International Journal of Computer Networks & Communications (IJCNC) Vol.14, No.5, September 2022

Hybrid Red Deer Algorithm with Physical Unclonable Function for Security Enhancement in IoT-WSN

Shilpa Venkata Rao and Vidya Anantha

Department of Computer Science and Engineering, Vivekananda Institute of Technology, Bangalore, Karnataka, India

Abstract. In this modern era, Wireless Sensor Network (WSNs) have turned out to be a more attractive option, because of the advancements in communication. If the network is insecure, an attacker can intercept messages and break the sensor nodes' security; as well as duplicate the authentication codes to launch a variety of attacks. As a result, Physical Unclonable Functions (PUFs) with unpredictable features are encouraged to be used in the development of lightweight cryptographic protocols. This work introduced the Red Deer Algorithm (RDA) with PUF as a new mutual authentication system. When a sensor receives a challenge from the gateway, the inbuilt PUF generates a key and distributes it to the sensor by providing complete resilience against malicious attacks. PUF is resistant to node acquisition, cloning, and malicious attacks, as well as node physical security flaws. Key distribution is moving too quickly and the adversary won't be able to conduct a harmful attack in time. Furthermore, PUF's unclonability and unexpected qualities provide key uniqueness and two-way authentication for improving the security. When compared to existing Tunicate Swarm Grey Wolf optimization (TSGWO) and PUF-Based Mutual-Authenticated Key Distribution (PUF-MAKD), the proposed RDA-PUF demonstrated better results. The simulation results are obtained in terms of minimizing energy consumption as 0.7 J, end-to-end delay as 7 sec, packet delivery ratio of 97%, increasing network lifetime to 1330 sec, and improving secure connectivity to 1.211.

Keywords: Network Lifetime, Physical Unclonable Function, Red Deer Algorithm, Security, Wireless Sensor Network.

1 Introduction

Wireless Sensor Network (WSN) is now a social transmission network with sensor nodes, mortal structures and Base Stations (BSs) [1]. Internet of Things (IoT) develops inventive ideas and advances a variety of communication formats. IoT structures rely on WSNs to collect data, and cloud/edge/fog computing can boost their computational dimensions [2], [3], [4]. Several IoT services and applications have been provided in this manner. IoT offers to make the Internet more pervasive, with the potential to influence several aspects of consumers' entertainment [5]. Because of insufficient sensor techniques, exploitation of energy throughout the routing procedure may cause a problem. Several hops are directed at the vast possibilities of land section over a few wireless machines [6]. WSN is a critical component of the Internet of Things, and it has evolved into a variety of different practical applications [7]. WSNs and the Internet of Things (IoT) now have a variety of precarious and non-critical manifestations that affect nearly every aspect of an individual's daily life [8]. WSN nodes are frequently tiny and rely on battery-powered technologies [9]. As a result, energy-efficient ways extend the network's lifespan, which is critical. There are several approaches and procedures for implementing an energy-efficient notion in WSN-based IOT architectures [10], [11].

Many exploratory projects have focused on the design of routing/ clustering procedures and additional schemes [12] for energy saving in recent years, but only a few have accomplished to model the systems that deliberate the construction of clustering and routing

DOI: 10.5121/ijcnc.2022.14503

mutually [13], [14]. WSNs' Quality of Service (QoS) must be improved in the current circumstances because the system must last for a long time [15]. A structure using effective clustering/routing via optimization approach [16] is another source of motivation, because the lack of network resources, necessitates the task of creating an energy-efficient transmission path and set-up design [17]. Researchers have developed different authentication techniques based on a PUF in a Radio Frequency Identification (RFID) system to avoid clone attacks. However, most protocols require verifiers to connect to a database containing a high number of PUF Challenge-Response Pairs (CRPs), which is not feasible for memory-constrained WSN nodes [18]. The current study focuses on the clustering/routing method developed for WSN-based IoT presentations. The routing method is shown as an important aspect of transferring the data gathered from sensors to the end point for further processing. After the data pre-processing is done, it is possibly used in a variety of applications to help people develop in their lives [19], [20].

The paper represents RDA-PUF based clustering and routing for improving the network lifetime. The major contribution of this research are

- Initially, an RDA-PUF based clustering method is created using an effective particle encoding design and its fitness derivative.
- Then, combining the RDA-PUF with a random deployment model for large-scale sensor networks. A sensor is assigned to gateways to promote secure connectivity and protects a sensor using PUF.
- RDA-PUF based routing procedure is processed among the transmission distance and amount of data transferred for comprehensive multi-objective function.
- RDA-PUF is simulated and compared to other important distribution schemes in terms of energy consumption and security.

In existing methods, the major issue was presented in the design which are incapable to analyse the validity of received message and every CRP is exploited just once to avoid the attacks. In order to overcome these problems, proposed RDA-PUF is designed with resource-constrained devices which validates the message through PUF technology and derive a shared session key for secure communication. The structure of this research are mentioned as follows,

Section 2 describes the exiting studies based on clustering/routing and security in WSN-IOT. Section 3 defines the problem statement along with solution. Section 4 explains the preliminaries of PUF, energy model and overview of RDA. Section 5 defined the process of clustering/routing using proposed RDA-PUF, working process of key authentication and PUF security in detail. Section 6 demonstrates the simulations results and its comparative analysis. Finally, conclusion is declared in section 7.

2 Related Work

Wireless Sensor Network-Internet of Things (WSN-IOT) makes use of a variety of current procedures, methodologies, and ideas from traditional wireless networks. However, some significant changes necessitate the use of novel techniques and methods. In this segment, a few of the gathered studies on clustering and routing in WSN-IOT are briefly discussed.

PUF-Based Mutual-Authenticated Key Distribution (PUF-MAKD) for Dynamic Sensor Networks has been proven by YananLiu et al. [21] to assist the sink node in authenticating and distributing session keys to static and mobile sensors. A challenge-response

technique based on the PUF ensures lightweight mutual authentication. To combat the PUF Challenge-Response Pairs (CRPs) exposure problem, the CRPs are not sent in plain-text to protect PUF from a modelling attack. Furthermore, sensors are not required to recover any password, reduces loading overhead and increases sensor node attack resilience. However, the PUF response was not sent in plain form to avoid modelling attacks, which was exploited in other existing PUF-based techniques.

For WSN-IOT hot-spot problems, Mohammad Ali Alharbi et al. [22] developed an energy-efficient clustering/routing resolution. This clustering technique uses a basic Cluster Head (CH) selection method to choose a CH based on aggregate node communication loads and remaining batteries, and it is dependent on the placement of WSN nodes. As a consequence, offer a routing technique that assigns marginal connections to the selected cluster leader to address weak situations. On the other hand, the suggested process only achieves the highest performance requirements for 2–3 communication nodes only, after that it slows down automatically.

For WSN-IoT, IpekAbastkeles-TurgutGokhanAltan [23] presented the Fully Distributed Energy-Aware Multi-level (FDEAM) approach. And also, an inter-cluster transmission process is introduced to enhance efficiency. Furthermore, the coverage region of the second-level gathering was actively developed, offering BS cluster distance. The FDEAM technique was used by cluster heads without a primary appliance to choose clustering boundaries. FDEAM technique was a reasonable starting point, even though it is useless for non-uniform node assignments and is reliant on a particular source.

In WSN-IoT, KavitaJaiswal and VeenaAnand [24] designed an Energy-Efficient Optimal Multipath Routing (EOMR) algorithm to improve QoS metrics. The recommended EOMR display generates an imbalance in the network due to greater bandwidth. When finding the ideal path, the suggested method takes into account some characteristics, including dependability, lifespan, and increased traffic during the next node. Here, transmissions occurred regularly in some areas of the system, while others were used in all the regions.

The Tunicate Swarm Grey Wolf optimization (TSGWO) approach was used by Nitesh Chouhan and Jain [25] to create the multipath procedure. TSGWO generates numerous routes from a distinct node to several endpoint nodes. The source node immediately transfers data packets to the target point. The optimal path was the one with the lowest number of delays, the lowest routing distance, and the highest connection durability. Route conservation was also allowed for route splintering retrieval through DRINA in the event of a link failure. But this method ignores the servicing parameters.

Shilpa V and Vidya A [26] has provided secure transmission of data and mutual authentication for IoT-WSN using Hybrid Optimization Algorithm (HOA) and Shamir Secret Sharing (SSS) method. The arrangement of Grey wolf optimization (GWO) and Moth Flame Optimization (MFO) was termed as HOA where the fitness functions were calculated. Moreover, SSS was utilized for delivering mutual authentication amongst the nodes. The Cluster Head (CH) selection and optimal routing eliminates the malicious nodes that advanced to reduce the packet loss in the network.

Shilpa V, Vidya A, Santosh Pattar [27] has presented dependable secure transmission of data among IoT were attained by lightweight encryption method. Here, a Secure Reliable Message Communication (SEC-RMC) procedure by means of Mosquitto MQ Telemetry Transport (MQTT) message broker through cryptographic developments to provide security against hacking and packets exploitations. The suggested SEC-RMC method minimizes the amount of messages transferred amongst the Internet of Things (IoT) devices.

Li et al [28] has demonstrated a provably secure and real-world PUF dependent end-to-end mutual authentication and key exchange technique for IoT. This research suggests a scheme for IoT through integrating PUF with Certificate Less Public Key Cryptography (CL-PKC) on elliptic curve to improve the security. This process merely demands multiple handshakes without including the practical server contribution to deliver accurate secrecy. However, this method does not create the shared session key among applicants and public key encryption process to confirm the secrecy.

3 Problem Statement

- The key problem in routing process was losing connectivity during data transmission while utilizing energy control mechanisms.
- PUFs was assumed as one-way hardware functions that are simple to implement but difficult to clone, reproduce, or predict.
- Data loss has occurred due to a faulty network, therefore, data dependability must be monitored during data packet transfer.
- The involvement of various objects and nodes energy become important concerns in WSN, because of insufficient energy given to the nodes.

Solution: This research's main purpose is to provide energy-efficient clustering and routing for data transmission via the Wireless Sensor Network-Internet of Things (WSN-IOT). PUF can withstand node acquisition, cloning, and malicious attacks, as well as entirely prevent node physical security vulnerabilities. And key distribution development is too fast, so the attacker won't be able to launch a malicious attack in time. The proposed RDA-PUF architectural framework prevents the system from data loss, unbalanced load, inflexibility, and unsecured connectivity.

4 Preliminaries

The major goal of this study is to provide energy-efficient clustering/routing for data transmission over the Wireless Sensor Network-Internet of Things (WSN-IOT). The sensor would not have any keys pre-loaded in its storage, however, when it receives a request, it generates a PUF response on the fly to decrypt the key supplied by gateway. Load balancing, flexibility, and secure connectivity are all possible with the conceptual methodology. A current transmitting process must be accessible and adaptable to complete network changes.

4.1 Physical Unclonable Function (PUF)

PUFs are innovative circuit elements that extract information from the physical properties of Integrated Circuits (ICs). There are two parts to PUFs: a physical component and an operating component. The physical aspect is a difficult-to-replicate sophisticated physical system. Its unclonability is due to unpredictably fluctuating manufacturing techniques [29]. Within the instance of PUFs resting on IC, manufacturing modifications are frequently influenced by deep-submicron fluctuations. To convert the dynamic system into a service that can be used for identification, a set of relevant inputs and a set of suitably variable answers has to be provided.

Figure 1 shows the general working function of PUF. From the figure 1, there are four major components are presented, they are, Cluster Head (CH), Base Station, Sensor node

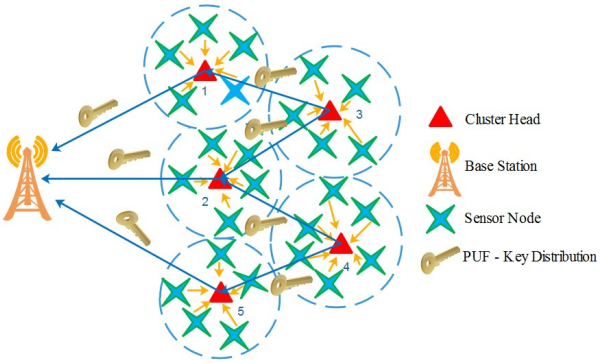

Fig. 1. General working process of PUF

and PUF-key distribution. To prevent clone attacks, researchers have explored various security approaches based on a PUF concept. Many algorithms, unfortunately, necessitate verifiers connecting to a library that contains a collection of PUF Challenge-Response Pairs (CRPs), which is not possible for memory-constrained Network elements. It clearly observed that the information from source to destination are passed through the Cluster Head (CH). If in case, PUF key distribution acknowledge the CH1 as leader, sensor node passes through CH1 to destination.

4.2 Energy Model

The energy model and its usage in Sensor setup has been defined in this subsection. The architectural system of WSN is mostly based on dualistic communications infrastructure characteristics, such as a multipath channel [30]. The bandwidth decreases with time as the sample free space resource is consumed, necessitating the use of a multi-path communication. The energy model's structure for source/destination is mathematically stated and presented in the equation (1),

$$Ener^{T}(1,D) = \left\{ \begin{array}{l} L{*}E^{Elec} + 1{*} \in^{FS} {*}D^{2},\ D < D^{0} \\ L{*}E^{Elec} + 1{*} \in^{MP} {*}D^{2}\ D \geq D^{0} \end{array} \right\} \tag{1}$$

The prerequisite energy in transmission networks is signified as $\in^{MP}$, if it is in free space, it is signified as $\in^{FS}$, whereas, in position of receiving channel it is nominated as E^{Elec} . The whole energy is essential for data communication during the distance d which is premeditated after eqn. (2). The receiver's demanded energy is formulated as eqn. (2),

$$Ener^{R}(L) = L{*}E^{Elec} \tag{2}$$

Receiver's required energy is characterized as $Ener(L)$ distance amongst the sender and receiver is signified as $\in^{MP} {*}D^{2}$. $\in^{FS} {*}D^{2}$. E^{Elec} is designed in the course of several characteristics.

4.3 Overview of Red Deer Optimization

Red Deer Algorithm (RDA) starts with a random population of search agents that is spread evenly throughout the population [31]. To assign the male red deer, the sensor nodes with the best potential in terms of residual energy, cluster head distance, and cluster to base station distance are picked, with the remainder nodes referred to as hinds. The sensor nodes having the best chance of being chosen as CH are male red deer. The hinds are

cluster members who serve as sensor nodes and are completely under the direction of the male red deer nodes.

Initial Population Generation The parameters considered for the most important optimization goals in establishing the global solution or near-optimal solution, are defined in equation (3). When the CH selection procedure is seen as a d-dimensional optimization method, the red deer indicates the number of d-dimensional arrays that range from 1 to d. Equation (3) is used to define red deer array as

$$R_{D(Array)} = \left[F_{S(1)}, F_{S(2)}, F_{S(3)} \ldots..F_{S(d)}\right] \tag{3}$$

Where, $R_{D(Array)}$ signifies the individual dimensions. Subsequently, the fitness function values are evaluated for every RD which is expressed in Equation (4)

$$Fit_{value}R_{D(Array)} = Fit_{Fn}\left[F_{S(1)}, F_{S(2)}, F_{S(3)} \ldots F_{S(d)}\right] \tag{4}$$

Primarily, P_{size} is stated as the size of the initial population which establishes the execution of the method. The best male RDs (RD_{male}) and the residual exploration solutions are elected as $RD_{Hinds} = P_{size} - RD_{male}$. Additionally, the amount of RD_{male} and RD_{Hinds} supports in preserving the amplification and diversification.

Roaring Stage In particular, the male RD solutions constantly modify their location which is updated as shown in Equation (5).

$$RD_{male} = \left\{ \begin{array}{c} RD_{male-old} + UDUD_{R(2)} \times \left((U_{TH} - L_{TH}) * UD_{R(2)} + L_{TH}\right) \text{ if } UD_{R(3)} \geq 0.5 \\ RD_{male-old} + UD_{R(1)} \times \left((U_{TH} - L_{TH}) * UD_{R(2)} + L_{TH}\right) \quad \text{if } UD_{R(3)} < .05 \end{array} \right\} \tag{5}$$

The current position of male RD is stated by $RD_{male-old}$; U_{TH} and L_{TH} depict the upper and lower search space respectively. The random variables are $UD_{R(1)}, UD_{R(2)}, UD_{R(3)}$ which are produced by means of uniform distribution (0 and 1).

Male Leader assortment from male red deer The male RD solutions are divided into two categories at this phase: leader and RD solutions. The proportion of male leader responses is estimated at this point using Equation (6).

$$RD_{Comd-Count} = Round\left(\beta, RD_{male}\right) \tag{6}$$

$RD_{Comd-Count}$ signifies the amount of leader male in the clusters. β is the initial value (0, 1) connected with the percentage of solutions measured for utilization. At this stage, the stag RD solutions ($RD_{stag-Count}$) are considered in Equation (7)

$$RD_{stag-Count} = RD_{male} - RD_{Comd-Count} \tag{7}$$

Stag and Male commanders fighting phase Here, one superior solution is determined in comparison to the leader and two additional solutions are discovered by following the procedure. Equation (8) and Equation (9) are used to illustrate the fighting process quantitatively.

$$New_{Sol(1)} = \frac{Sol_{Comd} + Sol_{Stag}}{2} + UD_{R(1)} \times \left((U_{TH} - L_{TH}) * UD_{R(2)} + L_{TH}\right) \tag{8}$$

$$New_{Sol(2)} = \frac{Sol_{Comd} + Sol_{Stag}}{2} + UD_{R(1)} \times \left((U_{TH} - L_{TH}) * UD_{R(2)} + L_{TH}\right) \quad (9)$$

Where, U_{TH} and L_{TH} represents the upper and lower search space. Moreover, $UD_{R(1)}$ and $UD_{R(2)}$ are also random variables generated using a uniform distribution. In this fighting stage, the first solution $New_{Sol(1)}$ selects the success solution and the second solution $New_{Sol(2)}$ helps in identifying losing solution.

Construction of Clusters During the cluster construction stage, the male leader answer becomes the cluster head, which controls the group of hinds. The amount of hind solutions are proportionally allocated among the commander solutions to build clusters as shown in equation (10).

$$N_{val} = Cmd_{power(n)} - Max\left(Cmd_{power(i)}\right) \quad (10)$$

Where, N_{val} and $Cmd_{power(n)}$ signify the normalized mean of leader and control of every entity leader, respectively, at every round of execution. After that, the leaders' normalized power is designed which is shown in Equation (11).

$$RD_{Comd(Power)} = \left| \frac{Cmd_{Power(n)}}{\sum_{i=1}^{RD_{Comd-Count}} Cmd_{Power(i)}} \right| \quad (11)$$

Where, $RD_{Comd(Power)}$ signifies the power infatuated by every leader for the duration of clustering and CH selection. For the duration of the clustering process, the number of hind alternatives can be controlled by the commander's solutions. Equation (12) is exploited to calculate the number of hinds that might conceivably occur in a cluster (harem).

$$RD_{Hind-Harem} = Round\left(\alpha, RD_{Hind-Cnt}\right) \quad (12)$$

Where, $RD_{Hind-Harem}$ represents the number of hinds present in a cluster, for the duration of CH selection. Overall, the parameter with a higher fitness function is referred as leader which is found to be superior to the hind options. In the operation of clustering in WSNs, the commander and hinds symbolize the CH and cluster members.

5 Proposed Method

RDA-PUF is meant to reduce the incremental energy usage at every node in this study. Initially, each node is created via similar energy sources. Energy is reduced during the period of communication and dictated by the development of each node. The overall structure of the suggested RDA-PUF is explained in Figure 2.

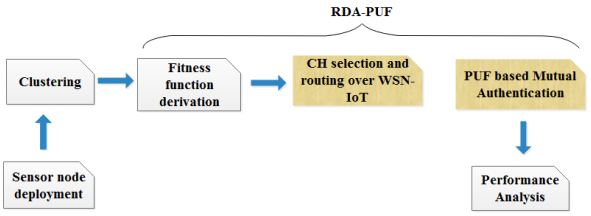

Fig. 2. Overall Structure of Proposed RDA-PUF

Step 1: At first, the network parameters are initialized with sensor node deployments in the network.

Step 2: Then the nodes are randomly positioned in the related region, after that mobile nodes are designated as energetic which is exclusively dependent on node location.

Step 3: The calculation of fitness function parameters are estimated.

Step 4: RDA-PUF is used for secure clustering, CH selection and routing process to find the shortest path.

Step 5: Routing process is created by means of proposed RDA-PUF which are exploited to develop the optimal route among CH and BS.

Step 6: Whenever the route from source to destination is recognised, the source node transmits the data in destination.

Step 7: After the data transmission, RDA-PUF based mutual authentication gets processed.

Step 8: Then RDA-PUF estimates the optimal path by taking various objective functions.

Step 9: BS is regularly exploited to detect the nodes energy. In order to eliminate secure in connectivity, energy consumption and data loss re-clustering/rerouting is done repeatedly.

The functionalities of each step and its requirements including CH selection, Fitness function metrics, route selection, PUF structure, Key distribution, Authentication and security along with flowchart for proposed RDA-PUF is explained clearly in the below sections

5.1 CH selection

The RDA-PUF is used for CH selection and routing. The suggested RDA-PUF is chosen since it has a collision prevention characteristic by default, making it particularly useful for generating congestion-aware routing in unexpected scenarios.

Fitness function The trust metric, Queue Utilization between Nodes (QUN), link quality, and distance are all employed in the RDA-PUF technique. As a result, the specified cost measurements are employed to prevent malicious nodes, by giving a major focus to the trust value for the trust metric, throughout the routing. To increase the presentation in terms of energy consumption and overhead, subcategories of the cost indicators like QUN, link quality, and distance are included.

Trust metric: Trust is a primary cost value for routing via an IoT-based WSN, and has been used to increase security against malicious nodes. The mobile nodes in an IoT-based WSN interact with one another by relying on the mutual trust established between the nodes over time. Direct trust is a packet-forwarding behavior that is based on the fraction of data (transferred) (TP_{ij}) and the amount of data packets (received) (RP_{ij}) . The direct trust degree is calculated based on the following equation (13).

$$Trust = \frac{TP_{ij}}{RP_{ij}} \tag{13}$$

QUN and link quality: QUN is demarcated as the ratio amongst the amount of packets engaged in the queue of j^{th} node (QUN_j) and quantity of obtainable packets in the particular node's queue (QUN_{total}). Equation (14) is utilized to calculate the QUN.

$$QUN = \frac{QUN_j}{QUN_{total}} \tag{14}$$

Link quality is described as the proportion amongst the quantity of transmission and retransmissions that are necessary for successful data transmission among node i and j .

$$Linkquality = \frac{1}{f \times r} \tag{15}$$

Where f and r state the forward & reverse information delivery respectively.

Distance: Euclidean distance among the nodes are premeditated to recognize the direct route over the IoT-WSN and deliberated through the equation (16).

$$Distance = \sqrt{(x_j - x_i)^2 (y_j - y_i)^2} \tag{16}$$

Where, x_i, x_j and y_i, y_j are coordinates of nodes i and j. In RDA-PUF, a weight value (δ) is considered for each cost value to convert into a single cost value as shown in the equation (17).

$$c_k = \delta_1 \times \text{ Trust } + \delta_2 \times QUN + \delta_3 \times \text{ Link quality } + \delta_4 \times \text{ Dis tan } ce \tag{17}$$

0.35, 0.25, 0.25 and 0.15 are the weighted mean for $\delta_1, \delta_2, \delta_3$, and δ_4 correspondingly. The malicious nodes that generate packet drops are avoided using the trust metric when designing the transmission path. Following that, to generate a route with less traffic, the QUN and link quality are taken into account in the cost measure. This reduces the chance of a communication collision and improves packet delivery. In addition, the shortest distance is determined to reduce the nodes' energy usage.

Route Selection When a client gets data in an IoT-based WSN, the client registers its ID in the routing table. The client begins forwarding the data to the desired destination after receiving it. The RDA-PUF evaluates the route with the highest pheromone rate if the source consumer receives multiple detection notifications from its neighbors. Direct transmission of data is performed by clients having a one-hop connection to the router, while multichip communication is performed by clients further away from the router via the RDA-PUF. As a result, data packets are transmitted along the path with the highest signal level. And once the routing path is established utilizing RDA-PUF, the data packet distribution is started. The queue length employed in routing is utilized to create a collision-free path that results to data being transmitted over a network with reduced congestion. The link quality is then utilized to determine the route's mean based on the sent and received packets. As a result, above-mentioned fitness parameters are exploited to determine the best data transmission route.

5.2 PUF Structure

Rather than keeping secrets in storage, PUF-based components are used to produce secrets from randomized variability in the production of electronic components. They don't necessitate costly cryptographic hardware like the Secure Hash Technique (SHA) standard. Because the "secret" is obtained from substantial features of the Integrated Circuit (IC), even with full comprehension of the semiconductor manufacturing, two equal transistors cannot be manufactured. PUF components would be investigated as a replacement that effectively uses a device's different characteristics as a hardware-based signature owing to

manufacturing variances. There are electro - optic PUFs and coating PUFs in addition to IC-based PUFs.

Every PUF has been treated as black-box ranking scheme, in which the system is presented with a number of challenges and returns with a collection of suitably varied solutions. PUF is described by a one-way transformation matrix, which may be written as Eq. (18).

$$\Gamma : R \to Y : \Gamma(x) = y, x \in X, y \in Y \tag{18}$$

In a PUF function, X and Y stand for challenge and response sets, respectively, in Eq. (18). For the given PUFΓ, a Challenge-Response Pair (CRP) (x, y) is formed by a detailed trial x and a matching response y. Because of qualities such as low-weighted, unclonable, and unpredictable, PUFs are used for two main purposes: low-cost validation and secure key creation. Subsequently, a sensor-based wearable PUF was developed, which makes use of different strengths supplied by a variety of sensors found on such devices. Low-level accessibility can be implemented during the production process or by the installation of a particular device controller to exploit such distinctive featured equipment.

RSA Cryptography RSA public key cryptosystem was established by Rivest, Shamir and Adleman, that is extensively exploited for secure data transmission. This research assesses the development of a number of symmetric and asymmetric encryption methods known as RSA in order to determine whether the encryption ratio is high when both encryption techniques are used. As per various criteria, every method has its own benefit. Because the key length in an asymmetric encryption technique is long, breaking the code in RSA is difficult. When it comes to throughput, more throughput means less power usage. RSA algorithm is stated as the better option in symmetric key encryption approaches and more secure in the asymmetric encryption technique because it generates keys by factoring high prime numbers. As a result, RSA is determined to be the superior answer in this manner. The comprehensive description of RSA is specified as follows.

Key Generation

Step 1: Initially, select two dissimilar and large primes $p\&q$ and calculates $n = p \times q$ and Euler's totient function is represented as $\varphi(n) = (p-1) \times (q-1)$

Step 2: Select a public key parameter e (i.e.) $1 < e < \varphi(n)$ and $\gcd(\varphi(n), e) = 1$.

Step 3: Then, calculates the private key parameter d (i.e.) $(e \times d) - 1 = 0 \bmod \varphi(n)$ by means of Extended Euclidean procedure. $\left(e, n \in Z \times Z^*_{\varphi(n)}\right)$ and $\left(d, n \in Z \times Z^*_{\varphi(n)}\right)$ are stated as public/ private key pairs.

Encryption The function of encryption $e_h : Z_n \to Z_n$ is stated as

$$e_h(M) : b = M^e \bmod n$$

Decryption The function of decryption $d_h : Z_n \to Z_n$ is stated as

$$d_h(M) : M = b^d \bmod n$$

Steps for Key Distribution

– Initialization
Ahead of deploying the network, every sensor S is drive-in PUF, as stated by Γ_S. C is referred to as an arbitrary challenge number that acts as input for Γ_S and receives the response R (output). The cycle is stored as $< id, C, R >$ into G (gateway).

– Distribution of Key
Once deployed in the network, G states the C from the list and directs it to S. It proceeds C as input and becomes the equivalent R as Eq. (19).

$$R = \Gamma_S(C) \tag{19}$$

S utilizes R to convert C then drives to G:

$$Cipher = E(R, C) \tag{20}$$

From equation (20), encryption key is referred as R, plaintext is referred as C, and cipher is referred as cipher text. G utilizes R to decode and associate through C:

$$Plain = D(R, cipher) \tag{21}$$

From the eqn. (21), the decryption key is referred as R which is obtained through S. If $Plain = C$ is true, G trusts S and is validated for the duration of Initialization. At that time it produces key k_{GS} and directs S through an encryption process of R, which is mentioned as Eq. (22):

$$Cipher2 = E\left(R, k_{GS}\right) \tag{22}$$

S decrypts $Cipher2$ and obtains k_{GS}.

Or else, if $Plain = C$ remains incorrect, G deliberates through an unauthenticated device which will make it incapable to create a session key by means of a sensor.

Authentication The CRP $< id, C, R >$ of every approved device with a PUF is saved by the gateway. When the sensor receives a challenge C, the PUF creates a response R and directs the Ciphertext $Cipher = E(R, C)$, and compares it against challenge $Plain = D(R, cipher)$, because only authorised sensors can deliver the right answer R in response to C. Then it transmits an encrypted assembly k_{GS} with R. Since only authorized gateways are familiar with the sensor's accurate PUF CRP sequence, this procedure aids the sensor in authenticating the gateway. The attackers might provide collision attacks on the entire network by accessing the passwords or other confidential documents in proportion to the captured nodes' memory. As the key distribution development is too fast, the opponent won't be able to launch a malicious attack on time.

PUF Security PUF's security is based on physical peculiarities that are impossible to replicate even at the industrial-technological sophistication. PUF must be incorporated into a node's chip. To put it another way, even if the attacker is aware of the PUF architecture and some difficulties, they will be unable to generate the appropriate replies. PUF can withstand node acquisition, cloning, and malicious attacks, as well as entirely prevent vulnerabilities of node physical security. Figure 3 shows the flowchart of proposed RDA-PUF method.

The flowchart steps are specified as follows:
Step 1: Initially, the sensor node is established.
Step 2: Once the node gets initialized, the process of roar male RDs is started.
Step 3: After that, select the energy efficient nodes (male commanders).
Step 4: Then harem formation is created.
Step 5: Mate is staged with the nearest hind to find the shortest path.
Step 6: Then the mobile node is selected for next set of generation.

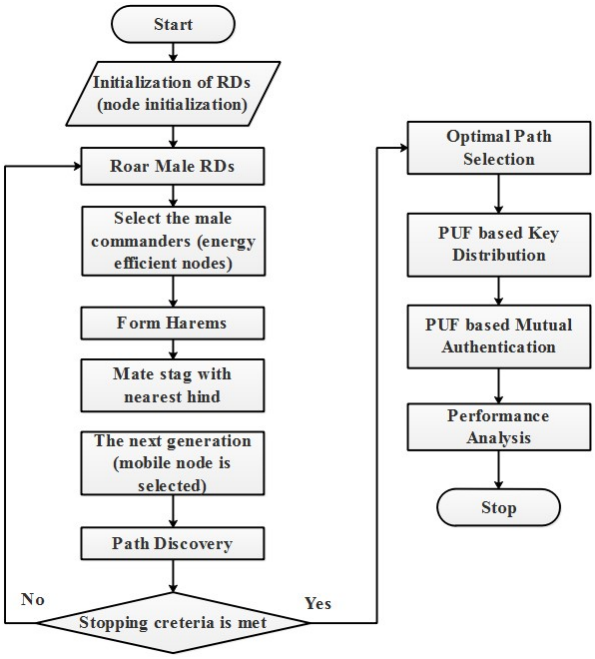

Fig. 3. Flowchart of Proposed RDA-PUF

Step 7: Identify the transmission path

Step 8: Check the stopping criteria

Step 9: IF No, go back to step 2; otherwise, select this optimal path for further transmission.

Step 10: Check the selected path with key distribution process.

Step 11: Following the clustering/routing procedure, the PUF-based mutual authentication mechanism can be examined to prevent malicious attacks.

Step 12: Examine the PUF's delivered performance parameters

Step 13: Stop the process.

Data Integrity Verification The trust value computation is used to validate and verify data integrity in WSN in this study. The observed information is secure utilizing shared symmetric encryption in this step. The encrypted data is then broken up into smaller chunks. After that, every one of these blocks is signed with a homomorphic tag and sent to the parent block, which has a higher trust value. The signed blocks are forwarded to the aggregator once they have been obtained. The sensor additionally gives the aggregator information about the parent block, as well as the block numbers. After confirming the accuracy of the data and confirming the integrity of every block, the aggregator applies the aggregation function to them. The combined output is then sent to the sink, in which it is double-checked by the sink. For the sensed data, this procedure is iterated by every sensor. Those findings were supported using the detection ratio in relation to node counts, as detailed in section 6.7 below.

6 Results and Discussions

The outcomes of developed RDA-PUF for multicast routing in an IoT-enabled WSN are discussed in this section. The conclusions and recommendations of the suggested RDA-PUF technique are fully described in detail. The 4-GB RAM and Intel Core CPU are used

by the RDA-PUF. The proven RDA approach is utilized to provide secure transmission between the source and the BS. Table 1 displays the design and simulation of the RDA-PUF technique under different parameter variables.

Table 1. Requirement of model parameters

Parameters	Value
Number of Nodes	400
Packet Size (bytes)	512
Receiving power (W)	1.0
Simulation Time (s)	100
Traffic type	CBR
Transmission power (W)	1.4
Data level (Kb/s)	300
Initial energy (J)	100
MAC layer	IEEE 802.15.4
Network Size (m)	500×500

6.1 Performance of Energy Consumption

The study of projected RDA-PUF and associated systems, such as FDEAM [23], EOMR [24], and TSGWO [25], in the context of energy consumption, is shown in figure 4. Figure 4 shows that when compared to the remaining three conventional approaches, the suggested RDA-PUF consumes lesser energy of 0.7 J. A node with less value is twisted by the packet boosting stage in the RDA-PUF approach. Furthermore, more energy is preserved by means of highest optimality factor continues to be important in progressing data packets; while, the traditional methods require an extra node when dispatching the same data packet; as a result, sophisticated energy is exhausted in conventional techniques.

Table 2. Performance of Energy Consumption

Number of Nodes	Performance of Energy Consumption (J)			
	FDEAM [23]	EOMR [24]	TSGWO [25]	Proposed RDA-PUF
100	0.8	1	8	0.5
150	7	9	15	6
200	10	14	19	8
250	14	19	26	13
300	26	30	31	20
350	29	36	37	23
400	41	47	44	29

The comparative examination of energy consumption performance is tabulated in Table 2. According to table 2, the developed RDA-PUF consumes less energy when compared to existing approaches. Figure 4 shows that the RDA-PUF method has a significant reduction in energy consumption when related to the conventional procedure because it deliberates the consistency, quantity and less energy established from base to endpoint. Furthermore, as the number of nodes in the arrangement grows, so does the amount of energy consumed also grows.

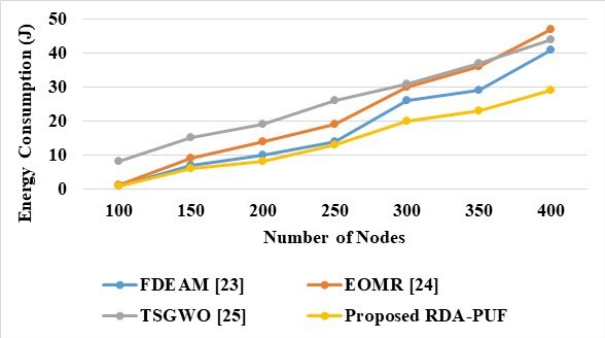

Fig. 4. Graphical view of Energy Consumption

6.2 Performance of End-to-End Delay

Figure 5 shows the investigation of end-to-end delay using RDA-PUF and existing approaches (FDEAM [23], EOMR [24], and TSGWO [25]). Figure 5 clearly illustrates that RDA-PUF has the shortest delay and is constantly attempting to send data packets to the best intermediary node, satisfying the ideal characteristic. On the other hand, the traditional approaches took a long time to determine the endpoint node. Furthermore, it initiates the prolonged return after the endpoint node. As a result, the associated system's usual delay is longer than the RDA-PUF technique. The investigation of end-to-end delay is tabulated in Table 3. When compared to existing methodologies, the suggested RDA-PUF achieves a shorter time delay, as shown in table 3.

Table 3. Investigation of End-to-end delay

Number of Nodes	End-to-End Delay Performance			
	FDEAM [23]	EOMR [24]	TSGWO [25]	Proposed RDA-PUF
100	8	10	8	7
150	14	17	15	8
200	15	23	19	10
250	23	30	26	16
300	28	35	31	19
350	32	42	37	22
400	40	50	44	25

6.3 Performance of PDR

Figure 6 shows a comparison between RDA-PUF and existing approaches (FDEAM [23], EOMR [24], and TSGWO [25]) in terms of packet delivery ratio performance. When compared to existing approaches, figure 6 appears to suggest that RDA-PUF yields greater PDR. Because, it recognizes that when the matching communication is single and binary, the PDR ratio becomes superior, and the overall assessment remains the same. The comparative examination of Packet Delivery Ratio performance is tabulated in Table 4. When compared to existing approaches, the proposed RDA-PUF, transfers additional packets as observed in table 4.

6.4 Performance of Network Lifetime

Figure 7 shows comparative analysis of network lifetime amongst the proposed RDA-PUF and the conventional methodologies. In RDA-PUF, there is a longer lifespan than existing

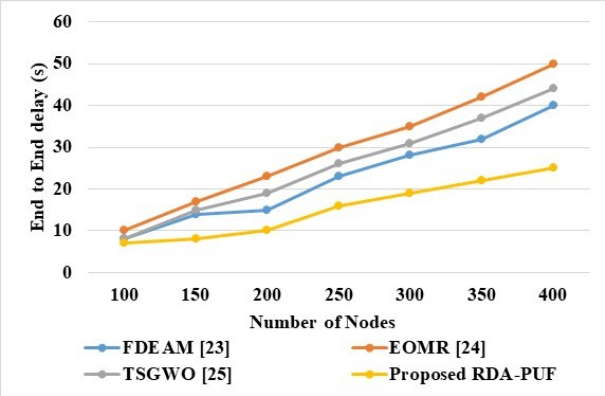

Fig. 5. Performance of End to End Delay

Table 4. Performance of PDR

Number of Nodes	Performance of PDR			
	FDEAM [23]	EOMR [24]	TSGWO [25]	Proposed RDA-PUF
100	80	70	73	84
150	86	84	85	90
200	86	85	87	92
250	90	87	89	93
300	92	88	89	94
350	92	88	90	95
400	94	89	92	97

FDEAM [23], EOMR [24], and TSGWO [25], because as the node count rises, extra nodes begin steering packets indiscriminately, and there is a higher chance that a node may expire at some point. Only the optimal node is assigned to transfer packets in the RDA-PUF approach, resulting in increased battery life and network longevity. The comparative examination of Packet Delivery Ratio performance is tabulated in Table 5. It displays that, when compared to conventional methods, the suggested RDA-PUF increases the network lifetime.

Table 5. Comparison of Network Lifetime

Number of Nodes	Performance of Network Lifetime			
	FDEAM[23]	EOMR [24]	TSGWO[25]	Proposed RDA-PUF
50	1245	1150	1220	1330
100	1170	1200	1208	1331
150	1138	1070	1109	1258
200	1072	990	1010	1127
250	1007	920	994	1072
300	968	860	951	982
350	927	853	915	985

From the analysis of all the performance parameters; Energy Consumption, End-to-End Delay, PDR and Network Lifetime, it can be concluded that an improved QoS in WSN is accomplished by multipath routing via RDA-PUF. The proposed RDA-PUF enhances the network performance via exploiting routing method to move the data from BS to end point, by selecting the best path.

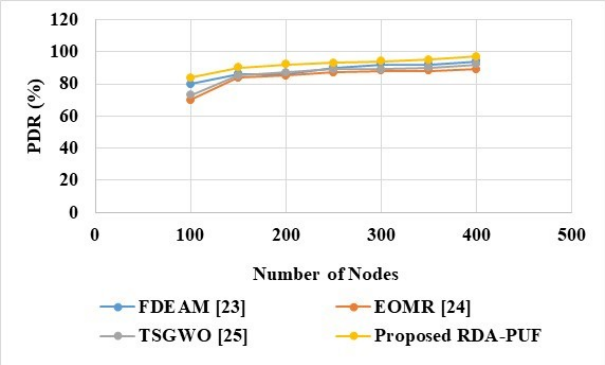

Fig. 6. Performance of PDR

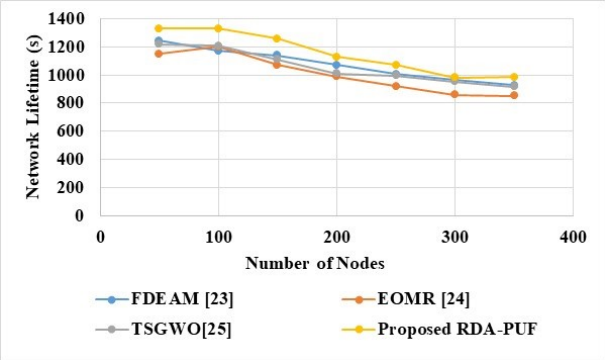

Fig. 7. Performance of Network Lifetime

6.5 Performance of Secure Connectivity

The possibility that two individuals can generate a session key to secure communications is characterized as a network's security connectivity. By considering "intra-cluster secure connectivity" a bilateral password is created in the network by a cluster-member, because this study primarily presents a method for intra-cluster authentication and key distribution. The effectiveness of secure connectivity is shown in Figure 8. The probability of sharing a key grows as the amount of preloaded keys increases, as seen in Figure 8. As the key pool size grows larger, the possibility of sharing a key reduces for almost the same settings.

Table 6. Comparative analysis Secure Connectivity

Key Pool Size	Existing PUF-MAKD [21]	Proposed RDA-PUF
2000	1.098	1.211
4000	1.097	1.209
6000	1.096	1.206
8000	1.095	1.204
10000	1.094	1.201

6.6 Performance of Time Duration

The ordinary time duration needed to implement associated cryptographic processes on the hardware tools through the system clock is fixed to 32MHz. And the below figure

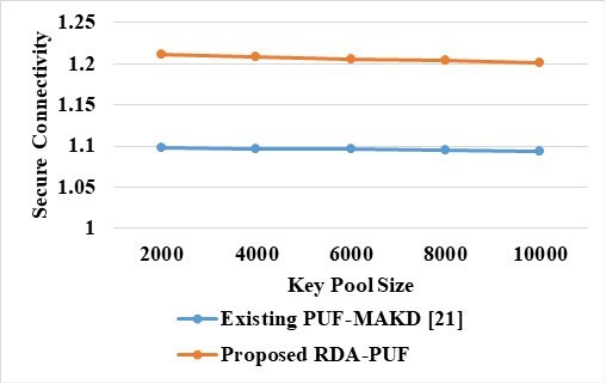

Fig. 8. Performance of Secure Connectivity

9 displays the time duration performances of existing CL-PKC [28] and proposed RDA-PUF protocol. From the figure 9, it clearly shows that proposed RDA-PUF achieves mutual authentication and key exchange in short interval of time. Table 7 shows the comparative analysis of time duration.

Table 7. Comparative analysis of Time Duration

Rounds	Existing CL-PKC [28]	Proposed RDA-PUF
1	2.41	2.33
2	2.33	2.27
3	2.36	2.30
4	2.38	2.32
5	2.46	2.35
6	2.35	2.27
7	2.31	2.24
8	2.42	2.29
9	2.49	2.33
10	2.43	2.30

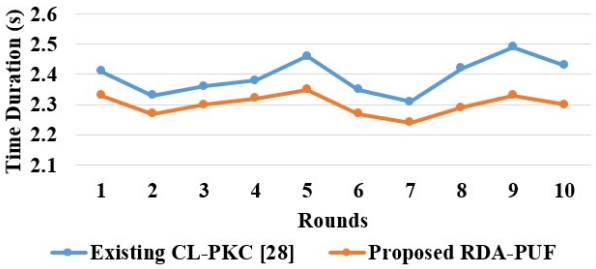

Fig. 9. Performance of Time Duration

6.7 Data Integrity and Verification

The detected data is encrypted using a shared symmetric key in this technique. The combined result is sent to the sink, where it is double-checked. For the sensed findings, this

procedure is iterated by every sensor. Figure 10 shows the data integrity performance through detection ratio. From the figure 10, it clearly shows that proposed RDA-PUF achieves higher detection ratio when compared to existing Data Validation and Integrity Verification for Trust Based Data Aggregation (DVIVTDAP) [32]. By examining the simulation results, it is indicates that the best method improves data accuracy.

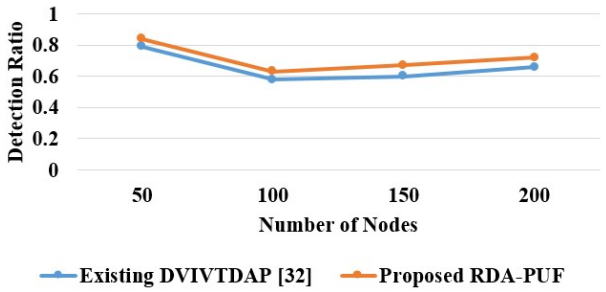

Fig. 10. Performance of Detection Ratio

7 Conclusion

In recent trends, WSNs have attracted a lot of attention as it has high resource constraints and principal concerns in computer technology. When transmitting point-to-point, however, these technologies have limited bandwidth, consumption, and resources. In sensor networks, how crucial information may be analyzed in a more energy-efficient approach, is a hot topic. In this research, RDA-PUF is offered as a method for transporting data from IoT to a target node with a longer delay. The proposed RDA-PUF could greatly improve secure communication in context of appropriate RSA protocol. Using a PUF in place of key administration and verification element to ensure protection in contradiction of malicious attacks. The overall simulation shows that the proposed RDA-PUF produced better results by reducing energy usage, end-to-end latency, network lifetime and PDR of proposed RDA-PUF is improved by 37%, 12%, 6.3% and 3.09%, respectively when related with existing FDEAM, EOMR and TSGWO technique. Similarly, the projected RDA-PUF enables highly secure connectivity (1.211) than the existing PUF-MAKD (1.098). In upcoming work, this technology can be broadened to include novel encryption methodologies for improving network performance.

References

1. Shen, Jian, Anxi Wang, Chen Wang, Patrick CK Hung, and Chin-Feng Lai, An efficient centroid-based routing protocol for energy management in WSN-assisted IoT, IEEE Access, Vol. 5, pp. 18469-18479, 2017.
2. Shrivastav, Khyati, and Kishore D. Kulat, Energy efficient scalability of three level hexagonal heterogeneous broad transmission distance protocol (3L-HEXA-HTBTDP) for WSN-IoT networks, International Journal of Communication Systems, Vol. 31, no. 17, pp. e3809, 2018.
3. L. Sasirega, Trust Establishment For Detecting Aggressor Nodes And Improving Route Stability In Wsn-Iot, Turkish Journal of Computer and Mathematics Education (TURCOMAT), Vol. 12, No. 11, pp6012-6020, 2021.
4. Reddy, M. Praveen Kumar, and M. RajasekharaBabu, A hybrid cluster head selection model for Internet of Things", Cluster Computing, Vol. 22, no. 6, pp. 13095-13107, 2019.
5. Jain, Bindiya, GursewakBrar, Jyoteesh Malhotra, and Shalli Rani, A novel approach for smart cities in convergence to wireless sensor networks, Sustainable cities and society, Vol. 35, pp. 440-448, 2017.

6. Hussein, Walaa, Jiwa Abdullah, and N. A. M. Alduais, Data Aggregation Algorithms with Multiple Sensors in Clustered-Based WSN/IoT, International Journal of Computing and Digital Systems, Vol. 9, No. 03, 2020.
7. Ullah, A., Azeem, M., Ashraf, H., Jhanjhi, N.Z., Nkenyereye, L. and M. Humayun, Secure Critical Data Reclamation Scheme for Isolated Clusters in IoT enabled WSN, IEEE Internet of Things Journal, 2021.
8. Reddy, M. Praveen Kumar, and M. RajasekharaBabu, Implementing self adaptiveness in whale optimization for cluster head section in Internet of Things, Cluster Computing, Vol. 22, No. 1, pp. 1361-1372, 2019.
9. Hao, Wang Zhi, Gwo-JiunHorng, and Gwo-Jia Jong, A New Bio-Inspired for Cooperative Data Transmission of IoT, IEEE Access, Vol. 8, pp. 161884-161893, 2020.
10. Anandkumar, M. (2020) "Multicast routing in WSN using bat algorithm with genetic operators for IoT applications", Journal of Networking and Communication Systems, Vol. 3, No. 2.
11. El-Sayed, Hamdy H, and Hilal Al Bayatti, (2021) "Comparisons of Some Multi-Hop Routing Protocols in Wireless Sensor Networks", Energy, Vol. 5.
12. Aadri, Alaa, and Najlae Idrissi, (2017) "A Cluster based routing algorithm minimizing energy consumption in WSN", International Journal of Wireless & Mobile Networks (IJWMN), Vol. 9, pp49-62.
13. Ara, Tabassum, M. Prabhkar, and PritamGajkumar Shah. (2018) "Energy efficient secured cluster based distributed fault diagnosis protocol for IoT", International Journal of Communication Networks and Information Security Vol. 10, No. 3, 539.
14. Dwivedi, Anshu Kumar, Awadhesh Kumar Sharma, and Pawan Singh Mehra. (2020), "Energy efficient sensor node deployment scheme for two stage routing protocol of wireless sensor networks assisted iot", ECTI Transactions on Electrical Engineering, Electronics, and Communications Vol. 18, No. 2, pp158-169.
15. L. Xu, G. MP O'Hare, and R. Collier, A smart and balanced energy-efficient multihop clustering algorithm (smart-beem) for mimoiot systems in future networks, Sensors, Vol. 17, No. 7, 1574, 2017.
16. L. Kaur, and R. Kaur, Comprehensive Survey for Energy-Efficient Routing Protocols on WSNs Based IoT Applications Enhancing Fog Computing Paradigm, In Applications of Artificial Intelligence in Engineering, pp. 339-354, 2021.
17. G. Sathishkumar, Bivariate Regression Adaptive Wald's Boost Energy Aware Routing for Wsn with IoT, Turkish Journal of Computer and Mathematics Education (TURCOMAT), Vol. 12, No. 7, pp2224-2241, 2021.
18. A.J. Manuel, G. Gopal Deverajan, R. Patan, Amir H. Gandomi, Optimization of routing-based clustering approaches in wireless sensor network: Review and open research issues, Electronics, Vol. 9, No. 10, pp. 1630, 2020.
19. H.K. Sekhon, and V. Singh, Clustering in Wireless Sensor Network: A Review", International Journal of Computers Technology, Vol. 16, No. 6, 2017.
20. J. Marietta, and B.C. Mohan, A review on routing in internet of things, Wireless Personal Communications, Vol. 111, No. 1, pp. 209-233, 2020.
21. Y. Liu, Y. Cui, L. Harn, Z. Zhang, H. Yan, Y. Cheng, and S. Qiu, PUF-Based Mutual-Authenticated Key Distribution for Dynamic Sensor Networks, Security and Communication Networks, 2021.
22. M.A. Alharbi, M. Kolberg, and M. Zeeshan, Towards improved clustering and routing protocol for wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, Vol. 2021, No. 1, pp. 1-31, 2021.
23. I. Abasıkeleş-Turgut, and G. Altan, A fully distributed energy-aware multi-level clustering and routing for WSN-based IoT, Transactions on Emerging Telecommunications Technologies, pp. e4355, 2019.
24. K. Jaiswal, and V. Anand, EOMR: An energy-efficient optimal multi-path routing protocol to improve QoS in wireless sensor network for IoT applications, Wireless Personal Communications, Vol. 111, No. 4, pp. 2493-2515, 2020.
25. N. Chouhan, and S. C. Jain, Tunicate swarm Grey Wolf optimization for multi-path routing protocol in IoT assisted WSN networks, Journal of Ambient Intelligence and Humanized Computing, pp. 1-17, 2020.
26. V. Shilpa, and A. Vidya, A Hybrid Optimization Algorithm and Shamir Secret Sharing Based Secure Data Transmission for IoT based WSN, International Journal of Intelligent Engineering and Systems, Vol. 14, No. 6, pp. 498-506, 2021.
27. V. Shilpa, A. Vidya, and S. Pattar, MQTT based Secure Transport Layer Communication for Mutual Authentication in IoT Network, in: Proceedings of Global Transitions Proceedings, In Press 2022.
28. S. Li, T. Zhang, B. Yu, and K. He, A provably secure and practical PUF-based end-to-end mutual authentication and key exchange protocol for IoT, IEEE Sensors Journal, Vol. 21, No. 4, pp. 5487-5501, 2020.
29. Z. Zhang, Y. Liu, Q. Zuo, L. Harn, S. Qiu, and Y. Cheng, PUF-based key distribution in wireless sensor networks, Computers, Materials Continua, Vol. 64, No. 2, pp. 1261-1280, 2020.

30. Del-Valle-Soto, Carolina, Carlos Mex-Perera, Juan Arturo Nolazco-Flores, Ramiro Velázquez, and Alberto Rossa-Sierra. "Wireless sensor network energy model and its use in the optimization of routing protocols, Energies, Vol. 13, No. 3, pp. 728, 2020.
31. A.M. Fathollahi-Fard, M. Hajiaghaei-Keshteli, and R. Tavakkoli-Moghaddam, Red deer algorithm (RDA): a new nature-inspired meta-heuristic, Soft Computing, Vol. 24, No. 19, pp. 14637-14665, 2020.
32. S.E. Roslin, Data validation and integrity verification for trust based data aggregation protocol in WSN, Microprocessors and Microsystems, Vol. 80, pp. 103354, 2021.

Authors

Shilpa Venkata Rao is currently working as Assistant Professor in Department of Computer Science and Engineering at Cambridge Institute of Technology, Bangalore, India. She received her Bachelor of Engineering degree in Information Science and Engineering from Visvesvaraya Technological University, Belagavi and Master of Engineering degree in Computer Networking from University Visvesvaraya College of Engineering, Bangalore University, Bengaluru. She is currently pursuing Ph.D. under the guidance of Dr. Vidya A in Computer Science and Engineering at Vivekananda Institute of Technology, affiliated to Visvesvaraya Technological University, Bangalore, India. Her research interest includes Internet of Things, with a focus on security and authentication protocols, Cloud Computing.

Vidya Ananth is currently working as Professor and Head of the Department of Compute Science and Engineering at Vivekananda Institute of Technology, Bangalore, India. She received her Bachelor of Engineering and Masters of Engineering degrees in Computer Science and Engineering from Bangalore University, Bangalore. She was awarded Ph.D. in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad. Her area of research includes Data Mining, Soft Computing, Pattern Recognition, Computer Networks and Image Processing. She is a Life Member of Indian Society for Technical Education, Computer Society of India and International Association of Engineers. She is a Fellow of Institute of Engineers.