Hindawi
Security and Communication Networks
Volume 2022, Article ID 2650474, 11 pages
https://doi.org/10.1155/2022/2650474

Research Article

DS-SWIPT: Secure Communication with Wireless Power Transfer for Internet of Things

Pu Gong,[1,2] **Thomas M. Chen**,[2] **Peng Xu**,[1] **and Qianbin Chen**[1]

[1]*Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing, China*
[2]*School of Mathematics, Computer Science and Engineering, City, University of London, London, UK*

Correspondence should be addressed to Thomas M. Chen; tom.chen.1@city.ac.uk

Received 16 December 2021; Revised 12 April 2022; Accepted 12 May 2022; Published 8 June 2022

Academic Editor: Zhengyu Zhu

Internet of Things (IoT) is promptly spreading and reaching a series of domains, including many industrial applications designed for monitoring purposes. In such networks, sensitive information is being collected and transmitted by IoT devices with limited resources, which leads energy efficiency and cybersecurity to become critical. Therefore, this paper proposes a novel approach for wireless communications and power for IoT monitoring applications with the aim of achieving energy efficiency and security. The proposed solution combines the advantages of Simultaneous Wireless Information and Power Transfer (SWIPT) for wireless power transfer to remote IoT devices and Direct Sequence Spread Spectrum (DSSS) for data confidentiality. The proposed DS-SWIPT is a security improvement over the original SWIPT. Simulation results show that the proposed DS-SWIPT can achieve energy efficiency along with acceptable data confidentiality.

1. Introduction

The Internet of Things (IoT) is a popular concept that refers to smart Internet-connected devices, and most of these IoT devices are usually wirelessly linked [1]. IoT has found various industrial applications, including mobile healthcare, smart transport, smart grids, and industrial automation [2]. For instance, it is expected that more than 1.1 billion smart meters used for utility billing are predicted to be deployed by 2022. Moreover, the data generated by such kinds of sensors is predicted to generate more than 30 exabytes in total every month [3].

As in any new technology, a number of architectural and technical issues have to be solved [4]. Along with the fast and vast expansion of IoT, some problems begin to arise. As a matter of fact, most IoT devices are sensor-enabled; therefore, IoT applications might face challenges similar to those once faced by wireless sensor networks (WSNs). This paper focuses on IoT applications coevolving with monitoring purposes, such as environmental monitoring and contamination detection. Therefore, we shall consider two specific issues related to wireless communications. First, IoT devices in some wireless monitoring applications are located in remote places and must operate for long periods with minimal servicing by humans [5]. Furthermore, due to the compact size of the IoT nodes and the slow improvement in battery capacity in recent years, the energy availability of these devices is limited. Second, IoT devices are sometimes collecting sensitive or personal data that should be protected against eavesdropping [6]. The proposed solution combines SWIPT (Simultaneous Wireless Information and Power Transfer) and spread spectrum techniques. SWIPT can provide long-term sustainable power for energy-sensitive IoT devices. Direct Sequence Spread Spectrum (DSSS) that is initially designed to identify different users in the network by assigning unique pseudo-noise codes to them, in a sense, has the effect of encryption through the spread factor, adding a level of security that is not inherent to SWIPT itself [7]. Furthermore, we can take full advantage of the existing PN code assignments in DSSS to guide the SWIPT switching between different operating modes while no additional mechanism is required. Moreover, it is also noted that any

802.15.4 compatible WSN/IoT device supports DSSS related modulation as DSSS has been included in this standard [8], so no hardware upgrade is needed. To the best of our knowledge, this paper is the first to combine SWIPT with DSSS into DS-SWIPT. Rather than simply piecing together two technologies, a novel joint design is proposed to deliver a unified and efficient solution to the two crucial issues of energy efficiency and security. It is mutually beneficial for SWIPT and DSSS as both receive notable enhancements. DSSS is well known but has not been considered with SWIPT before.

The outline of this paper is as follows: Section 2 reviews previous relevant research. Section 3 illustrates the proposed network structure for the nominated IoT applications. Section 4 describes how the proposed DS-SWIPT technique works in the considered network scenario. Section 5 gives details of the SWIPT assisted secure communications within the IoT network. Section 6 discusses theoretical performance metrics for evaluations. Section 7 presents results of simulation experiments. Finally, Section 8 concludes the paper.

2. Related Work

WSN holds several features such as sensor integration, digital communication, adequate energy efficiency, scalability, and secure transmission. These capabilities make WSN an economically reasonable solution for many IoT applications related to smart farming and environmental surveillance [9, 10], including smart monitoring, smart water management, agrochemical applications, disease management, disaster-area management, smart harvesting, supply chain management, and smart agricultural practices [11, 12].

Due to the limited battery capacity in IoT/WSN nodes, it is vital to have a reliable external energy source to provide additional power. Many possible ambient energy sources for energy harvesting in wireless communications, such as solar, wind, and motion, have been discussed [13]. These sources are predictable but not controllable and hence cannot provide a stable power supply. In comparison, wireless power transfer (WPT) is a promising approach employing an artificial energy source that is fully controllable and can provide a reliable power supply for IoT devices. WPT transmits power from a source via electromagnetic waves to a capable receiver that can consume these transmitted energies by means of specific electrical components [14]. WPT has excellent potential and is meaningful for many IoT applications such as smart healthcare, where implantable biomedical devices are widely utilized. It can significantly reduce the system without additional surgery for battery replacement for an extended period of time [15]. WPT is also well suited for the IoT nodes considered in this paper that are often deployed in remote or unreachable places. Recently, WPT (especially far-field WPT) has been combined with wireless data transmission, called SWIPT [16]. Despite SWIPT being a promising approach to combine data transmission and reliable power distribution, it does not include any security features.

In the practical IoT systems where sometimes sensitive data are being collected, malicious eavesdroppers usually intend to intercept information transmissions, and this becomes a great concern for data communication; therefore, security issues have drawn increasing attention. Li et al. [17] leverage statistical learning methods to characterize the device behavior and flag deviations, which can effectively detect anomalous behaviors and improve IoT security. The authors of [18] propose artificial intelligence-based two-stage intrusion detection empowered by software-defined technology, which achieves superior performance with lower overhead in intrusion detection for IoT networks. Lu et al. [19] propose a secure communication scheme for the unmanned aerial vehicle mobile edge computing systems, which can improve the system's secure calculation capacity. Chatterjee et al. [20] propose an artificial neural network (ANN) based authentication mechanism in IoT networks that can take full advantage of the already-existing asymmetric RF communication framework without requiring any additional circuitry. Azmoodeh et al. [21] present a deep learning-based method to detect IoT malware via the device's Operational Code (OpCode) sequence, which shows robustness in malware detection together with its sustainability against junk code insertion attacks.

Originally, for military purposes, DSSS has been used in 3G CDMA mobile networks and IEEE 802.11 b wireless LANs. It is attractive for being in possession of capabilities such as antijamming, multiple access, and multipath resolving [22]. The multiple access capability is fascinating for IoT because different legitimate users can be recognized and share utilization of the system securely. Compared to other security measures available for IoT [23], DSSS is already part of the 802.15.4 standard, which means no additional hardware is required. Furthermore, the security is assured through the communication process itself, without any separate encryption operation, and causes no additional computing and energy resource consumption. To the best of our knowledge, this paper is the first to incorporate DSSS into SWIPT.

3. Proposed Network Structure for Nominated IoT Application

As mentioned in Section 1, the nominated environmental monitoring applications of this paper, such as contamination detection, usually have a cluster-based structure. Similar applications, such as the IoT-based farming monitoring network mentioned in [24] and the environmental tracking system based on wireless video sensor network (WVSN) addressed in [25], adopt the same cluster-based structure as shown in Figure 1, where the IoT nodes in the network autonomously organize themselves into interconnected clusters. Each cluster contains a cluster head or so-called fog node. It can be seen that the network's coverage area is split into several subregions, and each is monitored by a cluster of nodes. This type of architecture has adequate scalability and can be expanded for a more extensive coverage range by adding more subregions.

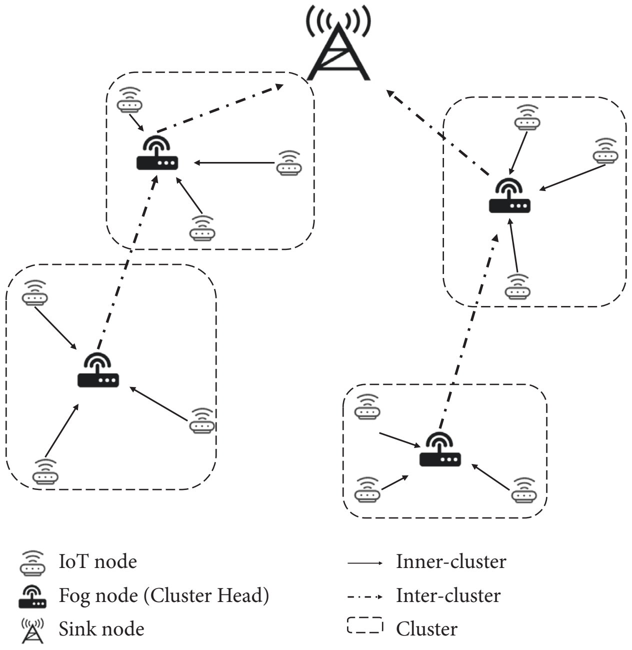

Figure 1: Cluster-based IoT network scenario.

Normal IoT nodes are compatible with the IEEE 802.15.4 standard, their main functions are environmental sensing and raw data collection, and they can be partially powered by RF (Radio Frequency) energy harvesting (see Section 4 for more details).

Data collected at these IoT nodes are first sent to their associated fog node, which serves as a gateway for all the data collected within the associated cluster before they are forwarded to other fog nodes or the sink node (serving as data aggregation and processing center). Data may be sent directly or routed through multiple hops, depending on the fog location and its distance to the destination. In the reverse direction, for example, if the sink would like to send a specific control message (such as a data collection request) to a particular node, the message arrives at this node's associated fog first before finally reaching the node itself.

4. DS-SWIPT: Joint Design of DSSS and SWIPT for IoT

The original SWIPT and DSSS sound "irrelevant" at first sight; therefore, how to take advantage of their characteristics to securely transmit the "mixed" signal (one part carrying information and the other part bringing energy) under the threat of potential eavesdroppers is worth investigating. To accomplish this, we propose to combine SWIPT with DSSS, which will be discussed in detail in Section 5.

Since the proposed solution provides unified and efficient management for secure communications and wireless power transfer, it is mutually beneficial as there are notable enhancements for both of SWIPT and DSSS:

1 For SWIPT, it initially needs an additional mechanism (see the part regarding basic architectures of SWIPT later in this section for more information) to switch itself between information decoding state and energy harvesting state properly. In DS-SWIPT, this type of switching is guided by taking advantage of existing pseudo-noise (PN) assignments in DSSS, and no additional mechanism is needed anymore.

2 Speaking of DSSS, it is even more difficult for potential eavesdroppers to overhear transmitted contents as the network is constantly changing back and forth between information transmission and power transfer in a DSSS manner. Moreover, no meaningful information is included in the power transfer stage, which may further confuse eavesdroppers. Therefore, we can expect new security gains to be illuminated in the network, in addition to the security feature already provided by the original DSSS.

More details are given in Section 5.

As mentioned in Section 3, the IoT nodes in the network are 802.15.4 compatible [26] and already equipped with DSSS, so no extra hardware or setup is required for DS-SWIPT in this paper. In addition, switching between information decoding state and energy harvesting state DS-SWIPT is now guided by assigning proper PN codes; the extra mechanism that is initially required to perform this process is no longer needed. Therefore, the complexity of DS-SWIPT is limited to minimal (roughly a factor of 1) compared to any existing WSN/IoT network.

It is also necessary to describe the role of SWIPT in an IoT network. At the receiving end, a SWIPT receiver can have one of four basic architectures: separate receiver, time switching, power splitting, and antenna switching [16].

1 Separate receiver architecture power is received by one receiver while information is received at a different receiver (naturally, the receivers have different antennas).

2 Time switching architecture receiver antenna switches alternately between information and power reception circuits in a time-dependent manner.

3 In power splitting architecture, the receiver splits the incoming signal into two parts, each with different power levels and power split ratio. Both parts are then passed to an information decoder and power harvester, respectively.

4 In antenna switching architecture, antennas are divided into two subsets, one for information reception and the other for power harvesting. Note that theses "sets" are not stationary; the antennas included in a set may change over time.

The architecture adopted in this paper can be considered as an evolved version of "time switching receiver." In addition, in this new version, as shown in Figure 2, switching between information decoding and energy harvesting is guided by the existing PN nodes assigned by DSSS, dispensing with any extra mechanism and cost.

On the other hand, SWIPT capabilities of different types of nodes need to be addressed: In the considered IoT

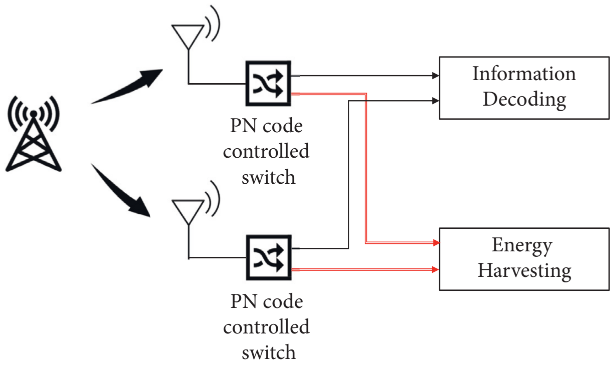

Figure 2: Revised time switching architecture.

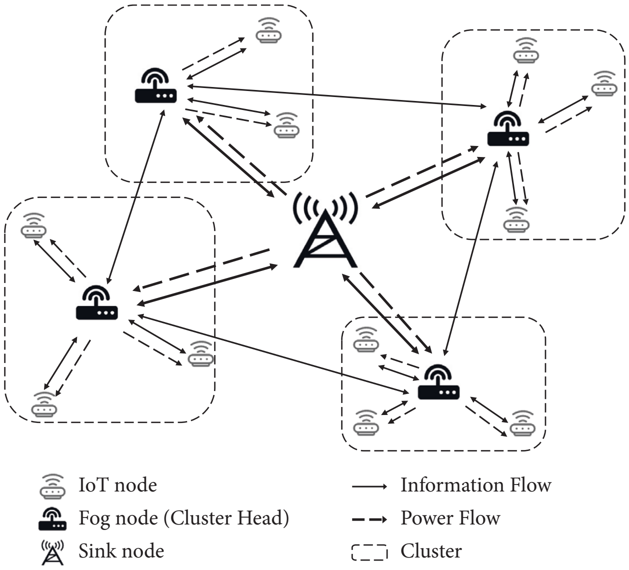

Figure 3: SWIPT capabilities of different types of nodes.

network, not all the nodes are fully capable of SWIPT. Figure 3 shows the capabilities of different nodes. Regular IoT nodes with limited energy storage can exchange information with neighboring nodes but are not supposed to provide power via WPT for others. In this case, they are just partially capable of SWIPT in the sense that they can act only as receivers rather than WPT transceivers.

Fog nodes with relatively sufficient energy storage and computational capability (compared to regular IoT nodes) are fully capable of SWIPT. They can provide additional power for its cluster members and exchange information with them.

The sink node with superior computational capacity and energy storage can provide auxiliary power for any other node in the network, and of course, it is fully capable of SWIPT.

5. SWIPT Assisted Secure Communications in IoT

All the transmissions within the network can be classified as intra-cluster communications or inter-cluster communications. The first type takes place inside a particular cluster, while the latter type comes up between fogs (cluster heads, which serve as gateways) and sometimes includes the sink.

5.1. Secure Intra-Cluster Communications. Intra-cluster communications are further categorized into two types: downlink (from fog to normal IoT nodes) and uplink (from normal IoT to fog nodes) transmissions. Due to the differences in hardware and functionalities of fog and IoT nodes, each type has different communication modes.

5.1.1. Downlink Mode (Power and Information). In this mode, the fog node can transmit power and information to its associated cluster members (whose energy storage is limited) in a DSSS manner. DSSS was initially designed to identify different users by their assigned unique PN code. Inspired by this idea, network nodes utilize this technique together with SWIPT to securely differentiate transmitted contents from one another. Only the legitimate senders and receivers know the associated PN codes of different types of content. Even though some efforts have been made to break DSSS as seen in previous papers [27], these studies reveal that the probability of "breaking" (the formal term is "blind estimation") DSSS transmission is inversely related to the signal-to-noise ratio (SNR), which means it is almost impossible for blind estimations below a certain SNR threshold. Thus, if we can maintain the communications under a certain SNR level by adjusting transmitting power properly, the eavesdroppers cannot correctly unscramble the transmitted information despite the fact that they can overhear the transmitted signal.

Three unique PN codes are assigned as follows:

1 PN code 1 denotes transmission for data (the "I" of "SWIPT").

2 PN code 2 denotes transmission for power transfer (the "P" of "SWIPT").

3 PN code 3 denotes transmission for key distribution, which is further used in uplink mode (the other "I" of "SWIPT"), or PN code update for enhanced security in downlink mode.

The receiving node can switch to its internal information decoder or power harvester appropriately based on the PN code of the transmitted signal, as addressed in Section 4.

Since the PN codes are preset in IoT nodes before deployment rather than being transmitted in the air, only legitimate nodes can obtain the PN codes. Therefore, data transmissions are in a sense "hidden" behind the power transfer, and thus it is difficult for potential eavesdroppers to intercept them as well. In this way, downlink transmissions are secure.

Furthermore, it is also possible for the operator to periodically update the preset PN codes via transmissions utilizing PN code 3. This process needs to be done at the very beginning. The member nodes should be aware of the next set of PN codes and when to start using them. At the beginning of the new set's life cycle, the first job is to broadcast the upcoming set of PN codes and determine when to replace the current one. Repeating this process can keep the network even more secure because it will be complicated for the eavesdropper to continuously and blindly estimate the ever-changing PN codes.

5.1.2. Uplink Mode (Information Only). The normal IoT nodes have limited energy storage, so they are not supposed to provide power for any other devices in the network. Therefore, in the uplink mode, only information is being transmitted. In this case, it is not possible to secure the transmission by "hiding" the information behind the power transfer.

Therefore, we need to employ a proper encryption method for confidentiality. The candidate should provide adequate security and cost as little energy as possible. Previous research [28] showed that among all the available choices, the symmetric encryption standard Advanced Encryption Standard (AES) could achieve an acceptable compromise between security level and energy cost.

The AES key is pre-generated by the fog node (which has a relatively better computational capability), and the key can be distributed to cluster members in downlink mode transmissions with PN code 3 as mentioned in Section 5.1.1. Afterwards, the IoT nodes can send information securely by encrypting them with the received key. Note that these key distribution processes are under extra protection from transmissions in a DSSS manner which has been addressed in Section 5.1.1. Thus, they can deliver even more security, in addition to that already provided by AES. Furthermore, this protection also offers another way of updating keys securely (more details are given later in this section).

The length of the AES key is a critical factor in determining the security level of the network. A longer key is naturally more secure but costs more computing resources, and vice versa. AES with 128 bit keys (AES-128) is a widely accepted standard in most situations [29], as the US National Institute of Standards and Technology (NIST) recommends that 128 bit protection is sufficient to achieve relatively lasting security (to the year 2036 and beyond) [30]. Adoption of longer keys (such as AES-192 or AES-256) can definitely offer a higher security level, but an increment in energy consumption is inevitable, which has been experimentally evaluated by previous research [31].

In addition, the key can be updated periodically for the sake of additional security. The longer the time a key is used (generating more ciphertext), the higher the chance of the key being discovered by an adversary. However, note that more frequent key update naturally incurs a higher energy cost. Previous study [32] figures out the typical minimum required key update period in IoT applications. New keys are periodically regenerated and then securely distributed by fog nodes (cluster heads) by means of DSSS manner transmissions.

There are some other traditional ways like the well-known asymmetric encryption algorithms: RSA (Rivest–Shamir–Adleman) and ECC (Elliptic-Curve Cryptography) [33]. In general, ECC is more efficient than RSA, as suggested in previous research [28]. For instance, ECC with 160 bit keys (ECC-160) is equivalent in strength to RSA with 1024 bit keys (RSA-1024), and ECC-224 is equivalent to RSA-2048. Thus, ECC shows an advantage in energy efficiency over RSA in experimental tests. The relevant costs are evaluated and compared in Section 7.

5.2. Secure Inter-Cluster Communications. Sink and fog nodes (cluster heads) are involved in inter-cluster communications. Since any fog node is fully capable of SWIPT, it can act as a transceiver in SWIPT transmissions. In this case, both uplink mode (transmissions from fog to sink, or later part of that from a normal node to sink) and downlink mode (transmissions from sink to fog, or earlier part of that from sink to a normal node) in inter-cluster communications adopt the DSSS technique which is mentioned in Section 5.1.1. Therefore, additional cryptography (like the AES mentioned in Section 5.1.2) is not compulsory to ensure secure transmission, but if adopted, the security will be enhanced.

In this case, at least two unique PN codes are assigned in inter-cluster communications:

1 PN code 1 denotes transmission for normal data (the "I" of "SWIPT").

2 PN code 2 denotes transmission for power transfer (the "P" of "SWIPT").

If enhanced security is wanted, another PN code for key distribution can be assigned as well: PN code 3 indicates that this transmission is for key distributions, which are further used in inter-cluster communications (the other "I" of SWIPT).

The receiving end of inter-cluster communications can switch to its internal information decoder or power harvester dynamically according to the assigned PN code of the transmitted signal. This is the same concept as described in Section 5.1.1.

6. Performance Model

This section highlights the energy costs that factor in network performance. The following analysis reflects the energy cost of any specific data communication (from any possible source node to any possible destination node) that may take place in the network. In addition, security concerns involved in these transmissions are addressed as well.

This section provides theoretical foundation of performance evaluation addressed in Section 7.

6.1. Energy Cost of Data Transmission in a Single Hop

6.1.1. Energy Cost Utilizing DSSS Transmissions. This cost applies to downlink mode in intra-cluster communications and inter-cluster communications, as mentioned in Section 5.1.1. Furthermore, it applies to key distribution process utilizing DSSS as well. E_{fnD} denotes the energy consumption of a specific fog node for transmitting data to a certain cluster member node. It can be calculated as follows:

$$E_{fnD} = P_{ecD}t_{pD} + K\left(P_{txD} + P_{rxD}\right)t_D, \quad (1)$$

where P_{ecD} is the electronic circuitry power consumed for generating DSSS sequences; t_{pD} is the length of corresponding processing time; K is the predicted average number of retries after the transmission attempt is successful; P_{txD} is the minimum required radio transmission power; P_{rxD} is the power consumed for receiving these sequences; and t_D is the transmitting time.

According to [34], K can be further expressed as follows:

$$K = \frac{1}{1 - \mathscr{P}_{\text{out}}}, \quad (2)$$

where $\mathscr{P}_{\text{out}}$ is the maximum tolerated probability of unsuccessful transmission (or outage probability). Based on the previous work in [35], $\mathscr{P}_{\text{out}}$ can be expressed as a function in P_{txD} as follows:

$$\mathscr{P}_{\text{out}} = 1 - \exp\left(-\frac{N_0 \beta r_{sD}^{\gamma}}{P_{txD}}\right), \quad (3)$$

where N_0 is the variance of white Gaussian noise (AWGN), β is the signal-to-noise ratio (SNR) threshold, r_{sD} is the distance between sending and receiving end, and γ is the path-loss exponent.

6.1.2. Energy Cost When Utilizing AES for Communication Encryption.

This cost applies to uplink mode in intra-cluster communications. E_{nfA} denotes the energy consumption of encrypted data transmission initiated by a certain member node in a specific cluster. It can be calculated as follows:

$$E_{nfA} = P_{ecA}t_{pA} + K\left(P_{txA} + P_{rxA}\right)t_A, \quad (4)$$

where P_{ecA} is the electronic circuitry power consumed for encrypting the information by utilizing AES, t_{pA} is the length of corresponding processing time, P_{txA} is the minimum required radio transmission power, P_{rxA} is the power consumed for receiving these sequences, and t_A is the transmission time.

6.1.3. Energy Cost When Utilizing Asymmetric Encryption (Legacy RSA or ECC) for Key Distribution.

This cost applies to alternative encryption methods for key distribution mentioned in Section 5.1.2.

E_{fnR} denotes the energy consumption of a specific fog node for transmitting encrypted data to the a certain member node, and E_{fnR} can be calculated as follows:

$$E_{fnR} = P_{ecR}t_{pR} + K\left(P_{txR} + P_{rxR}\right)t_R, \quad (5)$$

where P_{ecR} is the electronic circuitry power consumed for encrypting the information by utilizing asymmetric methods (such as RSA or ECC), t_{pR} is the length of corresponding processing time, P_{txR} is the minimum required radio transmission power, P_{rxR} is the power consumed for receiving these encrypted information, and t_R is the transmission time.

As discussed in Section 6.1.1, K can be expressed as a function of P_{txR}.

6.2. Details of Wireless Power Transfer.

This is applicable to wireless power transfer that takes place in downlink mode of intra-cluster communications and inter-cluster communications. As explained in [16], at power transfer stage, the RF power P_{rxT} at the receiving end can be calculated by means of Friis free space equation:

$$P_{rxT} = A_e \cos^2\phi \frac{P_{tx}G_{tx}}{4\pi R^2}, \quad (6)$$

where A_e is the effective area of receiving antenna, which can be further written as follows:

$$A_e = \frac{\lambda^2 G_{rx}}{4\pi}. \quad (7)$$

λ is the wavelength, G_{rx} is the gain of the receiving antenna, $\cos\phi$ is the polarization loss factor, P_{tx} is the output power at the transmitting antenna, G_{tx} is the gain of transmitting antenna, and R is the distance between sender and the receiver.

For simplicity, P_{rxT} can be rewritten as follows:

$$P_{rxT} = P_{txD}h^2, \quad (8)$$

where h is the channel gain between the sender and receiver. Therefore, the power that could be harvested and further utilized at the receiver is given by the following equation:

$$P_{ij} = \eta P_{rxT} = \eta P_{tx}h^2, \quad (9)$$

where η is the efficiency factor of the energy harvesting process. Note that (9) utilizes a conventional linear energy harvesting model, and the energy that can be harvested is linearly increased with the input RF power. The purpose of adopting such an ideal assumption is to imply that there is a loss in the energy harvesting process. In practice, the process of harvesting energy in wireless power transfer is nonlinear as addressed in [36]. Furthermore, the experimental results in [37] show that under higher conversion efficiency (over 0.8) from the energy source to electrical energy stored by the IoT device, more harvested power can be achieved by IoT devices in the network based on linear energy harvesting model. When the conversion efficiency is relatively low (less than 0.6), more power can be harvested by IoT devices in the network based on the nonlinear energy harvesting model. Therefore, the impact of the nonlinear energy harvesting model on the performance (which is evaluated in Section 7) is positive or negative, highly depending on the conversion efficiency of practical IoT devices.

Suppose the fog has a sufficient power supply; thus, from the cluster member's point of view, the power transferred from the fog node can be considered as free energy. In other words, P_{ij} can be used to fully or partially deduct the energy cost mentioned in (1) or (4).

6.3. Energy Cost in a Complete Single Transmission.

Suppose the total number of possible routes between a specific source node and a destination node is N_r and, along any n-th route (n is an integer and $1 \leq n \leq N_r$), there are J_n nodes. On any chosen n-th route, the expected total transmission cost $E(n)$ in terms of energy can be calculated as follows:

$$E(n) = E(n,1) + E(n,2) + \cdots \infty + E(n, J_n - 1), \qquad (10)$$

where $E(n,m)$ denotes the estimation of transmission cost from the m-th node on this route to its next hop (m is an integer and $1 \leq m \leq J_n - 1$).

Given that a specific routing protocol is employed, the optimal route can be determined, and the transmission cost through this route can also be calculated. Note that the way of calculating $E(n,m)$ is not constant. It depends on the transmission mode of the specific hop. Please go back to Sections 6.1 and 6.2 for more details.

6.4. Security Concerns

6.4.1. Definition of Security Performance for Key-Based Encryption. Classic key-based encryption, such as RSA and AES, has been well studied [33] in terms of design as well as how to break it. It can be concluded that, basically, the security level dramatically depends on the length of the key used. In other words, the time required to break a cipher by brute force is proportional to the length of the key. Therefore, the security performance here can be defined as, under a certain level of key strength, the time that would be spent to break encryption (obviously the longer the better).

6.4.2. Definition of Security Performance for DSSS. As mentioned in Section 5.1.1, the probability of DSSS transmission being blindly estimated is inversely related to the SNR. Thus, the security performance here can be defined as, under a certain level of SNR, the probability that the DSSS can be broken (the lower the better).

7. Performance Evaluation

As addressed in Section 1, IoT nodes are energy sensitive since their battery capacity is limited while power refill is usually impossible. Therefore, energy efficiency performance is the most crucial metric and should be evaluated in the first place. Later, in this section, the energy efficiency performance of DS-SWIPT is numerically evaluated and compared with existing competitors in terms of end-to-end energy consumption in data communication. Their performances are analyzed in simulations written in MATLAB, a number of data communications between any two nodes (so-called end-to-end communications) in the network are performed, and the energy cost of these transmissions are recorded for further analysis.

Section 1 also mentioned the importance of security in IoT applications. Even though the security performance cannot be numerically evaluated and compared with existing competitors (reasons are given later in this section), qualitative analysis is still possible and later addressed in this section.

7.1. Simulation Setup. Texas Instruments (TI) CC2538-based IoT nodes are chosen in our simulations. According to the specifications provided by TI, they are designed explicitly for WSN and IoT applications and are fully compliant with IEEE 802.15.4 standards. In addition, they have a low power level plus hardware encryption engine for AES and RSA.

Different network topology with various numbers (from 50 to 90) of clusters is created. Details of the simulation setup are given in Table 1.

7.2. Result Analysis

7.2.1. Energy Consumption Analysis in Comparison with RSA-Based Key Distribution. DS-SWIPT uses a DSSS-based method to securely distribute keys (further used in AES encrypted transmissions), while traditional measures employ legacy RSA for this purpose. Both of their costs in terms of overall energy consumption are evaluated and compared in this subsection.

As illustrated in Figures 4–6, the average end-to-end transmission cost in terms of energy at different key update frequency (from every 1000 transmissions to every 4000 transmissions) is given.

For key update frequency of every 1000 transmissions, as shown in Figure 4, both curves of RSA and DS-SWIPT show the same decreasing tendency, because as the node number increases, there will be more choices of possible routes to the destination. As a result, the routing algorithm is more likely to find routes that bring less energy usage in transmissions. DS-SWIPT consistently consumes less energy than that of RSA due to the fact that key distribution utilizing the DSSS method is far more energy-efficient than using legacy RSA. Specifically, the energy cost saved by adopting DS-SWIPT can hit up to 19.90%.

When the updating frequency drops down to every 2000 transmissions, as illustrated in Figure 5, DS-SWIPT still has better performance than legacy RSA. Nevertheless, the advantage begins to diminish, and this is because as the key updating frequency declines, the energy saved in the key distribution process by DS-SWIPT is naturally less noticeable.

As the updating frequency continues to decline to every 4000 transmissions (as can be seen in Figure 6), the performance gap between DS-SWIPT and RSA continues to shrink and, in the worst case, could be as small as 2.22%.

Based on the aforementioned discussion, it can be concluded that DS-SWIPT can overcome RSA in terms of energy consumed in data communications under various key updating frequencies. However, note that as the updating frequency goes down, the relative advantage possessed by DS-SWIPT declines as well.

7.2.2. Energy Consumption Analysis in Comparison with ECC-Based Key Distribution. DS-SWIPT uses a DSSS-based method to securely distribute keys (further used in AES encrypted transmissions), while ECC is a commonly employed encryption for the same purpose. Both of their

Table 1: Simulation setup.

Parameters	Value
Number of clusters	50–90
Type of transceiver	TI CC2538
MAC and PHY	802.15.4
Data rate	250 kbps
Length of data	58 kbytes
Encryption method	AES, RSA, and ECC
Routing algorithm	AODV-EHA [38]
Cluster size	10 nodes per cluster

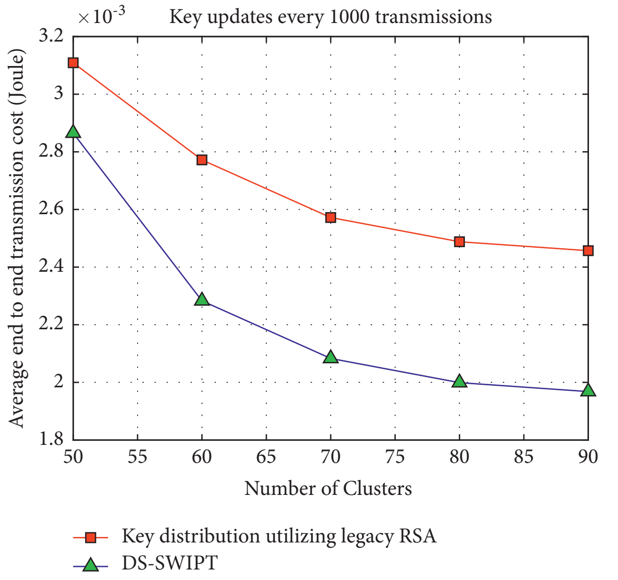

Figure 4: Energy consumption comparison when key is updated every 1000 transmissions.

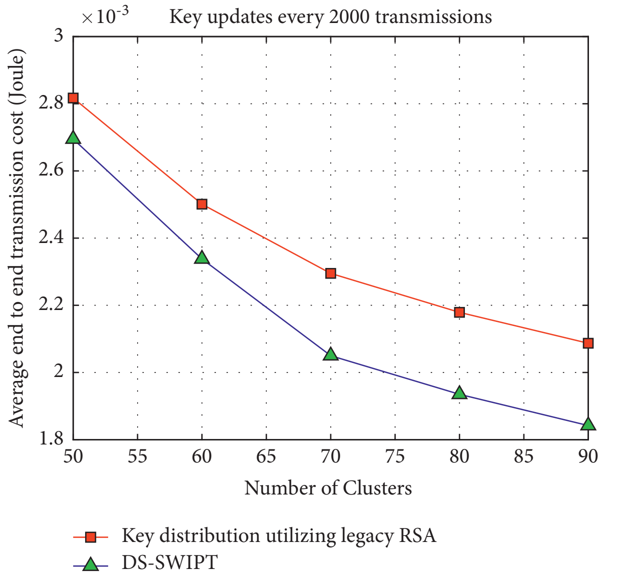

Figure 5: Energy consumption comparison when key is updated every 2000 transmissions.

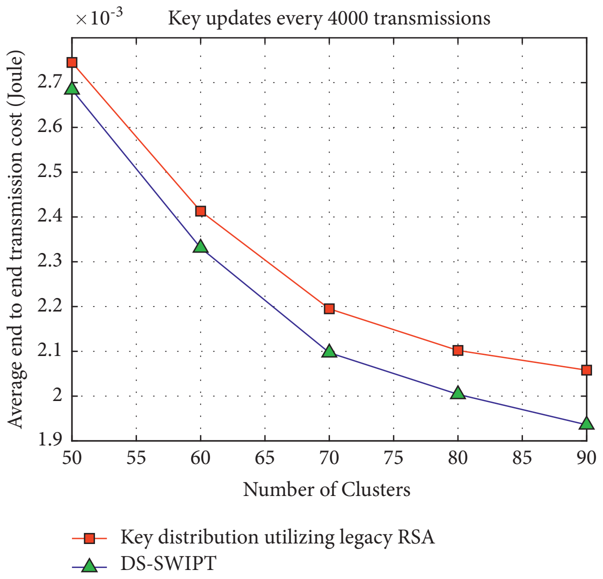

Figure 6: Energy consumption comparison when key is updated every 4000 transmissions.

costs in terms of overall energy consumption are evaluated and compared in this subsection.

As illustrated in Figures 7–9, the average end-to-end transmission cost in terms of energy at different key update frequency (from every 1000 transmissions to every 4000 transmissions) is given.

For key update frequency of every 1000 transmissions, as shown in Figure 7, both curves of ECC and DS-SWIPT have a clear decline trend. Similar to the reason already given in Section 7.2.1, with a more significant number of nodes, it is easier to find energy-efficient routes to the destination. Consequently, the routing algorithm tends to find routes with less energy usage in transmissions. Again, DS-SWIPT consistently consumes less energy than ECC. To be specific, the energy cost saved by adopting DS-SWIPT can hit up to 6.10%.

When the updating frequency drops down to every 2000 transmissions, as illustrated in Figure 8, DS-SWIPT still has better performance over ECC, but the advantage begins to shrink; this is because as the key updating frequency declines, the energy saved in the key distribution process by DS-SWIPT is naturally less noticeable.

As the updating frequency continues to decline to every 4000 transmissions (as can be seen in Figure 9), the performance advantage in terms of energy efficiency held by DS-SWIPT continues to drop and sometimes could be as small as 0.05%.

Based on the aforementioned discussions, it can be concluded that DS-SWIPT can overcome ECC in terms of energy efficiency in data communications under relatively higher key updating frequencies. Note that as the updating frequency goes down, the relative advantage possessed by DS-SWIPT becomes relatively unnoticeable. Nevertheless, compared to the commonly used ECC in resource-constraint IoT devices, DS-SWPIT requires less hardware (no discrete encryption engine is needed).

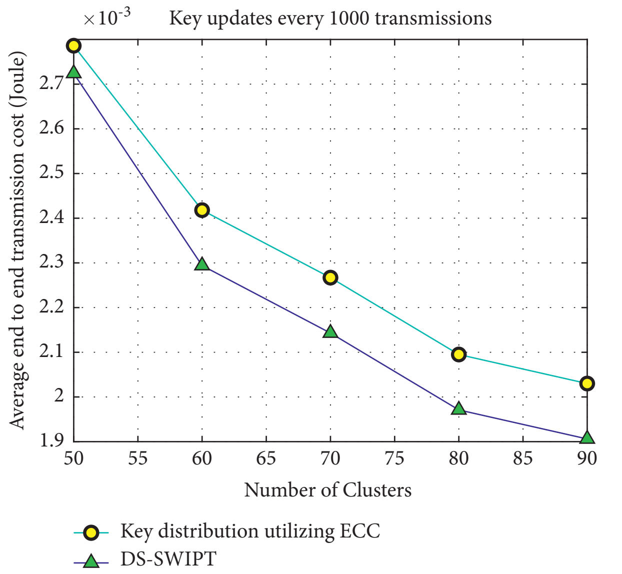

Figure 7: Energy consumption comparison when key is updated every 1000 transmissions.

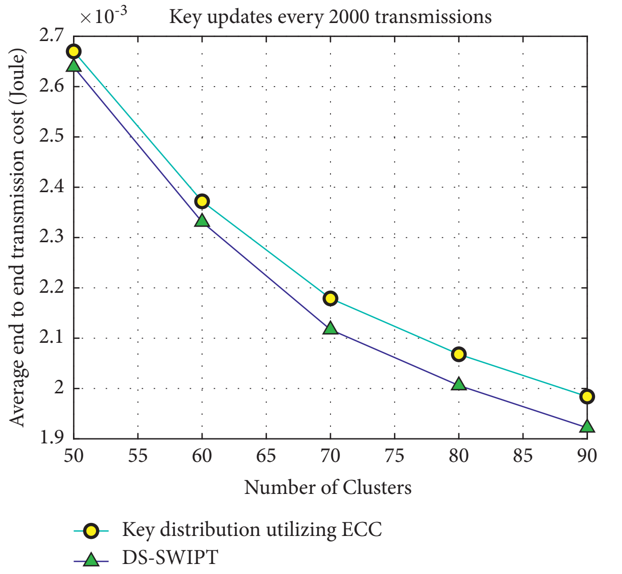

Figure 8: Energy consumption comparison when key is updated every 2000 transmissions.

7.2.3. Remarks on Security Performance Comparison. DS-SWIPT uses the DSSS-based method to securely distribute keys (further used in AES encrypted transmissions), while traditional measures employ asymmetric encryption like legacy RSA or ECC for this purpose.

As has been discussed in Section 5.1.1, when talking about breaking DSSS, it is a matter of probability that is closely related to SNR. To be more specific, the probability of successful blind estimation on DSSS transmission is inversely related to the SNR level; if we can maintain the communications under a certain SNR level, the probability of DSSS communication being unscrambled is close to zero; this is validated by the experimental results given in [27, 39].

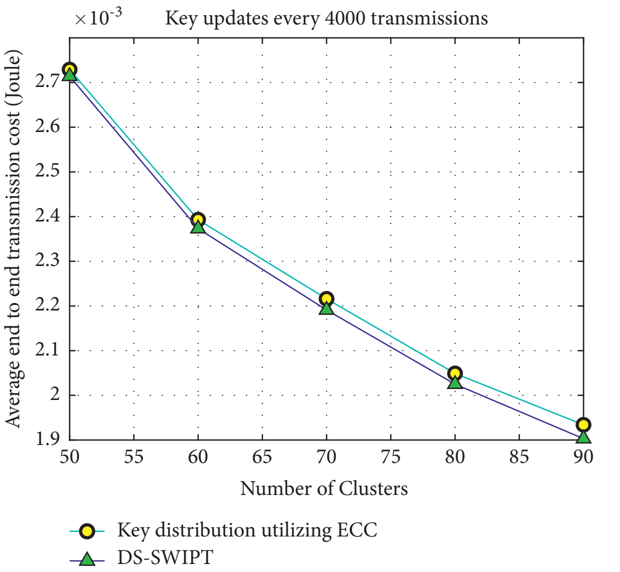

Figure 9: Energy consumption comparison when key is updated every 4000 transmissions.

On the other hand, breaking asymmetric encryption (such as RSA or ECC) is a matter of time associated with computing power. As long-standing encryption methods, both of the two methods and how to break them have been well studied [33]. It can be concluded that, in general, the security level of asymmetric encryption generally highly depends on the length of its private key. In other words, the time taken to break the ciphertext is proportional to the length of the private key.

In principle, time length and probability are not directly comparable; it is hard to tell which one is better since a fair comparison is impossible. However, looking at it another way, in the case of breaking asymmetric encryptions, no matter how strong the key is, given enough computing resources and time, the task can definitely be accomplished eventually; on the other hand, for the case of blind estimation for DSSS, if the SNR is below a certain level, the probability of "breaking" it can be very close to zero, which is roughly equivalent to "impossible." At this point, we may say, given that specific criteria are met, the DS-SWIPT has better security than conventional asymmetric encryptions.

8. Conclusion

In this paper, a novel DS-SWIPT is proposed for certain types of IoT applications. These applications coevolve with monitoring purposes and are in need of energy-efficient and secure communication solutions since the nodes comprising them are usually located in remote places. They must operate for long periods with minimal human servicing, limited computing, and energy resources. DS-SWIPT is equipped with a SWIPT feature and can provide accessible energy amid information transfer for remote IoT nodes which are hard to reach. Furthermore, it is able to offer additional security assurance in data transmissions that SWIPT does not initially guarantee by cooperating with DSSS and symmetric encryption techniques while reducing the energy cost compared to traditional methods. These advantages are evaluated and verified by simulation results.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Chongqing Natural Science Foundation Project under Grant cstc2019jcyj-msxmX0032.

References

[1] M. Zhou, G. Fortino, W. Shen, J. Mitsugi, J. Jobin, and R. Bhattacharyya, "Guest editorial special section on advances and applications of internet of things for smart automated systems," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1225–1229, 2016.

[2] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 10–16, 2016.

[3] S. Sen, J. Koo, and S. Bagchi, "Trifecta: security, energy efficiency, and communication capacity comparison for wireless iot devices," *IEEE Internet Computing*, vol. 22, no. 1, pp. 74–81, 2018.

[4] A. Samuel and C. Sipes, "Making internet of things real," *IEEE Internet of Things Magazine*, vol. 2, no. 1, pp. 10–12, 2019.

[5] M. O. Farooq, "Clustering-based layering approach for uplink multi-hop communication in lora networks," *IEEE Networking Letters*, vol. 2, no. 3, pp. 132–135, 2020.

[6] M. Safaei Pour, S. Torabi, E. Bou-Harb, C. Assi, and M. Debbabi, "Stochastic modeling, analysis and investigation of iot-generated internet scanning activities," *IEEE Networking Letters*, vol. 2, no. 3, pp. 159–163, 2020.

[7] A. Tayebi, S. Berber, and A. Swain, "Security enhancement of fix chaotic-dsss in wsns," *IEEE Communications Letters*, vol. 22, no. 4, pp. 816–819, 2018.

[8] C.-W. Hung, W.-T. Hsu, and K.-H. Hsia, "Using adaptive data rate with dsss optimization and transmission power control for ultra-low power wsn," in *Proceedings of the 2019 12th International Conference on Developments in eSystems Engineering (DeSE)*, pp. 611–614, Kazan, Russia, October 2019.

[9] G. Deepika and P. Rajapirian, "Wireless sensor network in precision agriculture: a survey," in *Proceedings of the 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, pp. 1–4, Pudukkottai, India, Feburary 2016.

[10] N. Harris, A. Cranny, M. Rivers, K. Smettem, and E. G. Barrett-Lennard, "Application of distributed wireless chloride sensors to environmental monitoring: initial results," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 4, pp. 736–743, 2016.

[11] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of things for the future of smart agriculture: a comprehensive survey of emerging technologies," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 4, pp. 718–752, 2021.

[12] A. Girma, N. Bahadori, M. Sarkar et al., "Iot-enabled autonomous system collaboration for disaster-area management," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1–14, 2020.

[13] M. L. Ku, W. Li, Y. Chen, and K. J. Ray Liu, "Advances in energy harvesting communications: past, present, and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1384–1412, 2016.

[14] K. Huang and X. Zhou, "Cutting the last wires for mobile communications by microwave power transfer," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 86–93, 2015.

[15] H. Lee, S. Jung, Y. Huh, J. Lee, C. Bae, and S. J. Kim, "An implantable wireless charger system with x8.91 increased charging power using smartphone and relay coil," in *Proceedings of the 2021 IEEE Wireless Power Transfer Conference (WPTC)*, pp. 1–4, San Diego, CA, USA, 2021.

[16] T. D. Ponnimbaduge Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (swipt): recent advances and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 264–302, 2018.

[17] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Song, "System statistics learning-based iot security: feasibility and suitability," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, 2019.

[18] J. Li, Z. Zhao, R. Li, and H. Zhang, "Ai-based two-stage intrusion detection for software defined iot networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2093–2102, 2019.

[19] W. Lu, Y. Ding, Y. Gao et al., "Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2704–2713, 2022.

[20] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2019.

[21] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 88–95, 2019.

[22] A. Sajid, A. Habib, S. Ali, and S. Ejaz, "Development of multi-user tdma-based dsss system," in *Proceedings of the 2019 2nd International Conference on Communication, Computing and Digital Systems (C-CODE)*, pp. 1–5, Islamabad, Pakistan, March 2019.

[23] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: internet of threats? a survey of practical security vulnerabilities in real iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[24] N. Ahmed, D. De, and I. Hussain, "Internet of things (iot) for smart precision agriculture and farming in rural areas," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4890–4899, 2018.

[25] A. Arar, A. Mohamed, A. A. El-Sherif, and V. C. M. Leung, "Optimal resource allocation for green and clustered video sensor networks," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2117–2128, 2018.

[26] Ieee, "IEEE Standard for Local and Metropolitan Area Networks Part 15.4: Low-Rate Wireless Personal Area Networks (Lr-wpans)amendment 5," p. 1, April 2013, https://ieeexplore.ieee.org/servlet/opac?punumber=6188486.

[27] X. Gu, Z. Zhao, and L. Shen, "Blind estimation of pseudo-random codes in periodic long code direct sequence spread spectrum signals," *IET Communications*, vol. 10, no. 11, pp. 1273–1281, 2016.

[28] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, pp. 324–328, Kauai, HI, USA, March 2005.

[29] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, Prentice Hall Press, Upper Saddle River, NJ, USA, 5th edition, 2010.

[30] S. A. Vanstone, "Next generation security for wireless: elliptic curve cryptography," *Computers & Security*, vol. 22, no. 5, pp. 412–415, 2003.

[31] A. Khalifeh, F. Alsyayid, H. Armoush, and K. A. Darabkh, "An experimental evaluation of the advanced encryption standard algorithm and its impact on wireless sensor energy consumption," in *Proceedings of the 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, pp. 1–6, Sakheer, Bahrain, December 2020.

[32] J. Han and J. Wang, "An enhanced key management scheme for lorawan," *Cryptography*, vol. 2, no. 4, p. 34, 2018.

[33] L. M. Batten, "The RSA Scheme," *IEEE*, pp. 59–79, 2013.

[34] J. H. Kleinschmidt, W. C. Borelli, and M. E. Pellenz, "An analytical model for energy efficiency of error control schemes in sensor networks," in *Proceedings of the 2007 IEEE International Conference on Communications*, pp. 3895–3900, Glasgow, UK, June 2007.

[35] A. K. Sadek, W. Yu, and K. J. R. Liu, "On the energy efficiency of cooperative communications in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 1, pp. 1–21, 2009.

[36] Y. Wang, Y. Wu, F. Zhou, Z. Chu, Y. Wu, and F. Yuan, "Multi-objective resource allocation in a noma cognitive radio network with a practical non-linear energy harvesting model," *IEEE Access*, vol. 6, Article ID 12973, 2018.

[37] Z. Wang, T. Lv, and W. Li, "Energy efficiency maximization in massive mimo-noma networks with non-linear energy harvesting," in *Proceedings of the 2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Nanjing, China, March 2021.

[38] P. Gong, Q. Xu, and T. Chen, "Energy harvesting aware routing protocol for wireless sensor networks," in *Proceedings of the Communication Systems, Networks Digital Signal Processing (CSNDSP)*, pp. 171–176, Manchester, UK, July 2014.

[39] S. Mehboodi, A. Jamshidi, and M. Farhang, "A low-complexity near-optimal algorithm for blind estimation of pseudo-noise sequences in dsss communication systems," in *Proceedings of the 2016 8th International Symposium on Telecommunications (IST)*, pp. 218–221, Tehran, Iran, September 2016.