




Article

Intelligent Trust-Based Utility and Reusability Model: Enhanced Security Using Unmanned Aerial Vehicles on Sensor Nodes

Santosh Kumar Sahoo¹, Niranjanamurthy Mudligiriappa² , Abdullah A. Algethami³ ,
Poongodi Manoharan^{4,*} , Mounir Hamdi⁴ and Kaamran Raahemifar^{5,6,7}

¹ Department of EIE, CVR College of Engineering, Hyderabad 501510, Telangana, India; santosh.kr.sahoo@gmail.com

² Department of Computer Applications, M S Ramaiah Institute of Technology, Visvesvaraya Technological University, Bangalore 560054, Karnataka, India; niruhds@gmail.com

³ Department of Engineering, Taif University, Taif 26312, Saudi Arabia; a_algethami@tu.edu.sa

⁴ College of Science and Engineering, Hamad Bin Khalifa University, Doha P.O. Box 34110, Qatar; mhamdi@hbku.edu.qa

⁵ Data Science and Artificial Intelligence Program, College of Information Sciences and Technology, Penn State University, Pennsylvania, PA 16801, USA; kvr5517@psu.edu

⁶ School of Optometry and Vision Science, Faculty of Science, University of Waterloo, 200 University Ave W, Waterloo, ON N2L3G1, Canada

⁷ Department of Chemical Engineering, Faculty of Engineering, University of Waterloo, 200 University Ave W, Waterloo, ON N2L3G1, Canada

* Correspondence: dr.m.poongodi@gmail.com



Citation: Sahoo, S.K.;

Mudligiriappa, N.; Algethami, A.A.;

Manoharan, P.; Hamdi, M.;

Raahemifar, K. Intelligent

Trust-Based Utility and Reusability

Model: Enhanced Security Using

Unmanned Aerial Vehicles on Sensor

Nodes. *Appl. Sci.* **2022**, *12*, 1317.

<https://doi.org/10.3390/app12031317>

31317

Academic Editors: Augusto Ferrante,

Mingcong Deng and Mihaiela

Iliescu

Received: 18 September 2021

Accepted: 30 December 2021

Published: 26 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: Due to its importance in prolonging the lifetime of battery-restricted wireless sensor networks, network longevity has garnered considerable research attention, with the rechargeable wireless sensor network emerging as a viable solution. In this research, the novel methodology of a trust-based mechanism for enhanced security integrated with an energy utility and re-usability model is proposed with software-defined networking (SDN) to maximize energy utilization. We proposed a novel framework with SDN for the service station in a wireless sensor network (WSN). The results showed that the life capacity of the network increases to a maximum of 290% when compared with no charging, with the charge increasing by 30% intervals. We also present how the network survives through this choice of sink. As there is variation in the network size while it increases, the proposed approach with the static method works well until the network size reaches 200. Furthermore, the proposed approach also uses the heuristic method to achieve the best performance.

Keywords: wireless sensor networks; energy utility model; unmanned aerial vehicle; intelligent-trust based model; wireless energy transfer

1. Introduction

Wireless Sensor Networks continue to attract the attention of both academic and industrial researchers all around the world due to its distributed nature and are exploited in numerous applications [1] from environmental monitoring to military surveillance including human computer interaction. Privacy, security, and consumption of energy by the nodes happen to be a foremost anxiety in the growth of WSNs, as they are exposed to malicious attacks. If a single sensor node becomes compromised, it can target multiple nodes to become engaged in and to obstruct the services rendered for legitimate users over the network. On the contrary, the wireless sensor network security needs to be addressed significantly; specifically, there is a need for mission-critical tasks [2]. It is a critical task to have secure WSNs, and it is also critical in the plans of action and applications in military battlefields. For instance, if the possibility of security vulnerabilities is present, it is

necessary for neighboring troops (nodes) to perform very well or even exceedingly well in the battlefield [3–6].

Another important issue that WSNs need to consider is the network lifetime as, on many occasions, outdoor sensor networks mostly rely on batteries for energy. Depending on the size of the deployments, proportionally larger batteries are required for larger deployments. If the network is located where regular recharging is not useful, crop growth under a bridge or in a field covered by sun and or affected by wind can significantly limit the battery life, relying solely on the effective network. We developed a system that allows for such situations in an energy feeding system using UAV by utilizing the energy of compromised nodes and external energy in the legitimate nodes to ensure 100% non-failure of the network system in the field, as shown in Figure 1.



Figure 1. UAV recharging a single node [7].

In our technique, we define the lifespan of a network and how it can be extended with UAV-based wireless charging. The extended life authenticates the addition of a recharge circuit to the sensor node. If there is a reasonable increase, we investigate under which conditions it works and focus on the amount of nodes that the UAV needs to reload. It also describes which nodes need to act as sinks for network data and how you can change the sinks to maximize network life in response to recharging.

The benefits of UAV charging in terms of WSN and the optimal use of UAV charging through compromised nodes have not been investigated. However, a significant examination into the community of the sensor network has considered highly efficient modules based on the energy- and cost-effective hardware communication [3], improved protocols with the software communication [4,5], and various approaches with data routing [6,8–10]. A large subset is considering a sufficient mobilization strategy [11–16]. Using this early research, we developed a method for sensor arrays to maximize the benefits of UAV charging.

In our research work, we proposed a new approach that reveals a technique to extend the life of a network using UAV-based wireless charging in three different cases.

- UAV recharges nodes from the entire network using the energy utilization and re-usability method from the detected compromised node by using the intelligent trust evaluation system and external energy.
- UAV recharges only the lowest-powered nodes in the network and utilizes the static method of choosing a sink, with the next sink consequently only utilizing the power from the energy utility model.
- UAV renews the sink node by recharging energy from the network with a different sink selection algorithm and provides the best sink node selection algorithm and performance measures of each algorithm with network scalability.

We performed some simulations introduced from a preliminary study [17] to investigate these issues that have shown that UAV charging can extend the network life by approximately three times. Then, we look at other issues and set up a list of guidelines dependent on the size of the network. According to the guidelines, we select the nodes (sink or low power nodes), the amount of UAVs required to enter that node, and what node to choose next. Interestingly, as the size of the network grows, it becomes more effective for the sink to remain intact, with up to 30% charged at every interval. However, when the network extends the number of nodes to 200, a change of sink is required.

This paper is further structured as follows: In Section 2, we review existing techniques used in detection systems with sensor nodes, in energy optimization models, in wireless charging models, and in energy maximization. Section 3 gives our complete research statement. Section 4 describes a range of reproducible sensor network problems in energy transfer through UAVs. Section 5 describes the energy utility and re-usability model, and Section 6 describes the UAV energy consumption and recycling model used to optimize energy distribution and shows the results of our analysis. Section 7 gives our conclusion and insights into future work.

2. Literature Review

WSNs exhibit low power interference, bandwidth transmission, memory size, and data storage. Following these WSN regulations (strong IT resources, power supplies, and temporary communication environments), a number of security measures (including infiltration detection methods) have been developed. However, these security measures do not work directly on the WSN environment for older wired/wireless networks. Despite all of the efforts made to find a way to infiltrate WSNs [9–13], methods of energy conservation (or energy recovery [14–16,18] are intended to generate energy in the environment, and their effectiveness for sensory networks is still measured in practice, although this may be due to nodes being malicious, which has however not been thoroughly researched, and there is no doubt that wireless networks are unreliable due to device checks and off-network connections. Security outbreaks against WSNs are divided into active and passive attacks. In unmanned attacks, the square-sized attackers are often hidden from view and can be a communications network that collects data or destroys active network components. Serious attacks can be categorized using visual inspection, node anomalies, and damage and traffic testing. In intense attacks, the opponent actually marks the performance of the network attacked. This result can also lead to a targeted attack. For example, network services can be compromised or interrupted with effect of the attacks. Acute attacks are categorized as DOS, jamming, hole attacks (black hole, worm, sinkhole, etc.), floods, and Sybil attacks. Readers interested in vulnerable security attacks against WSNs can visit [19–21] for more information.

The grounds of our research claim rely on a remarkable discovery of innovation on wireless power transmission by Kurs et al. [22], which was revealed in 2007 and has since gathered attention globally. In [22], Kurs et al. utilized constant frequency resonance for the transmission of energy efficiently, wasting comparatively less energy in extraneous objects.

This article further presents a novel approach for detecting compromised nodes and permits the sensor network to stay operational forever by victimizing and optimizing the energy utilized from the detected compromised node in the legitimate sensor nodes within the network through unmanned aerial vehicles.

3. Research Statement

We contemplate the set of WSN nodes denoted by N and forwarding nodes, which were distributed over a 2D area, as shown in Figure 2. Each sensor node sends sensing information periodically to monitor the events in military surveillance to the forwarding node, considered to be a trusted sensor node, which forwards the aggregation result A_{result} calculated using the double weighted trust evaluation [23] to the base station. The sensor node's battery capacity is denoted by E_{max} initially with fully charged battery up to the

maximum capacity. The minimum energy of a node is denoted as E_{min} for WSN nodes (for it to be capably operational). The weight trust evaluation system updates the weight of the sensor node periodically after the aggregation result to detect whether nodes are faulty or malicious in the WSN to make correct conclusions in monitoring applications based on prior decisions.

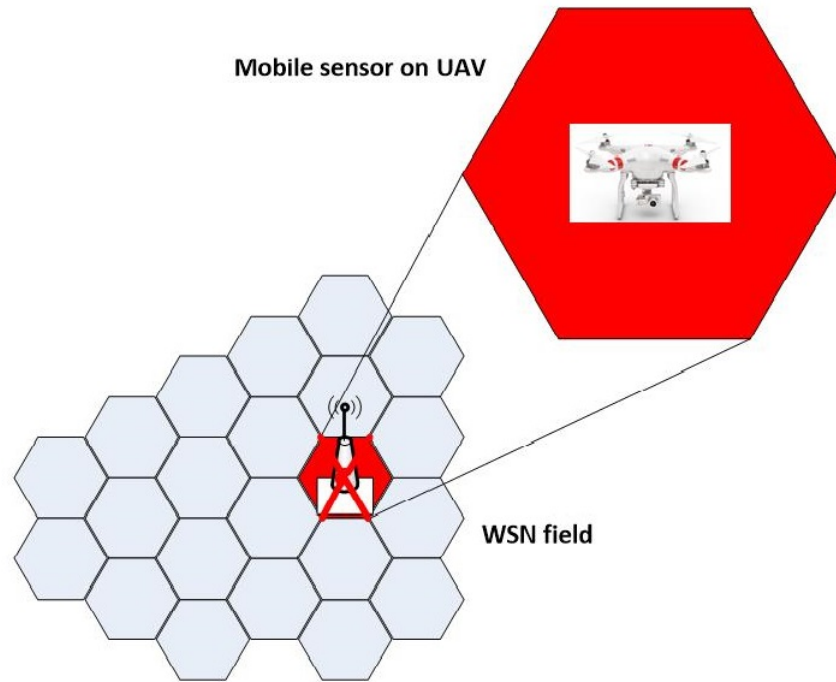


Figure 2. An example sensor network with N sensor nodes with unmanned aerial vehicles.

Affected or compromised sensor nodes transmit information to the base station. Accurate and timely identification of malicious nodes is essential to provide reliable operation of networks. Network life limitations are widely considered to be the main performance barrier to providing single network security and permanently changing the network in a wireless sensor network.

Every sensor node produces sensitive information (alarm) to monitor specific military use targets. In the divergence of a malicious node, when a node with normal characteristics starts sending an alarm, the neighboring node also starts sending an alarm after a short interval. The FN collects the sensor measurements of the corresponding sensor nodes, where “1” indicates the alarm. It calculates the weighted values as $A_{result} = 0$ or 1. At the end of the FN integration, all loads assigned to the member nodes are renewed [22,24,25].

Then, nodes with W_i that are more or less equal to a certain W_{min} converging value are identified as malicious. The W_{min} value is expected to be 0 if the load from 0 to 1 is considered a malicious terminal and is not disabled from full processing.

Every sensor node uses power to send and receive data. P_i is determined as the rate of consumption of energy by sensor node $i \in N$. In this research proposal, we utilize the certain energy dissipation [26,27]. Multi-hop data transfer is used to transfer data through nodes. The symbol f_{ij} implies that the transmission flow from the sensor network node is represented between i to j , whereas f_{iB} is the rate of flow transmission from network node i to the B , which represents the base station. The balancing constraint at every node i for the flow rate is shown by Equation (1).

$$P_i = \rho \cdot \sum_{k \in N, k \neq i} f_{ki} + \sum_{j \in N, j \neq i} f_{ji} + C_{iB} f_{iB} \quad \forall i \in N \tag{1}$$

where $C_{ij}/C_{iB} = \beta_1 + \beta_2 D_{ij}^\alpha$.

We proposed a novel approach to recharging the battery at every legitimate node: an unmanned aerial vehicle (UAV) is engaged in the network, and it is assumed that UAV is completely charged to complete a full rotation until it reaches the charging station for the next cycle. As discussed earlier, the double-weighted trust-based evaluation of nodes belonging to the network yields the value of W_i depending on the data sensed and on the aggregation result from the base station. The trusted weight for the individual node is calculated in the base station. Further aggregation result weighting is given accordingly. Faulty or malicious nodes are identified through the value of W_i . Here, we use the technology of wireless energy transfer [22] through which we can charge the sensor nodes via unmanned aerial vehicles [22,24,25]. The UAV begins from the service station (S), with its travel speed being V (in m/s). When it travels and stops at a legitimate node ($W_i \leq W_{min}$), τ_i is the interval required to charge the legitimate WSN node's battery wirelessly via the wireless energy transmission method. In the case of a malicious node ($W_i \leq W_{min}$), τ_{vac} time is taken for the UAV to be charged from the malicious node despite the node being isolated with the existing energy at the time when W_i reaches W_{min}) for the malicious sensor node. At each renewable cycle, the energy of the UAV is maximized to be spent on the legitimate sensor nodes from the energy obtained from the detected malicious nodes [25,28].

After the UAV visits all nodes placed in the network (see Figure 3), it returns to its original starting point (the service station) to be serviced and prepared for successive rounds. We denote this as a break period or the vacation period, τ_{svac} . Thanks to our proposed method, the energy acquisition ratio is maximized along the path of the cycle τ .

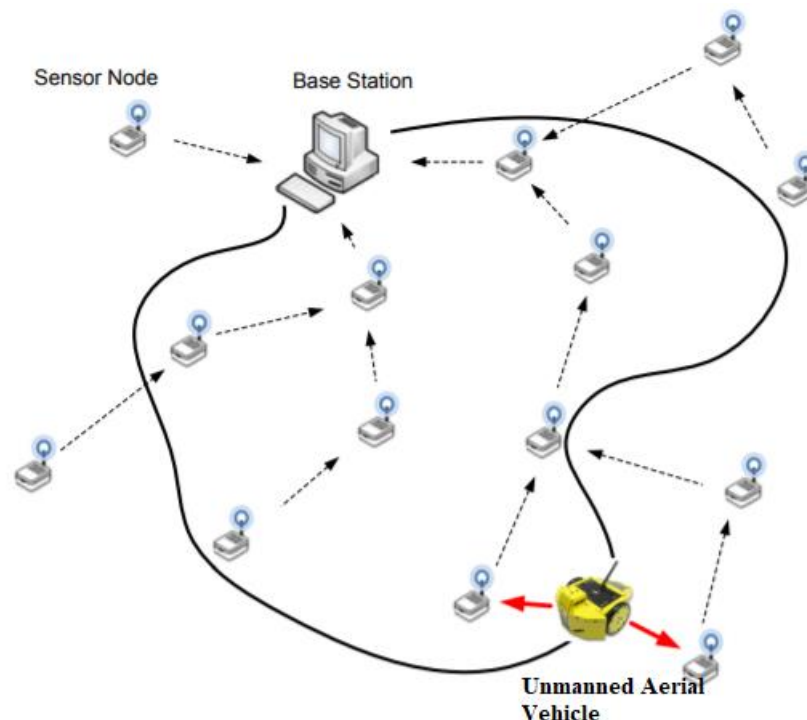


Figure 3. A UAV often visits every sensor node in regular intervals and the battery is charged via wireless energy transfer and through a compromised node.

4. Energy Transfer through UAV

Here, we present the renewable cycle framework. Let the process start with the service station; the travel of the UAV begin initially with the service station; and the travel take place over a path to reach all of the sensor nodes once in a cycle, coming back to the original position, the service station [25,28].

Path $P = (\pi_0, \pi_1, \pi_2, \dots, \pi_n)$ is the path traversed by a UAV over one cycle of the trip, starting initially with the service station and traveling over the path to reach all sensor nodes in a cycle, coming back to the original position, the service station (π_0) [25,28].

$$a\pi_i = \tau + \sum_{k=0}^{i-1} \frac{D\pi_k\pi_{k+1}}{V} + \sum_{k=1}^{i-1} \tau\pi_k \tag{2}$$

The i^{th} node reached by the UAV through path P is $\pi_i, 1 \leq i \leq |N|$. We specify $D_{\pi_0\pi_1}$ as service station as well as the initial node visited, with distance as P and $D\pi_k\pi_{k+1}$ representing the space between the k^{th} and $(k + 1)^{th}$ nodes. We set a_i as the UAV reaching time at node i in the initial roundtrip, as shown in Figure 4. We denote DP as the distance to path P and $\tau_p = \frac{DP}{V}$ as the total time spent for the distance path DP . Remember that τ_{vac} is the vacation time spent by UAV at the service station. Additionally, the rotation period τ can be represented [24,25]

$$\tau = \tau_p + \tau_{vac} + \sum_{i \in N} \tau_i \tag{3}$$

where $\sum_{i \in N} \tau_i$ is the time that the UAV devotes to all the sensor nodes for energy transfer from wireless energy transfer. The power intensity of node $i \in N$ demonstrates a renewable energy cycle when it satisfies the criteria below.

- It begins and finish with the same level of energy with a time τ and
- It does not go below E_{min}

$$\tau.P_i = i \in N \tag{4}$$

Consider the fact that the UAV reaches a node i at time period a_i through a renewable energy cycle; it does not need to recharge the sensor nodes' battery capacity to E_{max} .

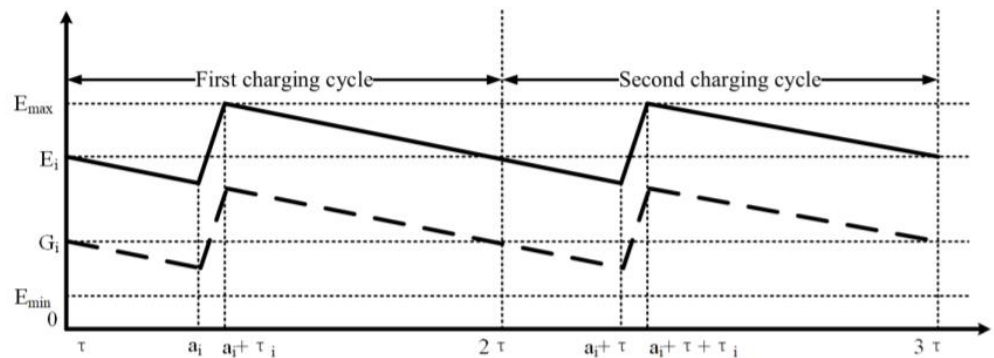


Figure 4. The nodes' energy levels for the two initial renewable cycles (moderately recharged vs. completely recharged) [22].

Gain in Energy at Sensor Node in the First Cycle

G_i symbolizes the initial energy state of sensor node i in a renewable cycle and $g_i(t)$ denotes the level of energy at time t (denoted with the sawtooth graph). During a roundtrip cycle $[\tau, 2\tau]$, we note the level of energy with only two slopes: [28] (i) a slope of p_i when the UAV is not at this node (i.e., non-charging period) and (ii) a slope of (Up_i) when the UAV is charged at a rate of U (i.e., charging period).

$$E_i = E_{max} + P_i(a_i + \tau_i) - U\tau_i \tag{5}$$

5. Energy Utility and Re-Usability Model through UAV

We propose the novel energy utility and re-usability model by considering the scenario in which the available energy from a detected malicious node is transferred to legitimate

nodes of the network to increase the lifetime of the network nodes. Thus, it reduces the DOS that occurs due to the low energy nodes [25].

Figure 5 shows the unmanned aerial vehicle energy through which the sensor nodes charged wirelessly during the energy renewable cycle.

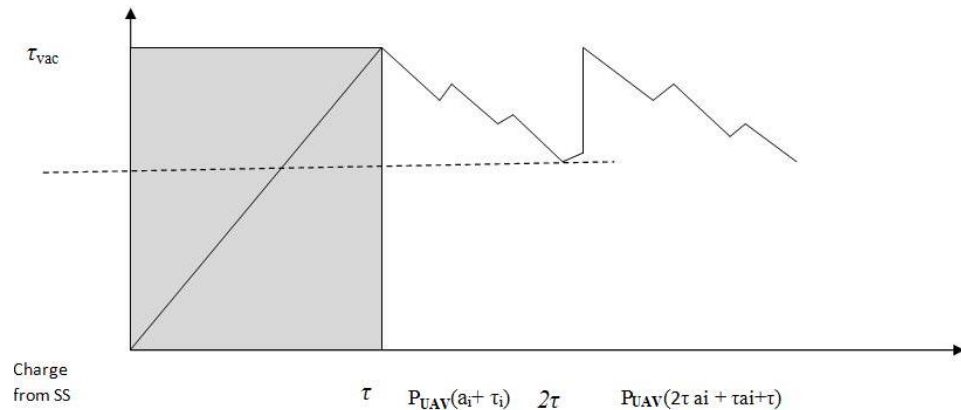


Figure 5. Shows the optimization of the energy to the legitimate sensor nodes in the network through the maximized energy of a UAV.

Considering the detected compromised nodes, the P_{UAV} energy was maximized, through which the average network life time has also been maximized [25].

Malicious node energy = $\sum_{i=1}^N P_i(\tau_i)(W_i < W_{min})$ Remaining Energy (RP) at time $a_i =$
Total Energy - Total Energy Consumed.

$$\text{Total Energy Consumed (TPC)} = \sum_{i=1}^N U\tau_i.$$

Remaining Power: After the duty cycle time, the detected compromised nodes are isolated and Tot nodes $N = N - \text{Tot node } W_i < W_{min}$

Figure 5 shows the evidence of the next cycle of renewable energy (represented with graph-Sawtooth), where E_{max} is the capacity of a battery energy charge during a UAV visit. The lifetime of the detected compromised nodes is allocated to the legitimate sensor node to optimize the energy failure among nodes in the sensor networks with practical implementation, as shown in Figure 5.

Remaining Energy

$$\text{Remaining Energy} = P_{UAV} + \sum_{i=1}^N P_i(W_i < W_{min}) + \sum_{i=1}^N U\tau_i$$

Here, we consider only the

average energy gain obtained from the detected compromised nodes at time τ_{vac} . This energy gain of UAV in addition to the charged Energy P_{UAV} at τ_{svac} has been analyzed in the Section 6.

$$\text{AverageEnergyGain} = \frac{\sum_{i=1}^N P_i(W_i < W_{min})}{N} \tag{6}$$

Equation (6) shows that the average energy gain from the detected compromised nodes is the maximum energy obtained through the energy utility and re-usability model Figure 6.

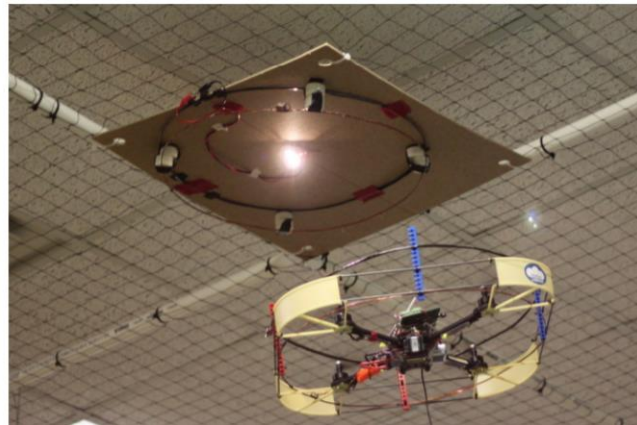


Figure 6. The energy transfer of an unmanned aerial vehicle during the two initial renewable cycles without considering the power of a compromised node.

6. Optimization of Energy Distribution

Theorem 1. *The distribution of energy attained using an unmanned aerial vehicle (UAV) from the compromised node detected using weighted trust evaluation raises an alarm. While the UAV travels on the path $P = (\pi_0, \pi_1, \pi_2, \dots, \pi_n, \pi_0)$, an alarm is raised from the node on the path π_i at the arrival time a_i and the time spent on the node i is τ_i , taking energy $p_i(\tau_i)$ of the compromised node.*

Proof. Case 1: $(W_i < W_{min}) P_{UAV}(a_i) < P_{UAV}(a_i) + p_i(\tau_i)$ (i.e) $P_{UAV}(a_i) < P_{UAV}(a_i + \tau_i)$ Here, $p_i(\tau_i)$ is the energy transferred from node i to the UAV through wireless energy transfer in addition to the total charged energy of P_{UAV} through the service station during vacation time, denoted as τ_{svac} . Case 2: $(W_i > W_{min}) P_{UAV}(a_i) > P_{UAV}(a_i + \tau_i)$ $P_{UAV}(g_i(t)) = P_{UAV} - U\tau_i$ or $P_{UAV}(e_i(t)) = P_{UAV} - U\tau_i$ Here, $U\tau_i$ is the energy charged from the UAV to the legitimate nodes during a cycle of the trip. In our proposed system, there is no loss of energy and the energy from a detected compromised node utilize. The energy is recycled to the legitimate node in the network, through which security has been enhanced, represented in Figure 7. □

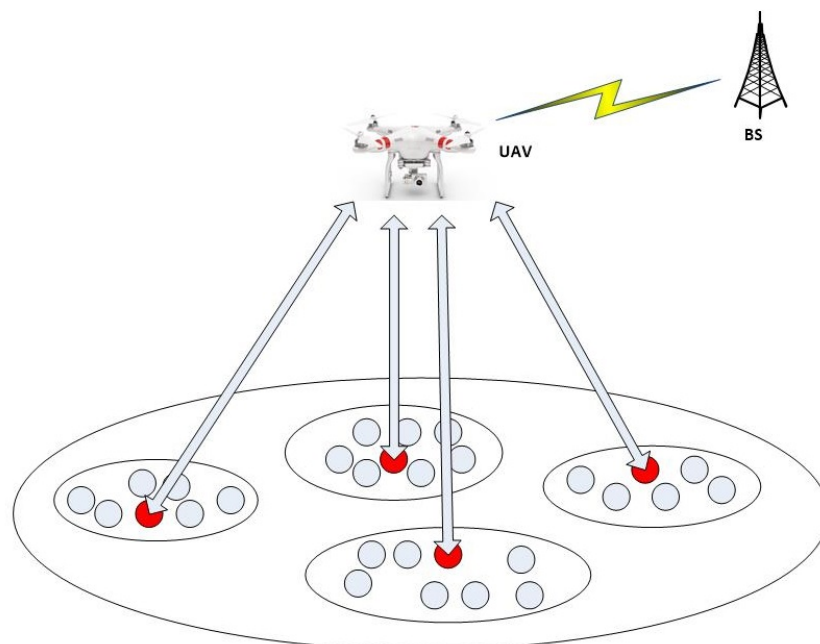


Figure 7. Optimization of energy distribution.

6.1. Optimization Proof

We prove the optimization by presenting the feasibility of reformulating the error function with respect to the normal objective and by tuning it with the controlled error gap, as shown in Equation (7).

$$\begin{aligned} \eta'_{vac} - \eta_{vac} &\leq \hat{\eta}_{vac} - \eta_{vac} \\ &= \left[1 - \sum_{s \in N} \hat{\eta}_s - \frac{u \cdot \tau_{tsp}}{E_{max} - E_{min}} \cdot \hat{\eta}_i \cdot (1 - \hat{\eta}_i) \right] - \\ &\quad \left[1 - \sum_{s \in N} \hat{\eta}_s - \frac{u \cdot \tau_{tsp}}{E_{max} - E_{min}} \cdot \eta_{max} \cdot (1 - \eta_{max}) \right] \\ &= \frac{u \cdot \tau_{tsp}}{E_{max} - E_{min}} (\gamma_{max} - \eta_{max}^2) \\ &\leq \frac{u \cdot \tau_{tsp}}{4(E_{max} - E_{min})} \cdot \frac{1}{m^2} \end{aligned} \tag{7}$$

6.2. Gain in Energy P_{UAV}

Thus, Figure 5 shows that the sum of energy gain at some points denotes $p_i(\tau_i)$ from the trips $(\tau, 2\tau\dots)$ of an energy renewable cycle.

$$P_{UAV}(e_i(t)) = P_{UAV} + \sum_{i=1}^N p_i(\tau_i) - \sum_{i=1}^N U\tau_i \tag{8}$$

$$P_{UAV}(g_i(t)) = P_{UAV} + \sum_{i=1}^N p_i(\tau_i) - \sum_{i=1}^N U\tau_i \tag{9}$$

The first renewable cycle $\tau \sum_{i=1}^N p_i(\tau_i) = 0$ in $g_i(t)$ becomes

$$P_{UAV}(g_i(t)) = P_{UAV} - \sum_{i=1}^N U\tau_i \tag{10}$$

so $P_{UAV}(e_i(t)) \geq P_{UAV}(g_i(t))$. In the another renewable cycle, $2\tau \sum_{i=1}^N p_i(\tau_i) > 0$

$$P_{UAV}(e_i(t)) = P_{UAV} + \sum_{i=1}^N p_i(\tau_i) - \sum_{i=1}^N U\tau_i \geq P_{UAV}(g_i(t)) \tag{11}$$

If $\sum_{i=1}^N U\tau_i > \sum_{i=1}^N p_i(\tau_i)$, $P_{UAV}(e_i(t)) < P_{UAV}(e_i(a_i))$. If $\sum_{i=1}^N p_i(\tau_i) > \sum_{i=1}^N U\tau_i$, check whether $N_{com} < \frac{N}{2}$ mostly satisfies $P_{UAV}(e_i(t)) > P_{UAV}(e_i(a_i))$. Furthermore, $\sum_{i=1}^N p_i(\tau_i)$ is considered τ_{ivac} . Node and UAV energy: The solution φ^* .Full achieves same maximum ratio of vacation time to the cycle time similar to the solution φ^* [25]. Under φ , it is proven that $e_i(a_i + \tau_i) = E_{max}$. Thus, it is a feasible cycle for node energy renewal. The assumption φ^* is the optimal solution for further increasing the objective value, as shown in Figure 5.

Lemma 1. At this condition, φ^β satisfies $P_{UAV}(e_i(t))$ at UAV and $e_i(t)$ at the nodes, both greater than $P_{UAV}(e_i(a_i))$ and $e_i(a_i)$, respectively, at the arrival time in our proposed solution. It satisfies the condition that both energy renewable sources and energy receiving sources co-ordinate with each other to utilize the waste energy of compromised nodes, recycled to increase the overall network lifetime.

Total energy gain at $\tau_{ivac} : N_{com} * p_i(\tau_i)$ when $(W_i < W_{min})$. This is the energy transferred to P_{UAV} in addition to the energy charged in the energy station at τ_{vac} time at cycles $(\tau, 2\tau\dots)$ until $N_{com} > \frac{N}{2}$, where the total number of nodes detected as compromised node in the network is denoted as N_{com} . P_{UAV} is maximum at some points at each cycle $(\tau, 2\tau\dots)$

when $W_i < W_{min}$ nodes transfer energy at τ_i is $p_i(\tau_i)$ to the sensor nodes by isolating the malicious nodes through the calculated weights denoted with W_i .

6.3. Optimal Travel Path

The UAV must move along the shortest Hamiltonian cycle, and the shortest travel path can be found by solving the problem called the Traveling Salesman Problem (TSP) [28]. The symbol D_{TSP} represents the distance traveled through the shortest Hamiltonian cycle, and let $\tau_{TSP} = dfrac{D_{TSP}}{V}$. The optimal travel path is

$$\tau_{TSP} + \tau_{svac} + \tau_{ivac} + \sum_i^N \tau_i = \tau \tag{12}$$

$$\tau_{vac} = \tau_{svac} + \tau_{ivac} \tag{13}$$

By our proposed system, the $\min \frac{\tau_{vac}}{\tau}$ was obtained, τ_{svac} is the time spent on the service station to be charged by a UAV, τ_{ivac} is the charging period to maximize the energy from a UAV at some points along the physical path, and τ_{vac} is period of time as mentioned in Section 6 case(1) such that $\max \frac{\tau_{vac}}{\tau}$ has been satisfied in OPT by the near optimal solution procedure in our proposed solution.

Here, in an optimized research solution with the maximum $\frac{\tau_{vac}}{\tau}$, the UAV must have traveled through the shortest Hamiltonian cycle that links all of the sensor nodes and the initial point (service station).

$$\text{OPT max } \frac{\tau_{vac}}{\tau} \text{ s.t}$$

$$\sum_{j \in N}^{j \neq i} f_{ij} + f_{iB}(i \in N) - \sum_{k \in N}^{k \neq i} f_{ki} = R_i(i \in N) \tag{14}$$

$$\rho \cdot \sum_{k \in N}^{k \neq i} f_{ki} + \sum_{j \in N}^{j \neq i} C_{ij}f_{ij} + C_{iB}f_{iB} - P_i = 0(i \in N) \tag{15}$$

$$\tau - \sum_{i \in N} \tau_i - \tau_{vac} = \tau_{TSP} \tag{16}$$

$$\tau p_i - U\tau_i = 0(i \in N) \tag{17}$$

$$\tau - \tau_i p_i \leq E_{max} - E_{min}, i \in N \tag{18}$$

$$f_{ij}, f_{iB}, \tau_i, \tau, \tau_{vac}, p_i \geq 0(i, j \in N, i \neq j).$$

In this research problem, the rate of flow f_{ij} and f_{iB} ; time periods τ , τ_i , and τ_{vac} ; and energy utilization p_i are the variables used to denote the optimization, and $R_i, \rho, C_{ij}, C_{iB}, U, E_{max}, E_{min},$ and τ_{TSP} are constants. This research issue has both a non-linear term $\frac{\tau_{vac}}{\tau}$ and non-linear terms (p_i and $\tau_i p_i$). Of note, there are two possible outcomes for the optimization problem OPT: either the solution is optimal or infeasible, denoted by OPTS. There are various scenarios where the outcomes may occur later, e.g., (i) the UAV energy charged rate is varied, and it may be very low or small or may be large; (ii) the interval between UAVs is high. Due to the problem constraints, OPT could not be held. These are some of restrictions for a UAV to regain some network energy with a maximized lifetime in a sensor network [28].

7. Results and Discussion

In the results, the proposed framework is shown to regain energy for a WSN by maximizing the energy of UAVs as well as the sensor node, with strong properties in such a network.

7.1. Simulation Settings

We consider the WSNs to consist of 50 nodes. The sensor nodes were deployed over a square area of 1 km × 1 km. The data rate (i.e., R_i , i belongs to N) from each node is random.

The data flow rate R_i and location for each node in a 50-node network is generated within [1, 10] kb/s. The energy consumption co-efficient $\beta_1 = \frac{50nJ}{b}$, $\beta_2 = \frac{0.0013pJ}{b.m4}$, $\alpha = 4$, and $\rho = \frac{50nJ}{b}$. The travel speed of the UAV is $V = 5$ m/s, and $P_{UAV} = 100$ KJ at the start of the vacation time.

7.2. Results

In this research problem, the rates of flow f_{ij} and f_{iB} ; time periods τ , τ_i , and τ_{vac} ; and energy utilization p_i are the variables used to denote the optimization, and $R_i, \rho, C_{ij}, C_{iB}, U, E_{max}, E_{min}$, and τ_{TSP} are constants. This research issue has both a non-linear term $\frac{\tau_{vac}}{\tau}$ and non-linear terms (p_i and $\tau_i p_i$). Of note, there are two possible results for the optimization issue OPT: either the result is optimal or infeasible, denoted by OPTS. There are various scenarios where the outcomes may occur later, e.g., (i) the UAV energy charge rate is varied, and it may be very low or small or may be large; (ii) the interval between UAVs is high. Due to the problem constraints, OPT could not be held. These are some of the restrictions for a UAV to regain some energy in a WSN network [22,25,29–41].

The good results estimated by the energy utility model proposed with UAV are shown in Figures 8–11.

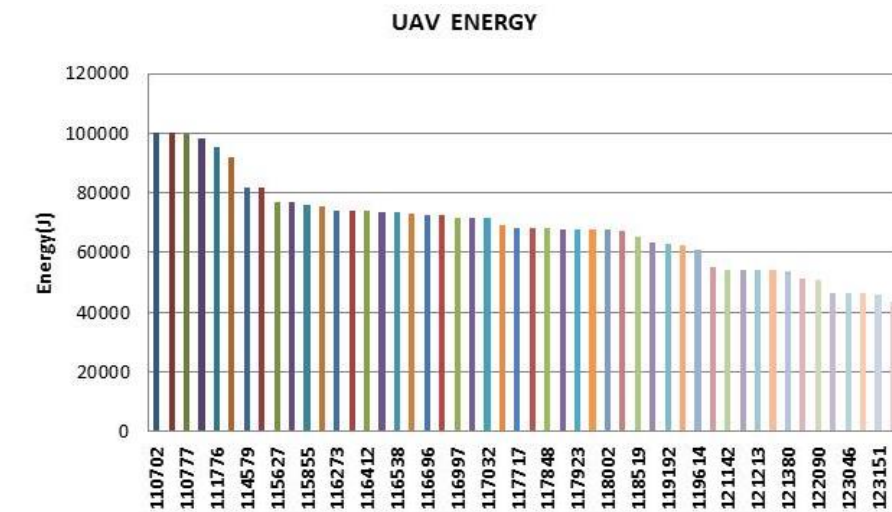


Figure 8. Energy transfer through the UAV of each node in a first renewable cycle and charging time at each node for the 50-node network.

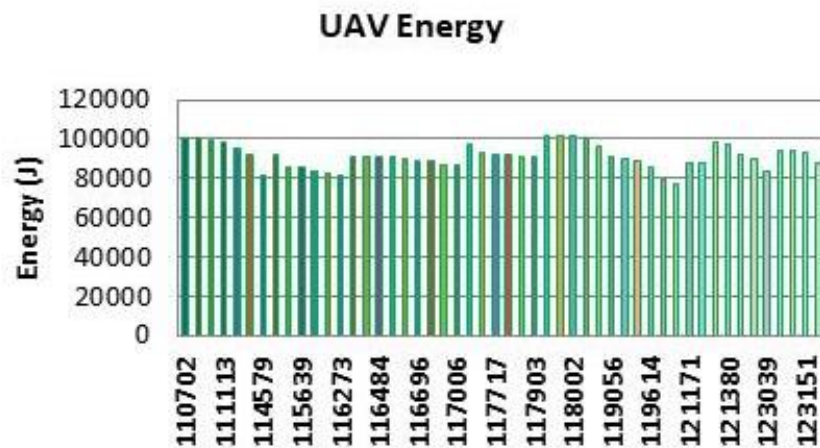


Figure 9. Maximizing the energy using the UAV utility and re-usability model from the detected compromised nodes.

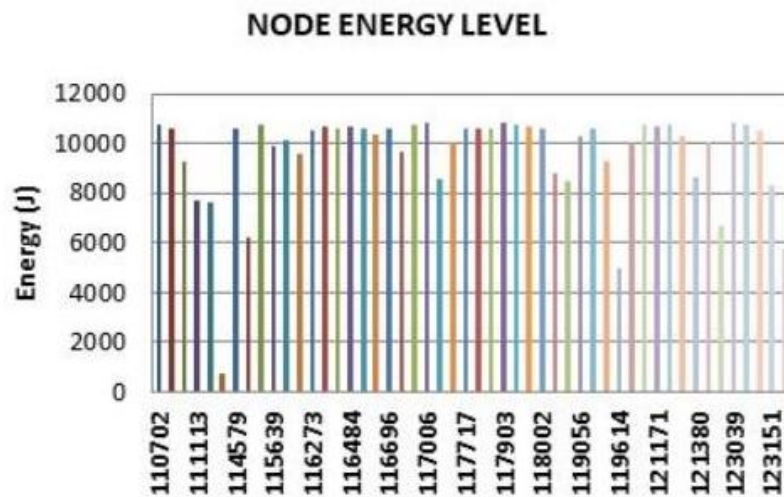


Figure 10. Node energy level at the first renewable energy cycle without energy transfer from the compromised nodes.

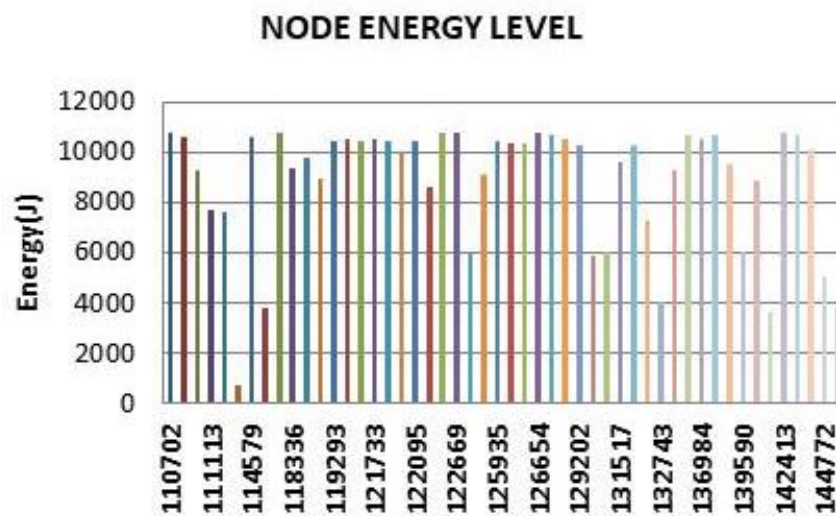


Figure 11. Node energy level using the energy utility and re-usability model with energy transfer from compromised nodes.

8. Conclusions

We found that there are energy blocking nodes in the network, with their energy dipping to a minimum. While considering a maximized P_{UAVs} through which security increased, we also optimized this type of node in the network by looking for the ratio of energy expended by each node in the appropriate travel cycle. Using the concept of SDN in WSNs, we easily tackled complex issues, such as energy utilization and maximization with network management and obtained a simplified solution. We also proposed an exclusive framework for software-defined WSNs; using that framework, we prevented this type of energy from falling to the network nodes by supplying energy with a suitable UAV. Scalability must also be achieved as the number of sensor nodes in the network escalates. Here, Kurs et al. [22] stated that transferring energy wirelessly can be achieved from a single resource node to several energy receiving nodes simultaneously. This recommends that a drone populates numerous nodes simultaneously in its travel path and therefore has the latent ability to operate within a densely deployed network of sensor nodes with security. We will discover these improvements in our future research, and future work will focus on comparing existing harvesting techniques such as backscattering based WSN, ambient-backscattering, and remappable WSN, which provide broad applications of energy utilization, and will give remarkable results within the wireless network field.

Author Contributions: Conceptualization, S.K.S. and N.M.; funding acquisition, P.M. and M.H.; design and methodology, K.R.; software, A.A.A.; visualization, S.K.S. and N.M.; writing—original draft, S.K.S. and N.M.; supervision, K.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that there are no conflicts of interest.

References

- Xie, H.; Yan, Z.; Yao, Z.; Atiquzzaman, M. Data Collection for Security Measurement in Wireless Sensor Networks: A Survey. *IEEE Internet Things J.* **2019**, *6*, 2205–2224. [\[CrossRef\]](#)
- Al-Mekhlafi, Z.G.; Hanapi, Z.M.; Saleh, A.M.S. Firefly-Inspired Time Synchronization Mechanism for Self-Organizing Energy-Efficient Wireless Sensor Networks: A Survey. *IEEE Access* **2019**, *7*, 115229–115248. [\[CrossRef\]](#)
- Islam, T.; Park, S.-H. A Comprehensive Survey of the Recently Proposed Localization Protocols for Underwater Sensor Networks. *IEEE Access* **2020**, *8*, 179224–179243. [\[CrossRef\]](#)
- Saeed, N.; Nam, H.; Al-Naffouri, T.Y.; Alouini, M. A State-of-the-Art Survey on Multidimensional Scaling-Based Localization Techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3565–3583. [\[CrossRef\]](#)
- Du, R.; Santi, P.; Xiao, M.; Vasilakos, A.V.; Fischione, C. The Sensable City: A Survey on the Deployment and Management for Smart City Monitoring. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1533–1560. [\[CrossRef\]](#)
- Chen, X.; Yu, L.; Wang, T.; Liu, A.; Wu, X.; Zhang, B.; Lv, Z.; Sun, Z. Artificial Intelligence-Empowered Path Selection: A Survey of Ant Colony Optimization for Static and Mobile Sensor Networks. *IEEE Access* **2020**, *8*, 71497–71511. [\[CrossRef\]](#)
- Basha, E.; Eiskamp, M.; Johnson, J.; Detweiler, C. UAV recharging opportunities and policies for sensor networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 824260. [\[CrossRef\]](#)
- Isolani, P.H.; Claeys, M.; Donato, C.; Granville, L.Z.; Latré, S. A Survey on the Programmability of Wireless MAC Protocols. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1064–1092. [\[CrossRef\]](#)
- Jiang, S.; Zhao, J.; Xu, X. SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments. *IEEE Access* **2020**, *8*, 169548–169558. [\[CrossRef\]](#)
- Otoum, S.; Kantarci, B.; Mouftah, H.T. On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. *IEEE Netw. Lett.* **2019**, *1*, 68–71. [\[CrossRef\]](#)
- Pundir, S.; Wazid, M.; Singh, D.P.; Das, A.K.; Rodrigues, J.J.P.C.; Park, Y. Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges. *IEEE Access* **2020**, *8*, 3343–3363. [\[CrossRef\]](#)
- Vinayakumar, R.; Alazab, M.; Soman, K.P.; Poornachandran, P.; Al-Nemrat, A.; Venkatraman, S. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access* **2019**, *7*, 41525–41550. [\[CrossRef\]](#)

13. Chen, H.; Meng, C.; Shan, Z.; Fu, Z.; Bhargava, B.K. A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation. *IEEE Access* **2019**, *7*, 32853–32866. [[CrossRef](#)]
14. O'Mahony, G.D.; Curran, J.T.; Harris, P.J.; Murphy, C.C. Interference and Intrusion in Wireless Sensor Networks. *IEEE Aerosp. Electron. Syst. Mag.* **2020**, *35*, 4–16. [[CrossRef](#)]
15. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 616–644. [[CrossRef](#)]
16. Khan, T.; Singh, K.; Abdel-Basset, M.; Long, H.V.; Singh, S.P.; Manjul, M. A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks. *IEEE Access* **2019**, *7*, 58221–58240. [[CrossRef](#)]
17. Poongodi, M.; Bose, S. Stochastic model: reCAPTCHA controller based co-variance matrix analysis on frequency distribution using trust evaluation and re-eval by Aumann agreement theorem against DDoS attack in MANET. *Clust. Comput.* **2015**, *18*, 1549–1559. [[CrossRef](#)]
18. Poongodi, M.; Bose, S. The COLLID based intrusion detection system for detection against DDOS attacks using trust evaluation. *Adv. Nat. Appl. Sci.* **2015**, *9*, 574–580.
19. Poongodi, M.; Malviya, M.; Kumar, C.; Hamdi, M.; Vijayakumar, V.; Nebhen, J.; Alyamani, H. New York City taxi trip duration prediction using MLP and XGBoost. *Int. J. Syst. Assur. Eng. Manag.* **2021**, 1–12. [[CrossRef](#)]
20. Hu, J.; Luo, J.; Zheng, Y.; Li, K. Graphene-Grid Deployment in Energy Harvesting Cooperative Wireless Sensor Networks for Green IoT. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1820–1829. [[CrossRef](#)]
21. Poongodi, M.; Malviya, M.; Hamdi, M.; Vijayakumar, V.; Mohammed, M.A.; Rauf, H.T.; Al-Dhlan, K.A. 5G based Blockchain network for authentic and ethical keyword search engine. *IET Commun.* **2021**, 1–7. doi: 10.1049/cmu2.12251 [[CrossRef](#)]
22. Kurs, A.; Karalis, A.; Moffatt, R.; Joannopoulos, J.D.; Fisher, P.; Soljacic, M. Wireless energy transfer via strongly coupled magnetic resonances. *Science* **2007**, *317*, 83–86. [[CrossRef](#)] [[PubMed](#)]
23. Poongodi, M.; Bose, S. Detection and Prevention system towards the truth of convergence on decision using Aumann agreement theorem. *Procedia Comput. Sci.* **2015**, *50*, 244–251. [[CrossRef](#)]
24. Pon, L.L.; Leow, C.Y.; Rahim, S.K.A.; Eteng, A.A.; Kamarudin, M.R. Printed Spiral Resonator for Displacement-Tolerant Near-Field Wireless Energy Transfer. *IEEE Access* **2019**, *7*, 172055–172064. [[CrossRef](#)]
25. Poongodi, M.; Al-Shaikhli, I.F.; Vijayakumar, V. The probabilistic approach of energy utility and reusability model with enhanced security from the compromised nodes through wireless energy transfer in WSN. *Int. J. Pure Appl. Math.* **2017**, *116*, 233–250.
26. Poongodi, M.; Bose, S. A firegroup mechanism to provide intrusion detection and prevention system against DDoS attack in collaborative clustered networks. *Int. J. Inf. Secur. Priv. (IJISP)* **2014**, *8*, 1–18. [[CrossRef](#)]
27. Pon, L.L.; Abdul-rahim, S.K.; Leow, C.Y.; Himdi, M.; Khalily, M. Displacement-Tolerant Printed Spiral Resonator With Capacitive Compensated-Plates for Non-Radiative Wireless Energy Transfer. *IEEE Access* **2019**, *7*, 10037–10044. [[CrossRef](#)]
28. Shi, Y.; Xie, L.; Hou, Y.T.; Sherali, H.D. On renewable sensor networks with wireless energy transfer. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 1350–1358. [[CrossRef](#)]
29. Wu, P.; Xiao, F.; Huang, H.; Sha, C.; Yu, S. Adaptive and Extensible Energy Supply Mechanism for UAVs-Aided Wireless-Powered Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 9201–9213. [[CrossRef](#)]
30. Wang, M.; Lin, Y.; Tian, Q.; Si, G. Transfer Learning Promotes 6G Wireless Communications: Recent Advances and Future Challenges. *IEEE Trans. Reliab.* **2021**, *70*, 790–807. [[CrossRef](#)]
31. Muniyappan, A.; Sundarappan, B.; Manoharan, P.; Hamdi, M.; Raahemifar, K.; Bourouis, S.; Varadarajan, V. Stability and Numerical Solutions of Second Wave Mathematical Modeling on COVID-19 and Omicron Outbreak Strategy of Pandemic: Analytical and Error Analysis of Approximate Series Solutions by Using HPM. *Mathematics* **2022**, *10*, 343. [[CrossRef](#)]
32. Ko, H.; Pack, S.; Leung, V.C.M. Energy Utilization-Aware Operation Control Algorithm in Energy Harvesting Base Stations. *IEEE Internet Things J.* **2019**, *6*, 10824–10833. [[CrossRef](#)]
33. Sun, R.; Wang, Y.; Su, R.; Cheng, N.; Shen, X.S. A Destination-Aided Wireless Energy Transfer Scheme in Multi-Antenna Relay Sensor Networks. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 689–692. [[CrossRef](#)]
34. Zhang, H.; Huang, Y.; Wang, J.; Wang, B.; Yang, L. Multiobjective Precoder Design for Coexisting Wireless Energy Transfer and Information Transmission Systems. *IEEE Syst. J.* **2020**, *14*, 445–456. [[CrossRef](#)]
35. Li, Y.; Zhao, J.; Yang, Q.; Liu, L.; Ma, J.; Zhang, X. A Novel Coil With High Misalignment Tolerance for Wireless Power Transfer. *IEEE Trans. Magn.* **2019**, *55*, 1–4. [[CrossRef](#)]
36. Poongodi, M.; Bose, S. A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET. *Arab. J. Sci. Eng.* **2015**, *40*, 3583–3594. [[CrossRef](#)]
37. Cetinkaya, O.; Dinc, E.; Koca, C.; Merrett, G.V.; Akan, O.B. Energy-Neutral Wireless-Powered Networks. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1373–1376. [[CrossRef](#)]
38. Bayguzina, E.; Clerckx, B. Asymmetric Modulation Design for Wireless Information and Power Transfer With Nonlinear Energy Harvesting. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 5529–5541. [[CrossRef](#)]
39. Wang, L.; Wu, K.; Xiao, J.; Hamdi, M. Harnessing Frequency Domain for Cooperative Sensing and Multi-channel Contention in CRAHNS. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 440–449. [[CrossRef](#)]

40. Mhamdi, L.; Hamdi, M. Scheduling multicast traffic in internally buffered crossbar switches. In Proceedings of the 2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577), Paris, France, 20–24 June 2004; Volume 2, pp. 1103–1107. [[CrossRef](#)]
41. Pun, K.; Hamdi, M. Distro: A distributed static round-robin scheduling algorithm for bufferless Clos-Network switches. In Proceedings of the Global Telecommunications Conference, Taipei, Taiwan, 17–21 November 2002; Volume 3, pp. 2298–2302. [[CrossRef](#)]