Hindawi
Journal of Computer Networks and Communications
Volume 2023, Article ID 5926294, 11 pages
https://doi.org/10.1155/2023/5926294

Research Article

Novel Framework for Secure Data Aggregation in Precision Agriculture with Extensive Energy Efficiency

G. S. Nagaraja,[1] K. Vanishree,[2] and Farooque Azam[3]

[1]*Department of Computer Science and Engineering, RV College of Engineering, Bengaluru, India*
[2]*Department of ISE, RV College of Engineering, Bengaluru, India*
[3]*School of Computer Science and Engineering, REVA University, Bengaluru, India*

Correspondence should be addressed to Farooque Azam; farooque.azam@reva.edu.in

Received 23 September 2022; Revised 5 January 2023; Accepted 6 February 2023; Published 24 February 2023

Academic Editor: Ihsan Ali

Precision agriculture (PA) is the next generation of a technological revolution in smart farming, where sensing technology is the core technological player. Energy-efficient data transmission in PA via sensing technology is possible only when additional security measures are synchronized. Nevertheless, security considerations often introduce additional overhead. Thus, it is necessary to develop an efficient mechanism to achieve an optimal trade-off between security and resource efficiency. The prime purpose of the proposed study is to introduce a lightweight communication protocol that can ensure an adequate balance between energy efficiency and maximum-security demands to benefit the success of PA. This paper proposes a synchronized framework where unique public-key encryption has been used, unlike any existing approach to facilitate the participation of legitimate on-field sensors in PA. On the other hand, an algorithm for energy efficiency where unique structural management of routing is discussed concerning aggregator nodes. In contrast, the security algorithm discusses a uniquely progressive and noniterative mechanism to perform secure data aggregation with a parallel validation technique. The proposed logic is scripted in MATLAB, considering a suitable PA environment where comparative assessment is carried out on a uniform testbed. The study outcome exhibited the effectiveness of the proposed scheme concerning better energy efficiency and higher resiliency from threats in contrast to existing schemes.

1. Introduction

The beneficial aspect of technological advancement has penetrated agriculture, leading to Precision Agriculture (PA) [1]. It can be discussed as exclusive management of farming, designed based on various external measurements associated with farming and the surrounding environment [2]. The concept of PA mainly relates to making an appropriate decision so crop cultivation can be optimized without much dependency on the usage of resources [3]. The conventional state of PA makes use of satellite-based information, e.g., Global Positioning System (GPS) and Global Navigation System (GNSS) [4]. This technology is also integrated with other sensing technology to make it more effective. Another conventional technology is variable rate technology (VRT), which was adopted to improve farming resource distribution. Apart from this, unmanned aerial vehicles, e.g., drone, is another frequently used technology to acquire imageries and other associated farming information [5]. Such information assists the farmers in deciding to adopt certain measures to resist upcoming environmental risks or improve production in PA. Out of all this, sensing technology is very cost-effective. It is easier to install in agricultural farms where the aggregated data could offer more comprehensive information about the farming land [6]. In this perspective, existing studies show that Internet-of-things (IoT) has been slowly adopted in smart/intelligent farming, which will accelerate the practical implementation of PA [7–9]. The usage of IoT will demand three things, viz. (i) usage of IoT device (or on-field sensors) to acquire direct data of plant, soil, or environment and forward to the sink node, (ii) a gateway node that offers translation service to

ease off the communication among different variants of sensors, and (iii) all the aggregated data being forwarded to distributed cloud-based storage unit called as datacenter [10]. Implementing and deploying this essential characteristic of IoT is not a difficult task. However, the challenges start next once IoT is deployed. The conventional IoT network uses independent on-field sensors, which could be extremely challenging to maintain both in terms of security and resource management. One effective solution is to implement a wireless sensor network (WSN) to create a compact network of on-field sensors and imply the process of data aggregation in conventional WSN to assist in PA. However, due to the inherent characteristics and vulnerabilities associated with WSN, this brings a significant security concern regarding the data aggregation process in agricultural farms.

On the other hand, ensuring efficient use of network resources (energy) is another important concern towards the long-term sustainability of farm ecosystems in PA. However, owing to the developing practical usage of IoT and WSN, there are still greater issues with secure data transmission when IoT is integrated with WSN. Currently, many energy-efficient protocols exist in both WSN [11] and IoT [12]. There are also many security protocols in WSN [13] and IoT [14]. However, they are not interoperable and cannot be directly implemented when two collaborative environments are used in PA. One of the essential problems identified is developing a security approach applicable in the scenario of PA using WSN, ensuring a good balance with energy efficiency. Hence, the proposed study aims to develop a novel yet simplified computational scheme of secure energy efficiency considering WSN deployment over the farming land. The idea of the study is to ensure that every node properly identifies malicious nodes using an exclusive authentication policy. The secondary idea of the proposed system is also to resist any form of an unknown attacker to the WSN deployed into the in-farming land.

The organization of this manuscript is as follows: Section 2 discusses existing literature about energy efficiency and security in WSN applicable for PA, and Section 3 highlights the essential limitation of existing studies. In contrast, Section 4 discusses the adopted methodology of the proposed study. The algorithm is discussed in Section 5, and the result analysis is given in Section 6, while Section 7 concludes the paper.

2. Related Work

Various variants of literature emphasize energy efficiency and security incorporation in WSN; however, as the proposed study is oriented towards investigating WSN concerning PA, only the studies where WSN is investigated concerning PA are considered in the study directly or indirectly.

2.1. Existing Approach to Energy Efficiency. Data aggregation potentially affects a network's lifespan [15]. Therefore, various schemes in this direction aim to connect network lifetime with energy efficiency. The approaches towards energy efficiency mainly emphasize the routing scheme that targets saving energy and addressing other associated issues. The most recent work of Azarhava and Niya [16] has implemented an energy harvesting mechanism for WSN, one of the frequently adopted schemes in PA. This work aims to develop a resource allocation model to minimize the cumulative consumption of energy to achieve higher energy efficiency and optimized throughput. A similar direction toward the energy-harvesting scheme has also been carried out by Ait Aoudia et al. [17], where a reinforcement-based learning scheme has been utilized. This scheme performs energy management based on the temporal aspect of environment dynamics using linear approximation. This model can be directly used in PA. The work by Zhang and Cai [18] has constructed a routing scheme using a double-hop probability approach considering a case study of underwater sensing. The sustainable route is based on forwarding number, residual energy, and node depth. Along with energy efficiency, the model offers a better packet delivery ratio. The existing system has also witnessed an optimization-based approach to achieve energy efficiency. The recent work of Wang et al. [19] has harnessed the hybrid ability of particle swarm optimization and ant colony optimization for addressing the network dissipation issues in WSN. PA has not witnessed much with a bio-inspired algorithm, but this approach could directly contribute to energy efficiency. A smart environment is another better option in PA for intelligent data transmission. Hence, a recent study by Ammad et al. [20] used fog computing over an IoT-based environment to improve network lifetime. Zhao et al. [21] have implemented another bio-inspired algorithm where the coverage issue is emphasized concerning energy problems. In addition, there is much literature on energy-aware approaches in WSNs-enabled agriculture systems. Deng et al. have established a model for energy collecting from several sources [22]. The work performed by Yu et al. [23] designed a single-hop communication protocol for decentralized WSNs for energy harvesting. An approach of information fusion is considered in the work of El-Fouly and Ramadan [24] for enabling energy-aware routing operations in WSN. In addition, the application of solar energy is used in the work of Gulec et al. [25] for energy harvesting and extending network lifespan significantly. Apart from this, studies are also conducted considering using mobile agents for energy efficiency during data aggregation (Mehmood et al. [26]). Further, the scheduling-based methodology is also witnessed to improve the energy efficiency in WSN, as noted in the work of Khan et al. [27]. There is also usage of 3D printing by (Estrada-López et al. [28]), and the fuzzy logic mechanism by (Jamroen et al. [29]) for enabling higher energy efficiency in the sensory network.

2.2. Existing Approaches of Security. Different security approaches had evolved in times when the focus was on farming. The recent work of Sontowski and Zhang [30] has presented a scheme to resist cyber-attack and denial of service. Using Raspberry Pi prototyping, the proposed system has developed a scheme for resisting deauthentication attacks owing to the

adoption of the frequently used IEEE standard of 802.11 in PA. Another recent work by Astillo et al. [31] implemented a mechanism to model the misbehavior of attackers in a farming environment. The study has developed rules for resisting attack environments in IoT using the Kalman filter. Another essential finding of this study is that IoT is one of the best options for improving PA process management both on a small and large scale. However, the IoT itself is shrouded by various security loopholes. Iqbal et al. [32] discussed associated security issues in IoT, where the software-defined network offers better decision-making while constructing countermeasures towards security threats in IoT. The work carried out by Fu et al. [33] is the only study carried out in the present time where both security and energy factors are focused. This study focuses on the connectivity between the threats in the agricultural farm and power supply using a mathematical modeling approach. It should be noted that smart farming is an integral part of PA in upcoming times, and various security challenges are associated with it. Various threats such as those cyber-attacks, are consistent in various smart appliances; hence, smart farming is not an exceptional case. This fact was discussed in the study of Gupta et al. [34]. At the same time, the paper also discusses a multilayered architecture that focuses on retaining maximum privacy levels in smart farming. In this case, various smart devices (e.g., drones, on-field sensors, machinery, and attached sensors over animals) communicate with an edge gateway to connect with the cloud services. The existing system has also witnessed the increasing usage of blockchain to secure such smart and intelligent farming (Wu and Tsai [35]). The adoption of blockchain increases the capability to defend against distributed denial-of-service. A bilinear pairing is applied to construct network security, which can authenticate the sensor nodes' identity. It also ensures greater privacy as the data are chunked and stored over different distributed ledgers every time, making it nearly impossible for attackers to access. The potential feature of blockchain for securing the communication environment in PA is also discussed by Ferrag et al. [36]. Further, the work carried out by Mehmood [37] has presented a session key design concerning healthcare applications. The scheme is highly dynamic and performs key re-initiation in case of a positive threat event. According to this discussion, privacy is the prime target when applying blockchain in farming. Therefore, it can be seen that there are split versions of research work being carried out with highly scattered approaches to solving both energy and security problems.

3. Research Problem

After reviewing the objectives, problems addressed, the methodology adopted, and the outcome achieved in the existing system, a certain conclusion has been derived. The open-end research problems associated with the existing approaches are as follows:

3.1. Less Emphasis on Energy Efficiency. There is no doubt about large archives of literature associated with improving energy efficiency in WSN. However, these solutions are not much applicable when WSN is deployed in PA. There is a need for energy-efficient techniques which can work in a distributed manner with an extensive saving of resources without compromising the data quality. Hence, the primary issue is that existing energy-efficient approaches must be fine-tuned to work on a large scale and distributed environment of PA, adhering to its real-time constraints.

3.2. Complex Security Approaches. There are some dedicated attempts where complex and sophisticated security mechanisms are implemented in smart/intelligent farming applications. This is highly beneficial for resisting potential threats such as cyber-physical attacks, but such security benefits come at the cost of resource consumption. A cost-effective security protocol must never affect communication performance by affecting the resources. Unfortunately, the existing state of work towards security in PA has never been carried out considering the energy aspect of it.

3.3. Attack-Specific Scenario. The present study on security improvement highlights that they consider a predefined attack scenario. It will mean that the solution model has a well-aware definition of the adversary and its launching strategy. Such security mechanisms are never applicable to different scenarios with different attack variants, making the existing security solution highly attack-specific and computationally expensive.

3.4. Few Studies with Energy and Security Together. The tools and systems used in PA have different variants of types of machinery, actuators, and on-field sensors, and out of all, sensing technology is commonly used in almost all the standard, conventional, and unconventional approaches. Hence, it is eventual that they will expend more energy to carry out a specific operation. At the same time, machinery with two different sensors will be very hard to protect when exposed to the same threat, as the solution to resisting threats could depend upon the system parameter. In short, a combined study of energy and security issues can bridge this trade-off in WSN over PA.

Hence, the statement of the problem of the existing study will be "incorporating a higher degree of security resiliency along with maximum retention of energy over the on-field sensors in PA is a challenging task."

4. Research Methodology

Developing a security approach for resource-constrainedon-field sensors and ensuring a higher degree of energy efficiency is a bigger challenge, especially if it is related to a large deployment area. This research challenge is addressed in the proposed study, where a combined emphasis on a resilient security approach and energy efficiency is achieved. The proposed research work considers an analytical modeling strategy to develop this framework for accomplishing security and energy efficiency.

The idea of an energy efficiency security approach in the proposed system is designed based on the following foundation concept viz. (i) reducing a load of all the on-field sensors to carry out data aggregation, (ii) developing the security approach using public-key cryptography, which offers faster execution and lesser dependency of storage. This concept will have two benefits viz. (i) reduced memory consumption with reduced occurrence of key storage will lead to faster operation, and extensive residual energy, and (ii) absence of stored information about private key will lead the attacker with no information about the security variable being used. The proposed study adopts an analytical approach and introduces the modeling of an energy-aware secure data aggregation scheme for PA. The proposed scheme is implemented using a set of specific network parameters and simplified public-key encryption in PA. The schematic representation of the methodology adopted in the system design is shown in Figure 1.

As shown in Figure 1, the main components of the proposed system are subjected to secure communication and data transmission. The modeling of each component of the system is carried out phase-wise. The system design assumes that a sensory device performs a progressive generation of security tokens to ensure multilayered security at each communication process. In contrast to existing approaches that use key management planning, the proposed system provides efficient and low-cost modeling of the security function that does not rely much on storing secret information and only emphasizes secret key generation.

It will mean that the secret key is generated only when requested, and the generated key is stored in a temporary buffer and instantly used for authentication. Once used, the secret key is disposed from the temporary buffer of the node, and thereby no information is finally stored in node memory. This way, it does not pose memory overhead problems while executing security operations. The ends of the system are connected to large cloud-based storage units that accept public keys, generate encryption keys for public-key operations, and generate private keys via sensors. The proposed study also introduces an aggregator node mechanism for authenticating the fused and aggregated sensory information. The core ideology is maintaining maximum safety and energy efficiency on a single target. The next section describes the implementation process that combines maximum safety features in an energy-efficient manner.

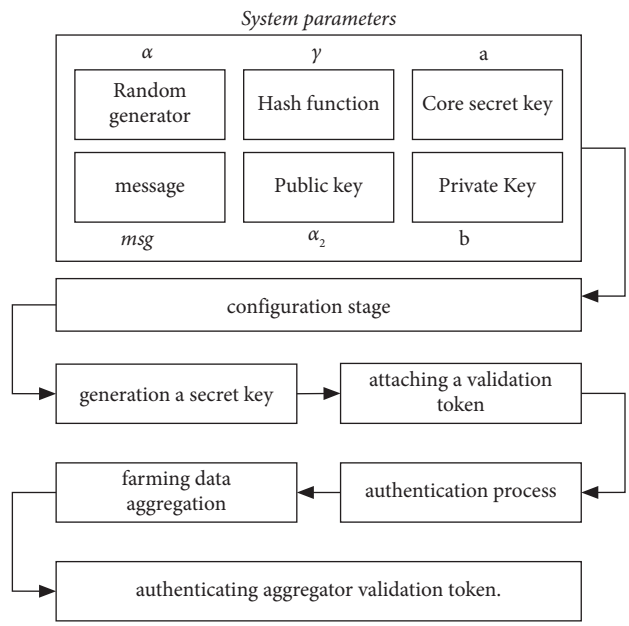

Figure 1: Block diagram of the proposed system.

5. Algorithm Implementation

This section discusses the algorithm of the proposed system, which caters to the dual purpose of (i) energy efficiency and (ii) security. An algorithm is a single unit for the proposed system; however, it is discussed concerning energy efficiency and security consideration for better illustration. Following is the discussion of the proposed algorithm:

5.1. Energy-Efficient Data Aggregation in PA. A large dimension of a farming area will possess a massive number of on-field sensors, eventually dissipating the energy required to carry out data aggregation. If all sensors carry the sensed data and forward it to the sink node, most will need to bear this transmission load. This algorithm addresses this problem, classifying the complete farming area into a smaller subfarming area. The core idea of this algorithm is to select a specific node that is potentially capable of aggregating the sensed data from the respective subfarming area to the sink node in the farming land. This will reduce the data transmission load from all the sensors, leading to extensive energy conservation. The significant steps for implementing energy-efficient data aggregation in PA are discussed in Algorithm 1. The algorithm takes the input of n (number of sensors), $s_{x,y}$ (position of sink), A (farming area), $d_{x,y}$ (datacenter position), E_o (initial energy), and n_{ag} (number of aggregator node) that after processing yields to an outcome of d (forward aggregated data). The algorithm initializes a specific number of on-field sensors n in a farming area of A with a fixed position of sink node $s_{x,y}$. The position of the sink node can be changed to any position within A.

The proposed algorithm disperses all the on-field sensors in a random fashion where (x_r, y_r) are random positions of the nodes within the coverage of the data center position d_{xy}. The complete farming area A is divided into a certain number of small areas called farming group f_g, where each farming group consists of one aggregator node n_{ag}. The algorithm then declares its arbitrary number α_o obtained by multiplying a random number a (core key) with prime number α, and it computes the public key of the distributed cloud-based storage unit α_2 by multiplying another random number b with prime number α.

It should be noted that the prime difference between the proposed and any existing public key encryption protocol is that the public key in the existing scheme is used as a default and is publicly accessible. In contrast, the public key of the proposed scheme is encrypted and still publicly available. The interested node using this public key must

```
Input: n, s_{x,y}, A, d_{x,y}, E_o, n_ag
Output: d
Start
init n, s_{x,y}
    (x_r, y_r, d_{x,y}) ← rand(n, A, d_{x,y1})
    f_g = (div(A), alloc n_ag)
α_o ⟶ (a. α) & α_2 ⟶ b. α
(η_1, η_2) = f_1(α)
T_fr = argmax(f_g)
T_1 = f_2(p, t)
For i = 1: T_fr
    ind ← ix(n_act)
    Apply Algorithm 2
    For j = 1:length(ind_2)
      If arb < T_1
        G(ind(ind_2(j)) = N_n
        selected_ag = 1
        d_agg ⟶ flag forward data
      End
    End
End
End
```

Algorithm 1: Energy-efficient data aggregation.

confirm its identity first to have access to it. Moreover, the proposed scheme generates a mechanism to perform node indexing which any attacker cannot replicate. Hence, an extra layer of security is formulated in the proposed public key encryption.

The next process of this algorithm is to obtain two cyclic groups, η_1 and η_2, by applying an exclusive function $f_1(x)$, an arbitrary number generator. The algorithm then computes the maximum number of the farming groups present in f_g to obtain a structure of the total farming region T_{fr}. Further, the algorithm applies a cut-off for opting for the proportion of nodes that will be considered aggregator nodes. It will mean that aggregator nodes are selected from the normal sensor nodes. An explicit function $f_2(x)$ is applied over the input argument of p and t, representing the probability of selecting a sensor node as an aggregator node and simulation time t.

It should be noted that parameters p and t are a part of the primary input for this algorithm, along with other input arguments. For all the total farming region T_{fr}, the algorithm initially finds if the sensor is a member of the subfarming region, followed by searching for only alive nodes. Nodes with a minimum of residual energy E_{th} are considered alive nodes. The algorithm then extracts the index *ind* of alive nodes nact where the variable *ix* represents the index of all nodes within a specific subfarming region. *Ix* is a method formulated as a two-dimensional matrix that assigns a new index to the sender and receiving nodes as a ticket to perform legitimate communication.

The algorithm then executes the second algorithm, which incorporates secure authentication of all the participating sensors for data aggregation. Once the security algorithm has performed its execution, the outcome of it results in identifying if the target node is regular or malicious. Once it is found to be a regular node, it performs the further operation. In this situation, all the index ind_2 of the candidate aggregator node is chosen where an arbitrary number *arb* of generated and compared with the threshold T_1. The variable ind_2 represents the index of the next aggregator node, i.e., the candidate node. Further, the aggregator nodes are selected from the candidate aggregator node N_n, where G represents initialized values for all the nodes. Therefore, the statement $G(\text{and } (\text{ind}_2(j)) = N_n$ will refer to the allocation of candidate aggregator node N_n to the G matrix where the primary index *ind* matrix is accessed concerning the index for candidate aggregator node ind_2. Further, in this line of action, it should be noted that the loops used for authorizing the participating sensor are highly energy-efficient. Apart from this, it should be noted that the proposed algorithm authenticates only the nodes actively participating in the data aggregation process. Nodes not in range will not be participating; however, this is unlike a case as the initial deployment of nodes is carried out in such a way that it is either connected by single or multihop to each other. The simulation of node topology is highly interconnected with each other.

Finally, the aggregator node is confirmed in this algorithm. All the other nonaggregating on-field sensors forward the sensed farming data to this aggregator node which further aggregates the data d_{agg} that is finally forwarded to the sink node. This completes the operation of forwarding the aggregated data. It is to be noted that the proposed system has also initialized E_o along with other energy parameters to ensure that less energy is consumed while performing security operations in the proposed system. Hence, a cost-effective data aggregation process is implemented in the proposed system. A discussion of the security aspect follows next.

```
    Input: n
    Output: Auth_agg
    Start
(1) For i = 1 : n
(2)   λ:(η_2 ← η_1 × η_1)
(3)   select (a, b) ∈ Z, alloc α_o, α_2, α_3
(4)   (β_i, pr_i) = [γ_1(iden_i), a(pr_i)]
(5)   gen st = (τ_1i, τ_2i, iden_i, msg)
(6)   For j = 1: n
(7)     If λ(cond_1) = λ(cond_2)
(8)       successful authentication
(9)     End
(10)    χ = f_3(attr), τ_1j = f_4(χ, τ_1j)
(11)    If λ(cond_3) = λ(cond_4)
(12)      Auth_agg ⟶ authenticated aggregation
(13)    End
(14)  End
(15) End
     End
```

Algorithm 2: Authenticating aggregation.

5.2. Algorithm for Authenticating Aggregation. This algorithm works as an intermediate process in the first algorithm of data aggregation. The complete construction of this algorithm is carried out on certain assumptions. The first assumption is the presence of a distributed cloud-based storage unit capable of processing the sensitive data forwarded by on-field sensors and then forwarded via the sink node. The design and development of the proposed security system are carried out using improved public key encryption. Unlike the existing system, where public keys are not emphasized, the proposed system offers significant encoding of public keys to offer extended security apart from computing private keys. The study assumes that all the distributed cloud-based storage units obtain a public and secret key, i.e., α_2 and α_3, respectively. The next assumption is about the aggregator node capable of authenticating messages. They are the only authorized node to have access to the public key α_2. The aggregator node can also forward the aggregate validation token to the distributed cloud-based storage unit. However, for extended security toward identifying the legitimacy of the aggregator node, a trusted authority, along with system parameters, generates its private key. It should be noted that owing to multiple aggregator nodes, the trusted authority generates multiple private keys specific to the aggregator node's respective identity. The generated private keys are stored in the temporary buffer of the node. Therefore, the role of the trusted authority (sink node) is to bridge the connection between itself and all other sensor nodes, which gather all the aggregated data and further forward it to the user application. Apart from this, trusted authority also plays a role in developing the private key. The aggregator node is embedded with the system parameter and private key while deployed in farming region A. The steps of the algorithm are as follows:

This algorithm takes the input of n (number of the sensor) that yields an outcome of Auth_{agg} (authenticated aggregation) after processing. Further, taking sensor nodes n, the algorithm constructs a cryptographic function λ, which generates a group η_2 from η_1. The algorithm considers α to be a random value that is generated for η_1. It should be noted that α is not a function but a variable to hold a random number of secret keys. The study also considers the hash function of γ_1, γ_2, and γ where the values of the hash γ_1 and γ_2 are within the probability scope of [0, 1] for η_1 while the hash value of γ is another natural number and associates with η_2. The trusted authority considers selecting two random values, a and b (natural number). The trusted authority performs the computation of $\alpha_o = b.\ \alpha$ and $\alpha_2 = b.\alpha$ and $\alpha_3 = b$. The system parameters considered by the trusted authority is $\text{param} = \{\lambda,\ \eta_1, \eta_2, \alpha,\ \gamma_1,\ \gamma_2,\ \gamma,\ \alpha_o\}$ where the variable a is considered to be the core key. The distributed cloud-based storage units will be a pair of public and secret keys, which are $(b.\alpha)$ and b, respectively. This completes the configuration stage. The second process of this algorithm is to carry out the secret key generation by the sensor node for data aggregation. The computation of this key is carried out by $\beta_i = \gamma_1(\text{iden}_i)$, while the private key is $pr = (a.\beta_i)$, as shown in Line 4. It should be noted that β and pr represent the secret key (a part of the encoded public key) for data aggregation and the private key for encryption as a standard procedure for secret key management, respectively. This algorithm's third process is embedding a validation token within the message msg_i. The sensor node computes three variables τ_i, τ_{2i}, and τ_{3i}. The equivalent computation for these variables is as follows: $\tau_{1i} = r_i.\alpha$, $\tau_{2i} = \gamma_1(r_i, \text{iden}_i, msg_i)$, and $\tau_{3i} = (\text{pr}_i + r_i.\tau_{2i})$ as shown in Line-5. The generation of the security token st is finally formed, as shown in Line 5. The fourth process of this algorithm is about performing authentication to find the equivalency of two conditions, cond_1 and cond_2, concerning λ. The first condition, cond_1, is equivalent to (τ_{1i}, α), while the second condition, cond_2, is $\lambda(\alpha_o, \beta_i).\ \lambda(\tau_{2i}, \tau_{3i})$. The fifth process of this algorithm is to

carry out farming data aggregation. During data aggregation, each sensor node with a specific identity embeds the security token with the message. After obtaining the public key α_o, the aggregator node computes a new variable χ and $\tau_{1j.}$ The computation of the first variable is carried out by applying function $f_3(x)$ using input attribute *attr,* which is equivalent to $\gamma(\lambda(\tau_{1j.,}\alpha_2),\ldots)$, ... , $(\tau_{1n}, \alpha_2))$ while the computation of the second variable is carried out as $\chi.\Sigma\tau_{1j}$. Finally, the algorithm executes authentication of aggregated information, where the original message msg_i consists of an aggregated secret token $s_{t,}$ generated by the sensor within a specific subfarming region. In such a situation, the distributed cloud-based storage units check for two conditions, i.e., cond_3 and $\text{cond}_{4,}$ which are represented as $\lambda(\tau_{1j,}\alpha)$ and $\lambda(\alpha_o, \beta_i)$. $\lambda(\tau_2, \tau_3)$, respectively. If this condition is found to be valid, then the distributed cloud-based storage unit performs the computation of public key β_i and hash function $\gamma_i = \gamma(\tau_{2j,}\ \text{iden}_i, \text{msg}_i)$.

Therefore, the proposed authentication algorithm mainly offers multiple dependencies where public and private keys undergo dependable information, e.g., arbitrary numbers consideration by a trusted authority, hash functions values, and identity information are only accessible by the authorized nodes. Any attacker attempting to have access will end up in denial towards accessing these resources resulting in primary resistance towards their participation with malicious intentions. A closer look into this algorithm shows that it offers connectivity to each step where similar variables are continued with updates in every process, which makes sure that if any step of this algorithm is compromised, the attacker does not have any control or authority to decode the contents of message msg_i which require secret token s_t. An attacker cannot know the process of decoding secret tokens with higher dependencies of security variables.

6. Result Analysis

The implementation of the proposed algorithm is carried out over MATLAB, where the idea of analysis is to assess the impact of the proposed security algorithm on energy efficiency. This section discusses the result obtained from the simulation study concerning its accomplishment from both energy and security perspectives.

6.1. Simulation Environment. The simulation environment for the proposed system consists of 1000 on-field sensors distributed over the farming land of $1100 \times 1200\,\text{m}^2$ area. The complete farming area is further divided equally into four subfarming areas. Each subfarming area consists of a specific form of on-field sensor and one aggregator node. A sink node (also represented as a trusted authority) could be positioned at any point in the farming area. The study considers that each sensor possesses 10 meters of sensing range capable of forwarding 5000 bytes of the data packet. The nominal size of the control message is kept at 30 bytes which are 50 nano-joules of the initial energy considered for all the nodes. Existing studies towards energy efficiency have been evaluated using energy consumption parameters mainly, while literature on security have been evaluated using multiple parameters, viz. memory utilization [31], energy in the form of electric output [33], and execution time [35]. As the proposed scheme aims for energy efficiency and security, therefore performance metrics opted for are mainly energy-based metrics, execution time, and security analysis.

6.2. Analysis of Energy Efficiency. Energy consumption is the standard performance metric to assess the effectiveness of any approaches claiming to achieve energy efficiency. However, for better inference, the proposed system analyzes energy efficiency concerning two performance parameters, i.e., alive nodes and residual energy of the on-field sensors. For effective analysis, the study outcome is compared with a standard work of secure LEACH [38]. The prime reason to consider this existing system is its target of achieving security and energy efficiency together. In Figure 2, a comparative analysis is shown to evaluate the performance of the proposed scheme for the number of remaining active nodes in the progressive communication rounds. The results show that the proposed scheme outperforms the existing systems.

The design of the security function is based on a lightweight mechanism of encryption and hashing. Another important feature of the proposed scheme is the noniterative approach of verification token generation, which makes it suitable for energy conservation and highly responsive in execution. Furthermore, information aggregation is carried out only through aggregator nodes, which does not allow other nodes to waste their energy in data transmission. It is also observed that the existing technology, i.e., Secured Leach, is based on a complex cryptographic mechanism, making it unsuitable for WSN-based PA.

Figure 3 highlights the comparative analysis of the proposed and existing system concerning residual energy. It can be seen that the proposed system maintains a better distribution of energy utilization and sustains nodes for the longer run.

On the other hand, Figure 4 highlights that if the same secured LEACH algorithm and proposed system are analyzed for two test environments of secured data aggregation (agg-existing and agg-proposed) and insecure data aggregation (unagg-existing and unagg-proposed). It is found that the proposed system with secured aggregation always excels in a better outcome in contrast to any other situation.

6.3. Analysis of Execution Time and Security. As the proposed system claims of a novel public key encryption scheme, therefore, it is necessary to offer sufficient evidence to claim its effectiveness in contrast to existing public key encryption approaches, e.g., digital signature algorithm (DSA), Rivest Shamir algorithm (RSA), elliptical curve digital signature algorithm (ECDSA), Diffie–Hellman key agreement protocol (DHKAP). The proposed scheme *Prop* is compared with all those mentioned above public key encryption standards concerning execution time, as highlighted in Figure 5. The outcome in Figure 4 showcases that the proposed scheme offers approximately 52% faster

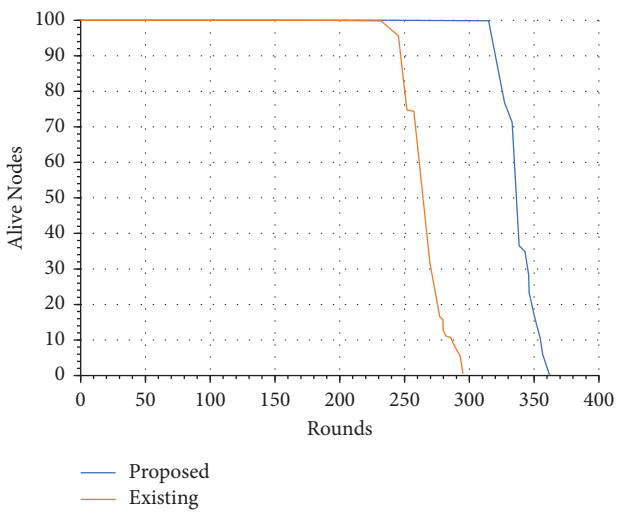

Figure 2: Comparative analysis of alive nodes.

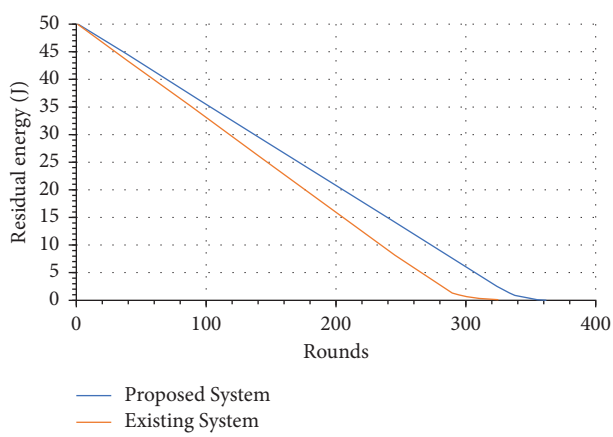

Figure 3: Comparative analysis of residual energy.

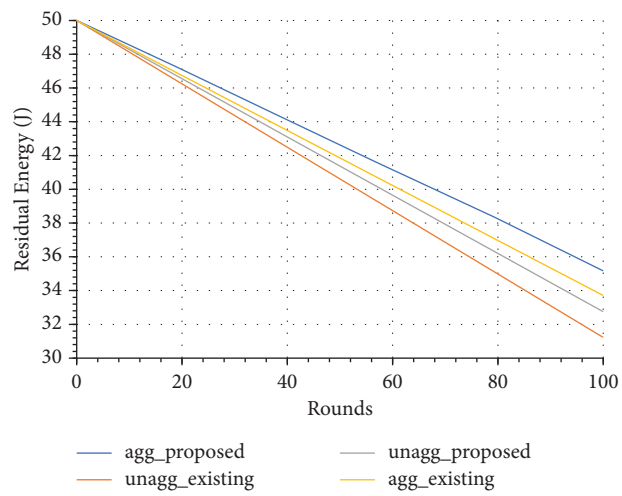

Figure 4: Comparative Analysis of residual energy.

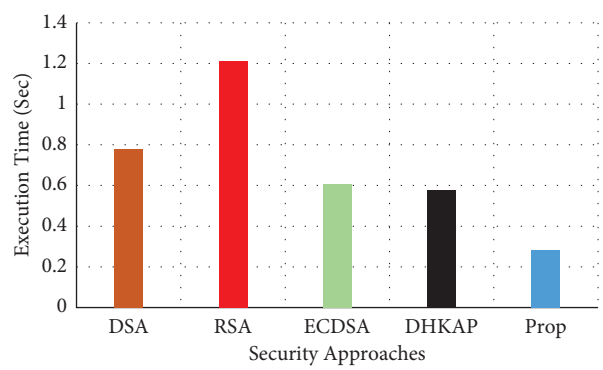

Figure 5: Comparative analysis of execution time.

execution speed in contrast to existing schemes. The execution time of the RSA algorithm is quite as due to its larger key size and its dependency on asymmetric only.

Apart from this, RSA also has higher dependencies on third parties to authenticate the legitimacy of public keys, which is not practically accepted in PA applications. However, these problems do not exist in DSA. Still, owing to the inclusion of a complex form of the remainder operator, the DSA algorithm performs better than RSA in a given test environment, although slightly increased in its execution time. Further adoption of ECDSA offers significant control over the key size. Still, its dependencies towards signature computation in dual stages consume much time, although it is a better form of authentication.

Further, DHKAP suffers from a computationally intensive process of higher dependencies over CPU resources. The proposed scheme exhibited none of the above-stated features, making the algorithm processing quite faster. The authentication process has less inclusion of sophisticated empirical calculations and has more conditional operation resulting in faster operation. Further, it only uses hash for encoding, making it much more lightweight.

To talk about security architecture, it is essential to investigate and know the behavior of an attacker. No attacker will attempt to directly introduce an attack as it is unaware of the attack-resistance policy. So, let us illustrate this concerning possibility of mechanisms of attacks as follows:

(i) forward flooding messages via some victim node (regular on-field sensor with poor resources)

(ii) introduce themselves as a regular node by overhearing the signal being exchanged

(iii) attempt to perform eavesdropping by listening to the exchange of communication

Such an attack can be launched by introducing a rogue sensor over the farming area or by even using the airborne vehicle in the vicinity of the sensing range of the sensor. Hence, keeping this scenario in mind, the first thing common in all attack-introduction approaches is understanding the legitimacy of neighboring nodes and their message. A neighboring node's first round of legitimacy can be carried out by assessing its identity and a public key generated by a trusted authority.

The mechanism of resisting attacks by the proposed scheme will be as follows: if this node is malicious, the value of the core key, i.e., will never match, as it is a randomly

Table 1: Comparison with energy-efficient scheme.

Approaches	Advantage	Limitation
Routing-based [18, 22–24]	Effective route formulation	Highly iterative
Energy-harvesting [16, 17, 25]	Higher energy efficiency	Uncertainty of resource availability
Bio-inspired [19, 21, 28]	Optimize energy of nodes	Not assessed over large and complex network
Fog computing [20]	Simplified architecture	Cannot resist congestion
Fuzzy logic [29]	Highly specific problem solving	Dependency towards rule set formulation
Proposed	(i) Handle large dynamic network (ii) Noniterative, energy-efficient (iii) Effective traffic management (iv) Less burden of node buffer (v) Benchmarked	

Table 2: Comparison with security scheme.

Approaches	Advantage	Limitation
Prototyping [30]	Can resist deauthentication attack	Hardware resource inclusion is not considered
Rule-based attack resistance [31, 33]	Flexible formulation of attack-resisting rules	Attack specific solution
Software defined network [32]	Offer more intelligence	Cost-effectiveness is not assessed
Privacy preservation [34]	Ensure better data integrity and privacy	Computationally extensive algorithm
Blockchain [35, 36]	Robust security	Consumes large energy
Proposed	(i) Can handle multiple forms of attack and threats in PA (ii) No sophisticated encryption is used (iii) Multiple layers of security in each step (iv) A higher degree of forward and backward secrecy (v) Offers data security along with energy efficiency	

generated number by the distributed cloud-based storage unit. Hence, the authentication fails firsthand. Even on consecutive levels, if the attackers attempt to access any chunk of the message, they will never be able to decode them. To decode, they will be required to possess the system parameters param, which is possessed only by the trusted authority. They will not make the mistake of requesting trusted authority for this purpose, as they will have higher chances of being caught owing to the unmatched public key. Apart from this, the keys are generated and distributed by the trusted authority itself; however, the uniqueness is that generated secret keys are encrypted forms of public keys that cannot be accessible by any unauthorized nodes. Apart from this, the distributed keys are also subjected to hashing and followed by encrypting steps ensuring that they cannot be decomposed by any secondary member who is not authorized.

Therefore, the proposed system does not emphasize identifying and capturing the malicious node. Still, it ensures that if an attacker compromises an encoded data packet, they should never be able to decode it. Hence, from this potential to resist illegitimate requests, the proposed system can be claimed to resist cyber-physical, sinkhole, worm, and distributed denial-of-service.

Tables 1 and 2 show that the proposed scheme offers a better balance between energy efficiency and security demands.

7. Conclusion

The proposed study has introduced a solution to balance energy efficiency and security. The key contribution of the proposed work are (i) unlike existing public-key encryption, the proposed study does not make use of sophisticated encryption apart from hashing, (ii) different from existing approaches of public key encryption, the proposed system performs computation as well as encoding of the public key to be forwarded in the public channel to offer an extra layer of security, (iii) different from existing key management techniques, proposed system doesn't store a private key, it rather generates it whenever the transaction is required in PA, (iv) the complete modeling is carried out considering that there is preapproved information about the adversary and hence the resistivity of the proposed system towards every form of dynamic attackers are increasing in its scope of resiliency, and (v) the proposed system offers a significant saving of residual energy of a maximum number of nodes as all on-field sensors are not required to communicate directly with the sink node. Hence, the proposed system offers a cost-effective solution for balancing energy and security issues in PA. The proposed scheme offers approximately 35% more alive nodes as well as 32% of higher retention of residual energy in contrast to the existing aggregation scheme. Further, the proposed scheme offers 52% faster execution than existing schemes.

The future work of the proposed scheme is towards accomplishing further optimization of the secure data aggregation process, considering more potential threats. For this purpose, a complex adversarial model with multiple dynamic attackers who initiate the propagation of concurrent malicious codes will be constructed. This is followed by further developing an optimized model which can identify it.

Data Availability

This research does not use any preexisting dataset. However, the experimental data are available from the authors upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank Dr. Nagaraja G S, IEEE Senior Member, and acknowledge the support from the Department of CSE of the RV College of Engineering and Dr. Farooque Azam, Senior Member (IEEE) from School of CSE of REVA University for his contribution towards this research.

References

[1] D. Kent Shannon and D. E. Clay, *Precision Agriculture Basics*, Wiley, Hoboken, NJ, 2020.

[2] J. V. Stafford, *Precision Agriculture'19*, Wageningen Academic Publishers, Wageningen, Netherlands, 2019.

[3] A. Mouazen, A. Castrignano, and D. Moshou, *Agricultural Internet of Things and Decision Support for Precision Smart Farming*, Elsevier Science, Amsterdam, Netherlands, 2020.

[4] A. B. Lawal, *How to Design GPS/GNSS Receivers Books 2, 3, 4 & 5,-The Principles, Applications & Markets*, A B. Lawal, USA, 2020.

[5] L. Ahmad and S. S. Mahdi, *Satellite Farming an Information and Technology Based Agriculture*, Springer International Publishing, Midtown Manhattan, NY, USA, 2019.

[6] Q. Zhang, *Precision Agriculture Technology for Crop Farming*, CRC Press, Boca Raton, FL, USA, 2015.

[7] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A survey on the role of IoT in agriculture for the implementation of smart farming," *IEEE Access*, vol. 7, pp. 156237–156271, 2019.

[8] S. Lee, H. Ahn, J. Seo, Y. Chung, D. Park, and S. Pan, "Practical monitoring of undergrown pigs for IoT-basedlarge-scale smart farm," *IEEE Access*, vol. 7, pp. 173796–173810, 2019.

[9] W. L. Chen, Y. B. Lin, Y. W. Lin et al., "AgriTalk: IoT for precision soil farming of turmeric cultivation," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5209–5223, 2019.

[10] 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.

[11] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 551–591, 2013.

[12] D. Ma, G. Lan, M. Hassan, W. Hu, and S. K. Das, "Sensing, computing, and communications for energy harvesting IoTs: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1222–1250, 2020.

[13] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2205–2224, 2019.

[14] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[15] R. Molose, B. Isong, N. Dladlu, and A. Abu-Mahfouz, "Data aggregation schemes for maximal network lifetime: review," in *Proceedings of the 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp. 1–8, Prague, Czech Republic, July 2022.

[16] H. Azarhava and J. M. Niya, "Energy efficient resource allocation in wireless energy harvesting sensor networks," *IEEE Wireless Communications Letters*, vol. 9, no. 7, pp. 1–1003, 2020.

[17] F. Ait Aoudia, M. Gautier, and O. Berder, "RLMan: an energy manager based on reinforcement learning for energy harvesting wireless sensor networks," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 2, pp. 408–417, 2018.

[18] M. Zhang and W. Cai, "Energy-efficient depth based probabilistic routing within 2-hop neighborhood for underwater sensor networks," *IEEE Sensors Letters*, vol. 4, no. 6, pp. 1–4, Article ID 7002304, 2020.

[19] H. Wang, K. Li, and W. Pedrycz, "An elite hybrid metaheuristic optimization algorithm for maximizing wireless sensor networks lifetime with a sink node," *IEEE Sensors Journal*, vol. 20, no. 10, pp. 5634–5649, 2020.

[20] M. Ammad, M. A. Shah, S. U. Islam et al., "A novel fog-basedmulti-levelenergy-efficient framework for IoT-enabled smart environments," *IEEE Access*, vol. 8, pp. 150010–150026, 2020.

[21] X. Q. Zhao, Y. P. Cui, C. Y. Gao, Z. Guo, and Q. Gao, "Energy-efficient coverage enhancement strategy for 3-D wireless sensor networks based on a vampire bat optimizer," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 325–338, 2020.

[22] F. Deng, X. Yue, X. Fan, S. Guan, Y. Xu, and J. Chen, "Multisource energy harvesting system for a wireless sensor network node in the field environment," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 918–927, 2019.

[23] C. Yu, D. Yao, L. T. Yang, and H. Jin, "Energy conservation in progressive decentralized single-hop wireless sensor networks for pervasive computing environment," *IEEE Systems Journal*, vol. 11, no. 2, pp. 823–834, 2017.

[24] F. H. El-Fouly and R. A. Ramadan, "E3AF: energy efficient environment-aware fusion based reliable routing in wireless sensor networks," *IEEE Access*, vol. 8, Article ID s, 112159 pages, 2020.

[25] O. Gulec, E. Haytaoglu, and S. Tokat, "A novel distributed CDS algorithm for extending lifetime of WSNs with solar energy harvester nodes for smart agriculture applications," *IEEE Access*, vol. 8, pp. 58859–58873, 2020.

[26] G. Mehmood, M. Zahid Khan, M. Fayaz, M. Faisal, H. Ur Rahman, and J. Gwak, "An energy-efficient mobile agent-based data aggregation scheme for wireless body area networks," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 5929–5948, 2022.

[27] M. N. Khan, H. U. Rahman, M. Z. Khan et al., "Energy-efficient dynamic and adaptive state-based scheduling (EDASS) scheme for wireless sensor networks," *IEEE Sensors Journal*, vol. 22, no. 12, pp. 12386–12403, 2022.

[28] J. J. Estrada-López, A. A. Castillo-Atoche, and E. Sanchez-Sinencio, "Design and fabrication of a 3-D printed concentrating solar thermoelectric generator for energy harvesting based wireless sensor nodes," *IEEE Sensors Letters*, vol. 3, no. 11, pp. 1–4, Article ID 5500904, 2019.

[29] C. Jamroen, P. Komkum, C. Fongkerd, and W. Krongpha, "An intelligent irrigation scheduling system using low-cost wireless sensor network toward sustainable and precision agriculture," *IEEE Access*, vol. 8, pp. 172756–172769, 2020.

[30] S. Sontowski and L. Zhang, "Cyber attacks on smart farming infrastructure," in *Proceedings of the 2020 IEEE 6th*

International Conference on Collaboration and Internet Computing (CIC), pp. 135–143, Atlanta, GA, USA, April 2020.

[31] P. V. Astillo, J. Kim, V. Sharma, and I. You, "SGF-MD: behavior rule specification-based distributed misbehavior detection of embedded IoT devices in a closed-loop smart greenhouse farming system," *IEEE Access*, vol. 8, pp. 196235–196252, 2020.

[32] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10250–10276, 2020.

[33] X. Fu, D. Yang, Q. Guo, and H. Sun, "Security analysis of a park-level agricultural energy network considering agrometeorology and energy meteorology," *CSEE Journal of Power and Energy Systems*, vol. 6, no. 3, pp. 743–748, 2020.

[34] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: challenges and opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020.

[35] H. T. Wu and C. W. Tsai, "An intelligent agriculture network security system based on private blockchains," *Journal of Communications and Networks*, vol. 21, no. 5, pp. 503–508, 2019.

[36] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020.

[37] G. Mehmood, "An efficient and secure session key establishment scheme for health-care applications in wireless body area networks," *Computer Science, Journal of Engineering and Applied Sciences*, vol. 10, 2018.

[38] M. Masdari, S. M. Z. Bazarchi, and M. Bidaki, "Analysis of secure LEACH-based clustering protocols in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 4, pp. 1243–1260, 2013.