org/10.1109/TVT.2019.2944248

37. Sharma PK, Upadhyay PK. Cognitive Relaying With Transceiver Hardware Impairments Under Interference Constraints. IEEE Communications Letters. 2016; 20: 820–823. https://doi.org/10.1109/LCOMM.2016.2533500

38. Zhong C, Chen X, Zhang Z, Karagiannidis GK. Wireless-Powered Communications: Performance Analysis and Optimization. IEEE Transactions on Communications. 2015; 63: 5178–5190. https://doi.org/10.1109/TCOMM.2015.2488640

39. Xia M, Aissa S. On the Efficiency of Far-Field Wireless Power Transfer. IEEE Transactions on Signal Processing. 2015; 63: 2835–2847. https://doi.org/10.1109/TSP.2015.2417497

40. Amodu OA, Othman M, Noordin NK, Ahmad I. Outage Minimization of Energy Harvesting-Based Relay-Assisted Random Underlay Cognitive Radio Networks With Interference Cancellation. IEEE Access. 2021; 9: 109432–109446. https://doi.org/10.1109/ACCESS.2021.3101047

41. Ogundile O, Alfa A. A Survey on an Energy-Efficient and Energy-Balanced Routing Protocol for Wireless Sensor Networks. Sensors. 2017; 17: 1084. https://doi.org/10.3390/s17051084 PMID: 28489054

42. Sun H, Naraghi-Pour M, Sheng W, Zhang R. Outage Analysis of Hop-by-Hop Relay Selection in Multi-Hop Cognitive Relay Networks. ICC 2020—2020 IEEE International Conference on Communications (ICC). IEEE; 2020. pp. 1–6.

43. Onwuegbuzie IU, Razak SA, Isnin IF, Al-dhaqm A, Anuar NB. Prioritized Shortest Path Computation Mechanism (PSPCM) for wireless sensor networks. PLoS One. 2022; 17: e0264683. https://doi.org/10.1371/journal.pone.0264683 PMID: 35271603

44. Rabby MKM, Alam MS, Shawkat MSA. A priority based energy harvesting scheme for charging embedded sensor nodes in wireless body area networks. PLoS One. 2019; 14: e0214716. https://doi.org/10.1371/journal.pone.0214716 PMID: 31009483

45. Elaraby S, Soliman HY, Abdel-Atty HM, Mohamed MA. Joint 2D-DOA and Carrier Frequency Estimation Technique Using Nonlinear Kalman Filters for Cognitive Radio. IEEE Access. 2017; 5: 25097–25109. https://doi.org/10.1109/ACCESS.2017.2768221

46. Selim M, Kamal A, Elsayed K, Abd-El-Atty H, Alnuem M. A novel approach for back-haul Self Healing in 4G/5G HetNets. 2015 IEEE International Conference on Communications (ICC). IEEE; 2015. pp. 3927–3932.

47. Bhatnagar MR, Mallik RK, Tirkkonen O. Performance Evaluation of Best-Path Selection in a Multihop Decode-and-Forward Cooperative System. IEEE Trans Veh Technol. 2016; 65: 2722–2728. https://doi.org/10.1109/TVT.2015.2419451

48. Van NT, Duy TT, Hanh T, Vo Nguyen Quoc Bao. Outage analysis of energy-harvesting based multihop cognitive relay networks with multiple primary receivers and multiple power beacons. 2017 International Symposium on Antennas and Propagation (ISAP). IEEE; 2017. pp. 1–2.

49. Jianhua Mo, Meixia Tao, Yuan Liu. Relay Placement for Physical Layer Security: A Secure Connection Perspective. IEEE Communications Letters. 2012; 16: 878–881. https://doi.org/10.1109/LCOMM.2012.042312.120582

50. Laneman JN, Tse DNC, Wornell GW. Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior. IEEE Trans Inf Theory. 2004; 50: 3062–3080. https://doi.org/10.1109/TIT.2004.838089

51. Matthaiou M, Papadogiannis A, Bjornson E, Debbah M. Two-Way Relaying Under the Presence of Relay Transceiver Hardware Impairments. IEEE Communications Letters. 2013; 17: 1136–1139. https://doi.org/10.1109/LCOMM.2013.042313.130191

52. Bjornson E, Matthaiou M, Debbah M. A New Look at Dual-Hop Relaying: Performance Limits with Hardware Impairments. IEEE Transactions on Communications. 2013; 61: 4512–4525. https://doi.org/10.1109/TCOMM.2013.100913.130282

53. Ding X, Song T, Zou Y, Chen X. Security-Reliability Tradeoff for Friendly Jammer Assisted User-Pair Selection in the Face of Multiple Eavesdroppers. IEEE Access. 2016; 4: 8386–8393. https://doi.org/10.1109/ACCESS.2016.2607783