Wireless Personal Communications (2020) 114:2135–2169
https://doi.org/10.1007/s11277-020-07469-x

SecDL: QoS-Aware Secure Deep Learning Approach for Dynamic Cluster-Based Routing in WSN Assisted IoT

S. Sujanthi[1] · **S. Nithya Kalyani**[2]

Published online: 20 June 2020

Abstract
In WSN-assisted IoT, energy efficiency and security which play pivotal role in Quality of Service (QoS) are still challenging due to its open and resource constrained nature. Although many research works have been held on WSN-IoT, none of them is able to provide high-level security with energy efficiency. This paper resolves this problem by designing a novel Secure Deep Learning (SecDL) approach for dynamic cluster-based WSN-IoT networks. To improve energy efficiency, the network is designed to be Bi-Concentric Hexagons along with Mobile Sink technology. Dynamic clusters are formed within Bi-Hex network and optimal cluster heads are selected by Quality Prediction Phenomenon (QP^2) that ensure QoS and also energy efficiency. Data aggregation is enabled in each cluster and handled with a Two-way Data Elimination then Reduction scheme. A new One Time-PRESENT (OT-PRESENT) cryptography algorithm is designed to achieve high-level security for aggregated data. Then, the ciphertext is transmitted to mobile sink through optimal route to ensure high-level QoS. For optimal route selection, a novel Crossover based Fitted Deep Neural Network (Co-FitDNN) is presented. This work also concentrates on IoT-user security since the sensory data can be accessed by IoT users. This work utilizes the concept of data mining to authenticate the IoT users. All IoT users are authenticated by Apriori based Robust Multi-factor Validation algorithm which maps the ideal authentication feature set for each user. In this way, the proposed SecDL approach achieves security, QoS and energy efficiency. Finally, the network is modeled in ns-3.26 and the results show betterment in network lifetime, throughput, packet delivery ratio, delay and encryption time.

Keywords QoS · Security · Mobile sink · BiC-Hex · Deep learning · Multi-factor authentication · WSN-IoT

✉ S. Sujanthi
sujanthi.s@gmail.com

S. Nithya Kalyani
mail2nithyakalyani@gmail.com

[1] CSE, Ariyalur Engineering College, Ariyalur, India

[2] IT, K.S.R College of Engineering, Tiruchengode, India

1 Introduction

Wireless Sensor Network (WSN) comprises huge number of sensor nodes to perform particular task [1, 2]. Typically, these nodes are resource constrained since the battery energy will sustain for only small period of time. Thus, energy efficiency is the foremost issue in WSN. Likewise, Internet of Things (IoT) is an emerging paradigm that introduces even more smart applications [3]. In particular, IoT is integrated with WSN which can be applicable in smart city, healthcare, transportation, and so on. However, this integration also brings some challenges as scalability, interoperability, energy efficiency and security. In WSN, energy efficiency is improved by optimal clustering, routing and data aggregation along with the mobile sink node [4]. In that, cluster formation is adapted to improve energy efficiency in many research works [5, 6]. In cluster-based network, the sensor nodes are segregated into small clusters upon some criteria. Formation of clusters supports energy efficiency and Quality of Service (QoS) through data aggregation. In addition, the network energy efficiency is improved by constructing the network in an optimal structure. For example, the network is considered as hexagonal network [7–9] to improve the energy efficiency. The hexagonal-based WSN improves the performance of the network in scalability, reliability and energy efficiency. Specifically, it improves the data aggregation process by enabling hop-by-hop data aggregation.

Further, optimal routing is also performed in WSN-IoT for the objective of energy efficiency and QoS improvement [10, 11]. In the absence of efficient routing scheme, the data loss and the energy consumption will be high. The reason behind this degradation is increase in transmission distance. Thus, optimal routing is necessary for energy efficient WSN-IoT networks. Optimal routing also improves the efficiency of IoT applications like wildlife monitoring, smart city, and so on [12]. For satisfying QoS constraints, computational intelligence techniques like optimization techniques, fuzzy logic, reinforcement learning and machine learning (ML) techniques have been used [13]. In route selection multiple metrics are considered by authors. Some of them are residual energy level, hop count, distance, trust value, expected delay and link quality. However, computing these metrics for each route is the major challenging issue in routing. For this reason, some research works consider a single metric and objective. For example, optimal route is selected based on the energy consumption metric [53]. But these works are not able to achieve both QoS and energy efficiency. Security is one of the QoS services that is the major part of any network. However, many research works have been conducted in WSN and IoT in the perspective of security. As stated earlier, WSN-IoT nodes are resource constrained which means lightweight security scheme is essential [14]. A lightweight cryptography scheme mitigates the issue of complex encryption processes which further results in energy efficiency [15, 16]. Especially, the conventional cryptography schemes are designed with the aim to work with desktops and laptops (i.e.) devices with higher energy level. In contrast, the lightweight ciphers are designed to handle the resource constrained devices like sensors, RFID and so on. Thus, the lightweight security protocols become a research trend in recent years [17]. Besides, ML techniques are utilized to improve the security level of IoT networks [18]. These ML techniques are utilized for authentication, access control, cryptography and intrusion detection. The main feature of WSN-IoT network is that it involves both IoT devices like sensors, RFID and also IoT users who access the IoT device data [19]. Thus, it is essential to authenticate the IoT users in order to avoid the unauthorized user access. For authentication, multiple factors such as identity, physical context, tokens and past history are utilized [20]. An efficient authentication procedure will defend

many attacks in the WSN-IoT networks [21]. Thus many research works are held on WSN-IoT networks to improve energy efficiency, QoS and security. However, each work focuses on individual objective. In that too, many research problems are not focused. Thus it is necessary to design a new WSN-IoT network design to achieve better performance. With this in mind, this paper formulates the objectives as follows,

- To improve QoS in WSN-IoT environment along with energy efficiency
- To provide data security by using strong and lightweight cryptography technique
- To prevent unauthorized user access via strong authentication

Although, energy efficiency and security are also QoS constraints, we have separate objectives since both are major challenges in WSN-IoT.

1.1 Motivations

In recent years, WSN-assisted IoT has great attention in many application areas such as medical field, transportation fields, public safety, monitoring application and smart environments [22, 23, 52]. In general, the WSN-IoT network generates huge volume of data which has to be processed and accessed by the remote users [24, 25]. Due to this large volume of data generation and resource constraint ability make achieving QoS in WSN-IoT. Typically, WSNs are divided into multiple clusters to support energy efficiency [50, 51]. Further, security is also major aspect of WSN-IoT [26]. Mostly, the WSN-IoT networks are deployed in an open environment and the data is accessed by the remote users. Thus, there is high possibility for data leakage and theft. In most of the IoT applications, the data must be sure and do not disclosed to unauthorized users since the data is sensitive. In this case security is unavoidable. Majorly, WSN-IoT has following research problems [27, 28],

In QoS—Due to the wireless nature the data transmission is challenging in WSN-IoT. In addition, the data generation rate and dynamic network topology are also affecting the QoS. Till now, QoS is guaranteed through optimal routing and clustering. However, trade-off between QoS and energy efficiency is not yet achieved by previous works. Thus, achieving better QoS is still major challenging issue in WSN-IoT. In particular, the QoS affecting factors are listed as follows,

- Non-optimal route selection
- High energy consumption
- Poor algorithm design
- Lack of network management

In Energy Efficiency—As we know, WSN-IoT is typically large-scale network involves with huge number of resource constrained sensor nodes. Energy efficiency is achieved by minimizing energy consumption through cluster formation and data aggregation. Furthermore, redundant data is also major problem in WSN-IoT. Transmission of redundant data and retransmissions of data will result in huge energy consumption [54]. In cluster formation, CH selection also plays pivotal role. Thus, the factors affecting energy efficiency are,

- Network formation and topology creation
- Improper and frequent CH selection
- Redundant data transmission

- Inefficient data aggregation

In Security—In many research works, the conventional cryptography techniques are utilized for data security and user authentication [55]. However, these existing solutions are not suitable for resource constrained WSN-IoT environment. Besides, these works are unable to ensure high level security level. However, in WSN-IoT it is essential to achieve high-level security without increase in energy consumption. The major security factors are,

- Complexity results is high energy consumption
- Ineffectual algorithm design
- Lack of security in route selection
- Unauthorized user access

These problems are the major motivations of this research. Although all three issues are individual but has a logical relation. Since achieving high level security and QoS will demand high level energy consumption and vice versa. Thus, we are motivated to address this research problem of achieving better security and QoS without loss in energy efficiency in this work.

1.2 Major Contributions

The major contribution of this work lies on the objective design of QoS, Security and Energy Efficiency provision in WSN-IoT. For this objective, this paper has the following contributions,

- Novel SecDL approach is presented with mobile sink enabled Bi-Concentric Hexagonal (BiC-Hex) network structure. Further, the BiC-Hex structure is partitioned into different regions as per angular function.
- Data aggregation is handled by cluster formation in each region of BiC-Hex. Energy efficiency and QoS is achieved by optimal CH selection using Quality Prediction Phenomenon (QP^2) through cumulative parameters. Two-way Data Elimination then Reduction (TDETR) is presented for redundant data elimination which results in energy efficiency.
- Security is ensured for the aggregated data through dynamic one time key. For that, a One Time-PRESENT (OT-PRESENT) which is dynamic and lightweight cryptography technique is proposed.
- Secure data is transmitted through a trusted as well as quality-aware route. Here deep learning-based routing algorithm namely Crossover based Fitted Deep Neural Network (Co-FitDNN) is designed. The design Co-FitDNN converge QoS, energy efficiency and security parameters in routing.
- Finally, IoT users are authenticated by strong authentication scheme designed based on data mining concept. For IoT-user authentication a new Apriori based Robust Multi-factor Validation (ARMV) algorithm is proposed.

1.3 Paper Layout

The rest of this paper is organized as follows: Sect. 2 surveys previous research works held on WSN-IoT network. In Sect. 3, the major research problems are discussed. Section 4

explains the proposed SecDL approach with novel algorithms. In Sect. 5, the proposed SecDL approach is evaluated experimentally and the results are compared with prior works. Finally, Sect. 6 concludes the contributions of this paper. In Table 1, the notations used in this paper are listed out.

2 Related Works

This section surveys the previous research works held on QoS improvement, energy efficiency and security in WSN-IoT. From this critical survey, the existing research gap is identified.

2.1 QoS Improvement in WSN-IoT

Kumar et al. [29] have presented an artificial neural network and fuzzy inference system (ANFIS) for optimal route selection. Along with the ANFIS model, the fuzzy-based CH selection also presented. The major objective of this work is to improve the QoS performance of IoT-oriented WSN networks. For that, multiple parameters such as link bandwidth, centrality, latency, channel state information, SNR, and packet loss ratio are fused by ANFIS model to select optimal route. Here, the ANFIS model is trained by Particle Swarm Optimization (PSO) algorithm. Typically, PSO has convergence issues and falls in local optimal solutions. Thus, PSO-trained ANFIS algorithm degrades the efficiency of route selection. Elappila et al. [30] have proposed a survivable path-based routing in WSN for IoT applications. Authors focus on the performance improvement through optimal route selection. Optimal route is selected based on multiple criteria such as signal-to-noise ratio

Table 1 List of notations

Notation	Description
n	Number of nodes
α	Residual energy level
β	Distance
ω_i	Node degree
δ	Centrality factor
UB, LB	Upper and lower bound
Sim_Dis	Similarity distance
$A(P)$	Aggregated packets
Ξ_j	Random coefficient
$\varkappa$	Secret key of node
$OT - \Psi$	One time key
$\phi[A(P)$	Encrypted data
$\boldsymbol{\Phi} = \{r_1, r_2, \ldots, r_u\}$	Set of candidate routes
$\Pi\boldsymbol{\Phi} = \{r_1, r_2, \ldots, r \ \}$	All available routes
$f(r)$	Fitness of route
$\tau, \Gamma, \zeta, \eta$	Trust value, congestion level, delay, number of hops
ΔC	Correlation between attributes

(SNR), survivability factor, and congestion level. The survivability factor is derived as the ratio of minimum value of available residual energy among every node along that path to the total consumed energy for communication through that path. However, network management is not considered in this work. To improve the network performance it is also necessary to handle the large scale network since the node located far away from the sink will have large energy consumption and loss rate.

Amjad et al. [31] have designed a QoS-ware and heterogeneously clustered routing (QHCR) protocol. The QHCR protocol assures energy efficiency and provides dedicated paths for even delay-sensitive applications. The heterogeneity is introduced by using sensing nodes and fluctuating nodes conjointly in the network. Cost metric and path metric are designed for optimal CH and route selection respectively. The path metric is the cumulative score of initial energy, expected transmission count, and minimum loss. But, consideration of initial energy is not efficient for current route selection since the energy level of a node varies over time period. Zhang et al. [32] have introduced an energy and QoS aware routing protocol for WSN in industrial applications. AT first, the data is provided with priority level through sensing data classification. Then, optimal route is selected based on reliability parameters and timeliness parameters. For path reliability measurement, a link quality measure algorithm (LQMA) is proposed. The LQMA algorithm relies on the energy model and trigonometric function. Further, received signal strength indicator (RSSI) and link quality are used for reliability parameter. The considered parameters are limited and not suitable for selecting an optimal route in the network. Further, security is major aspect of industrial network and not considered in this work. Deepa et al. [33] have proposed an optimized QoS-based clustering with multipath routing (OQoS-CMRP) protocol. In this work, modified PSO algorithm is used for cluster formation and SingleSink-AllDestination algorithm is proposed for optimal multi-hop route selection. The routing algorithm allows the nodes to select optimal next hop in each round. However, PSO based clustering is not effective since it has the convergence issues. Thus, QoS provisioning works are suffered with non-optimal route and CH selection. That is, there is huge research space for QoS improvement in WSN IoT networks.

2.2 Energy Efficiency in WSN-IoT

Preeth et al. [34] have presented adaptive fuzzy multi-criteria decision making (AF-MCDM) approach in WSN-assisted IOT system. The AF-MCDM approach is made up of fuzzy analytical hierarchy process (AHP) and fuzzy technique for order performance by similarity to ideal solution (TOPSIS) methods. Energy efficiency is improved by opting optimal CH using AF-MCDM approach. Execution of fuzzy AHP and fuzzy TOPSIS for CH selection increases time and energy consumption. Ullah et al. [35] have used a hybrid hierarchical clustering approach (HCCA) in WSN-IoT. The HCCA organizes the sensor nodes in distributed three-layer architecture. The upper-layer heads are selected by sink node and are known as grid heads. Then the grid heads select the lower-layer heads which are known as CHs. Network management is performed in a hierarchical manner. Here all nodes are homogenous which means the energy level of all nodes is same initially. Thus selection of a normal node as grid head increases energy consumption for those particular nodes. Rani et al. [36] have introduced a dynamic clustering approach for WSN IoT applications. The major aim of this work is to improve the energy efficiency of the WSN network for IoT applications. For that, this work uses dynamic CH selection process. Dynamic CH is selected by using genetic algorithm (GA). In GA, fitness is evaluated based on

distance with sink node, cluster distance and standard deviation. GA is a typical algorithm that takes large time to find an optimal solution. Thus, using GA for dynamic CH selection is not efficient. Xu et al. [37] have designed an energy efficient region source routing protocol (ER-SR) for WSN-IoT networks. The ER-SR protocol uses a distributed energy region algorithm to select source nodes dynamically. Then the source routing nodes selects optimal path for data transmission. As the sink node is considered to be static, there is high energy consumption for nodes which are located nearer to the sink node. Srinidhi et al. [38] have designed a hybrid energy efficient and QoS aware (HEEQA) algorithm. The HEEQA is the combination of quantum PSO (QPSO) and non-dominated sorting genetic algorithm (NGSA). Authors have aimed to balance the energy among devices along with better QoS. This paper uses NGSA to overcome the convergence problem of QPSO algorithm. However, execution of QPSO and NGSA increases time consumption as NGSA typically consumes more time to converge. Thus energy efficient schemes lack with poor algorithm design which further degrades the energy efficiency.

2.3 Security in WSN-IoT

Li et al. [39] have presented a three-factor authentication scheme for WSN in IoT environments. In three-factor authentication, fuzzy approach is utilized for bio-metric extraction. In general, the considered three factors are biometric, smart card and password. An IoT user is considered to be authorized user when three-factors are satisfied. However, smart card based authentication is not reliable since it has high possibility to be lost. Sathyadevan et al. [40] have presented a protean authentication scheme for IoT environment. Authors have aim to achieve strong and extreme lightweight authentication for IoT end devices. This protean authentication scheme intends to change the security key in regular time interval. In each time, the changed keys are exchanged securely. However, the dynamic key generation process generates fresh keys at any time. This will consume more energy and also time consumption. Ali et al. [41] have attempted to enable trust-based scheme for IoT-assisted WSN. Here data aggregation is performed by external mobile elements (ME). For optimal ME selection, the trust based scheme has been proposed. The trust value for all MEs has been managed by base station and the sensors transmit the data to ME with high trust value. The trust value is updated based on the interaction history with the base station. In this work, trust computation needs the involvement of base station at all time. This means to increased complexity in the network.

Mughal et al. [42] have proposed a logical-tree based secure mobility management (LT-SMM) scheme using mobile service computing in WSN assisted IoT. LT-SMM scheme includes group deployment phase in which mobile node joining and migration protocol is incorporated. Initially, all devices are formed as secure groups. For security purpose, chaotic map based one-way hash function is utilized. Typically, the tree-based keying method increases time consumption and complexity in the network. Tabassum et al. [43] have considered void problem in the WSN-IoT network. In order to mitigate this void problem in routing, GAR and RUT schemes are implemented in which the next-hop neighbor is searched by a greedy search algorithm. The data is secured by using a random number for encryption. This work has limitations as follows: (1) Route selection by greedy algorithm is not efficient and leads to void problem (optimal next-hop selection will avoid this issue), (2) Appending key (random number) with the transmitted data increases the vulnerability of data and (3) Encryption strength is not ensured and fully depends upon the random number generated. Thus, this work is not suitable for IoT environment.

Literature Synthesis—Overall, QoS provisioning schemes, energy efficiency schemes and security schemes are unable to achieve better performance in WS-IoT. The major limitations addressed in these schemes are listed in Table 2. Thus there is achieving QoS, energy efficiency and security is still challenging due to many factors.

3 Problem Definition

This section summarizes the overall research problems considered in this work. This work considers a WSN-IoT network with n number of sensor nodes including static and dynamic nodes, m number of IoT users, mobile sink node and gateway. This work majorly concentrates on three problems as QoS provisioning, energy efficiency and security. For that, specific problems are defined from prior works.

A secure and energy efficient routing model is uses RSA for encryption and type-2 fuzzy for route selection [44]. In general, RSA algorithm requires large time and key size to attain high-level security. Thus, it is not suitable for resource constrained environment. Further, route selection by type-2 fuzzy and then reliability verification increases time consumption. One time pad (OTP)-based cryptography scheme is designed with random number generator [45]. However, generation of OTPs increases the complexity as the security level fully depends upon the randomness. A neuro-fuzzy scheme uses convolutional neural network (CNN) for energy efficient clustering and routing [46]. Here CH is selected based on energy level and distance which is not significant. But cluster formation decision considers multiple metrics which may results in imbalanced clusters (some CHs may have relatively small members compared to others). Cluster formation consumes large energy and time since CNN has to be executed in every sensor node for decision making. To achieve energy efficiency and QoS, energy and interoperable aware routing [47] and residual energy-based CH selection [48] approaches are proposed. The routing algorithm increases bandwidth and energy consumption for initial path set-up. Further, the CH selection by considering single metric is not effective for WSN-IoT. In addition, cluster formation by conventional low-energy adaptive clustering hierarchy (LEACH) protocol doesn't support better scalability.

Problem Statement—Overall, QoS and Security provisioning with energy efficiency lacks due to higher time complexity, energy consumption and poor algorithm design. Still, achieving all three objectives is challenging. Thus, it is necessary to design a novel WSN-IoT structure for this objective. This statement arises following research questions,

- How to design a WSN-IoT network such that it improves energy efficiency?
- What are the major criteria for CH and route selection?
- How to ensure high-level security without loss in energy efficiency?

All these research questions are addressed in this work. And novel algorithms and methodologies are derived to solve these research questions.

4 Proposed SecDL for WSN-IoT

This section explains the overall proposed SecDL approach for WSN-assisted IoT environment. Each proposed algorithm and methodology is explained in detail.

Table 2 Analysis on related works

Category	Methods	Drawbacks
QoS enhancement	ANFIS [29], Survivable Routing [30], QHCR [31], LQMA [32], OQoS-CMRP [33]	Improper route selection Insufficient parameter consideration Poor network management Not suitable for large scale networks
Energy Efficiency	AF-MCDM [34], HCCA [35], GA [36], ER-SR [37], HEEQA [38]	Time complexity High bandwidth and energy consumption Frequent CH selection Energy hole problem
Security	Three-factor authentication [39], Protean authentication [40], trust-based routing [41], LT-SMM [42], GAR&RUT [43]	Higher complexity Poor security credentials Unreliable authentication Untrusted route selection Poor security level

4.1 Network Model

In this work, we consider a network model with n number of sensor nodes denoted as $N_1, N_2, \ldots, N_n$ and m number of IoT users denoted as $U_1, U_2, \ldots, U_m$, a mobile sink (MS) and a gateway (GW). Further, the network is constructed as BiC-Hex structure with a mobile sink node. The BiC-Hex is constructed by arranging two hexagons in a concentric manner. Let the BiC-Hex consists of two hexagons such interior (Hex_I) and exterior (Hex_E). The network is constructed with two hexagons in order to improve energy efficiency. Consideration of two hexagons allows network division which enable effectual cluster formation. Then, the height and base of Hex_I (H_I, B_I) are always lower than height and base of Hex_E (H_E, B_E) i.e. $H_I, B_I < H_E, B_E$. The area of Hex_I is computed as,

$$A\left(Hex_I\right) = \frac{1}{2} H_I B_I \tag{1}$$

Similarly, the area of Hex_E is computed as,

$$A\left(Hex_E\right) = \left(\frac{1}{2} H_E B_E\right) - A\left(Hex_I\right) \tag{2}$$

Then, the BiC-Hex is split into six equal sectors to improve the energy efficiency by forming clusters within the sectors. In addition, splitting the network into sectors also allows the allocation of visiting points for MS. For that, the BiC-Hex is divided by 120° based on the origin point (O). This intersection is considered as the visiting point (VP) for the MS. A data collection round starts from VP_1 and ends with VP_6. In this way, MS visits each VP and collects the sensing data. The considered network model is shown in Fig. 1.

The proposed network model has following assumptions,

- The network involves with n_1 number of static (SN) and n_2 number of mobile (MN) sensor nodes such that $n_1 + n_2 = n$.
- Always, $n_1 > n_2$.

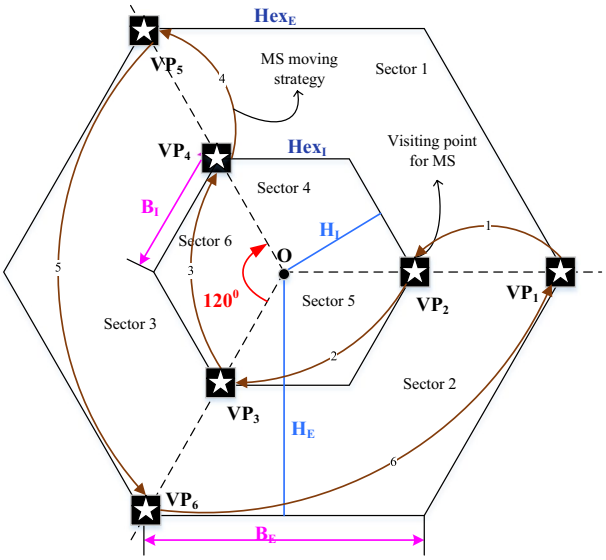

Fig. 1 The proposed WSN-IoT model

- Initially, all nodes have the same energy level and deployed random manner over the network. Each sensor uses GPS positioning technology to find the current location of its own and the neighboring nodes.
- The network is constructed with a mobile sink node to collect the data from all sensor nodes. From here, the sink node and the mobile sink node represent the same in this paper. The current position of sink node is known to all other nodes in the network.

With the above assumptions, the network is constructed and the proposed algorithms are applied.

4.2 Energy Model

In this work, all nodes perform sensing, transmission and reception. The energy is consumed for all three operations. Besides, processor energy (E_{pro}) function is also consumed by the processor.

The overall energy consumption for a node is computed as follows,

$$E_{Con} = E_{TX} + E_{RX} + E_{Idle} + E_{CCA} \tag{3}$$

where E_{Con} is computed in terms of energy consumed for transmission (E_{TX}), reception (E_{RX}), idle listening (E_{Idle}) and channel assessment (E_{CCA}). Further, E_{TX} and E_{RX} for transmitting and receiving ρ bits is computed as follows,

$$E_{TX} = E_{Proc} * \rho + \varepsilon_{FS} * \rho * d^2, d \leq d_0 \tag{4}$$

$$E_{TX} = E_{Proc} * \rho + \varepsilon_{MF} * \rho * d^4, d \geq d_0 \tag{5}$$

The E_{TX} is computed based on free space model parameter (ε_{FS}) and fading model parameter (ε_{MF}). The threshold distance d_0 is computed as follows,

$$E_{RX} = E_{Pro} * \rho \tag{6}$$

In the proposed network, each sensor node follows the above energy model.

4.3 Overall Architecture of SeC-DL

The overall architecture of SecDL approach is shown in Fig. 2. The BiC-Hex is split into six sectors such a way it supports effective data aggregation. Then, clusters are formed within each sector. Dynamic clusters are formed with optimal CHs. Then data is aggregated without any redundant data. For data collection, DL-based routing scheme is deployed. Data security and user security is ensured by lightweight cryptography and authentication schemes. Each process is explained in the following subsections.

4.4 Dynamic Cluster Formation

When the network is constructed, then the nodes in each sector are clustered in order to support data aggregation. Cluster formation improves both energy efficiency as well as QoS. In this work, the network model is considered with static and mobile sensor nodes. Energy consumption of mobile sensor node is greater than static nodes. Thus, static sensor

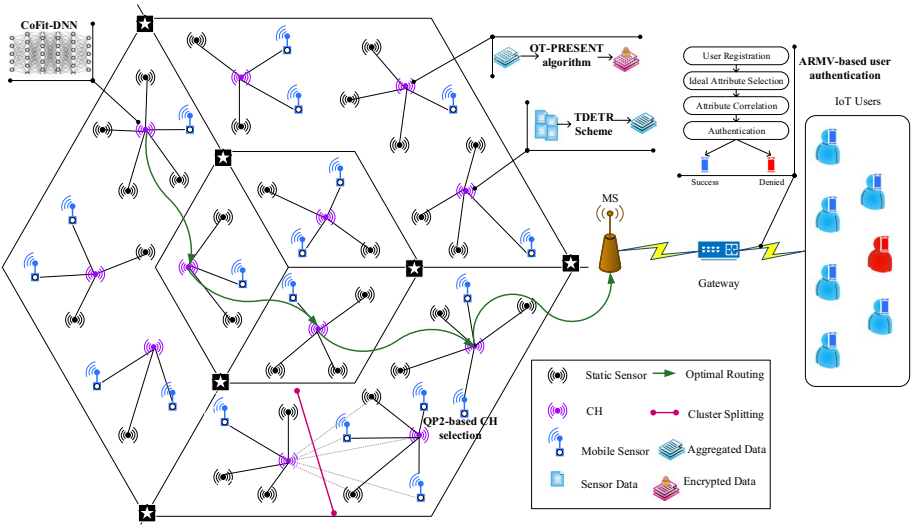

Fig. 2 Overall SecDL-based WSN-IoT Architecture

nodes are considered as CH candidates. The CH selection process is initiated by using QP^2. In each sector, the number of static nodes is fixed and the mobile nodes vary over the time period. At first, the CHs are selected in each sector. For that, QP^2 computes quality value (δ). A quality of a node to become CH is computed in terms of cumulative parameters such as remaining energy level (α), distance with VP (β), node degree (γ) and centrality factor (ω). Each parameter is defined as follows,

Definition 1 (*residual energy level*) It denotes the current energy level of the node. It is computed as the difference between initial energy level and total consumed energy over a period. A node with higher α is has high possibility to become CH since the CH is responsible for data collection and aggregation.

Definition 2 (*distance*) It represents the distance between a node and the nearby VP. As sink node aggregates the data at VP, it is necessary to select node nearby to the VP. The distance between node N_i and VP_j is computed by using Euclidean distance measure as follows,

$$\beta = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \tag{7}$$

Definition 3 (*node degree*) It is the measure of number of neighboring nodes connected with the candidate node. It can be determined through Received Signal Strength Index (RSSI) values recived from the neighboring nodes. Higher value of γ increases the possibility to become CH.

Definition 4 (*Centrality factor*) It defines the closeness of the candidate node with its neighbors. That is, it computes the average distance between the candidate node and its neighboring nodes. It can be computed as follows,

$$\omega_i = \frac{\gamma - 1}{\sum_{i \neq j} d(i,j)} \tag{8}$$

By using all four important parameters, optimal CH is selected. The quality value is determined as follows,

$$\delta = \frac{a.\alpha + c.\gamma + d.\omega}{b.\beta} \tag{9}$$

where a, b, c, d are the weight values and selected in way that $a + b + c + d = 1$. In this work, initial CH selection is performed by sink node and CH rotation is performed in a self-organized manner. After identification CHs, cluster formation is initiated.

Dynamic Clustering—Each CH sends Join_Req to its neighboring nodes. By receiving the request message, each non-CH node computes the distance with the CH. Then, the node sends Join_Rep to the CH which has minimum distance. When the CH is closer to the node, then the energy efficiency and QoS will be improved. Thus we perform clusters based on distance measure. As per our work, both static and mobile nodes are involved in the network. Thus, it is necessary to perform re-clustering in the case of node movement. In this work, clustering and re-clustering process is performed in self-organized manner (i.e.) without involvement of sink node. Thus, it minimizes the overhead introduced by sink node communication. Dynamic clustering and re-clustering is performed in following three cases,

Case 1—When a mobile node is moved from one cluster, then the current CH removes that node from member list. Similarly, the moved mobile node sends Rejoin_ Req to the nearby another CH. Upon receiving the request, the nearby CH joins that node as member and updates its member list.

Case 2—When a cluster has lower number of nodes due to movement of mobile nodes, then the CH of that cluster initiates the cluster merging process. For that, a lower bound (*LB*) value is set for number of nodes in the cluster. The *LB* value is computed as follows,

$$LB = \frac{2n - n}{k_{max}} \tag{10}$$

The lower bound is set based on the number of nodes in the network and the maximum number of clusters k_{max}. When cluster merging decision is made, then CH sends a Merge_ Req to nearby CHs. Then the CHs respond the Merge_Res to the CH with the information of number of members. Then the CH sends confirmation message Confirm_Res to the CH which has minimum number of nodes. Then, both clusters are merged and the CH with high quality value is selected as CH.

Case 3—Similar to case-2, when the number of nodes in a cluster exceeds the upper bound (*UB*), then the CH initiates cluster splitting process. The *UB* value is computed as follows,

$$UB = \frac{n}{k_{max}} \tag{11}$$

The *UB* is computed based on n and k_{max} value. When a cluster has more that *UB* members, then it starts cluster splitting process. For that, it sends splitting message Split_Msg to the member which has higher quality value. Then the member become a CH and performs cluster formation.

Thus, proposed cluster formation is performed in a self-organized manner without frequent involvement of sink node. When current CH drains out of energy, then it selects another node as next CH and rotates its role the next CH. Proposed dynamic cluster formation not only supports energy efficiency but also improves QoS.

4.5 Data Aggregation

In each cluster, CH performs data aggregation process to minimize the size of data to be transmitted to sink node. In several WSN-IoT applications, the nodes intend to report periodic report which leads to the presence of redundant data. On the other hand, network coding process has great attention in minimizing the transmission data size. Thus, we present TDETR-based data aggregation. The process of TDETR is twofold as: (1) it eliminates the redundant data from the aggregated data (2) then it reduces the data size through network coding. After aggregation of data, CH checks the similarity between a data against all other data. For example, consider a data series as $P_1, P_2, P_3, .., P_l$ where l denotes the number of members in the cluster. In first level, the similarity distance (*Sim_Dis*) is computed between each packet. It is formulated as follows,

$$Sim\_Dis = \left|x(P_i) - x(P_j)\right| + \left|y(P_i) - y(P_j)\right| \tag{12}$$

Here x, y represents the coordinates of data packets P_i and P_j. If $Sim\_Dis = 0$, then the both packets are more similar and one packet is dropped. In this manner, CH finds *Sim_Dis* between all data packets and eliminates all redundant data from the aggregated data.

In second level, the aggregated data is compressed into single packet in order to minimize the number of transmission between CH and MS. For data compression, TDETR uses random linear coding (RLC) approach. In RLC, a random coefficient is utilized to compress the aggregated data. Let $\mathbb{l}$ be the number of data packets after redundant data elimination. The CH compresses $\mathbb{l}$ packets into single packet as follows,

$$ComPac = \sum_{j=1} \Xi_j P_j \tag{13}$$

Here Ξ_j represents the random coefficient. At this stage, CH compresses $\mathbb{l}$ number of packets into single *ComPac*. That is, CH minimizes the number of transmissions with MS. Thus the proposed work minimizes energy consumption by minimizing the number of transmission between CH and MS.

4.6 Data Security Provision

After aggregation of data packets, the CH performs encryption top secure the aggregated data $A(P)$. For data security, we proposed a new OT-PRESENT which is the lightweight encryption protocol. The PRESENT algorithm is ultra-lightweight and works better than the conventional AES, RSA cryptosystem [58]. As it achieves better security level without increase in overhead, it can be used in WSN network. Initially, all mobile and static nodes are provided with a secret key $\varkappa$ which is generated by the sink node initially. Initial key is generated as the sequence of pseudo-random bits. In proposed work, 80-bits of pseudo-random bits are generated for each node by sink node. Although PRESENT is ultra-lightweight procedure, it is symmetric cryptography primitive. That is, it uses same key for encryption and decryption. Thus, we propose a novel OT-PRESENT algorithm which

generates OT-Cluster Key ($OT-\Psi$) at each round. The cluster key is the new concept in PRESENT algorithm that uses the secret keys of cluster members for key generation. As per the proposed SecDL, the clusters are formed dynamically which means the cluster members are varied over time period. With this in mind, we utilize this self-organized property for dynamic key generation.

Let us consider a cluster with l members as $N_1, N_2, N_3, \ldots, N_l$. Each node has initial secret key as $\varkappa_1, \varkappa_2, \varkappa_3, \ldots, \varkappa_l$ correspondingly. In the proposed work, the CH is responsible to generate $OT-\Psi$ in each round. For that, it applies simple XOR operations on the secret keys of its member nodes. The $OT-\Psi$ is generated at time t_1 as follows,

$$OT-\Psi = \varkappa_1 \oplus \varkappa_2 \oplus \varkappa_3 \oplus \cdots \oplus \varkappa_l \tag{14}$$

Likewise, when the cluster is organized dynamically, the member list will be modified. Thus, in next round the CH generates the $OT-\Psi$ with the new member keys. In this way, the cluster key is changed at each time. After the generation of $OT-\Psi$ performs encryption as in PRESENT algorithm. In PRESENT algorithm, 31 rounds are performed to produces the ciphertext. In each round, the RoundKey is XOR-ed with the data block that is resulted from previous round. At first round, the plaintext of $A(P)$ is XOR-ed with $OT-\Psi$. Then, the $OT-\Psi$ is shifted in a right circular manner to produce RoundKey. Then, the XOR-ed value from the first block is again XOR-ed with the RoundKey. In this manner, 31-rounds are performed to produce the ciphertext ($\phi[A(P)]$).

Pseudocode 1: OT-PRESENT algorithm

Input: $A(P)$ and $\varkappa_1, \varkappa_2, \varkappa_3, \ldots, \varkappa_l$
Output: $\phi[A(P)]$
Begin
  //One Time Key Generation
  Check Cl
  For $\forall N_i \in Cl$
    Initialize← $\varkappa_1, \varkappa_2, \varkappa_3, \ldots, \varkappa_l$
    Generate ← $OT - \Psi$
  End **For**
  //OT-PRESENT Encryption
  $Round \leftarrow 1$
  $State \leftarrow Plaintext\ A(P)$
  If $(Round < 31)$, Then
    $RoundKey = OT - \Psi$
    $State \leftarrow RoundKey \oplus State$
    $State \leftarrow SBoxLayer(State)$
    $State \leftarrow PermutationLayer(State)$
    $Round \leftarrow Round + 1$, do
    $RoundKey \leftarrow RightCircularShift(OT - \Psi, 19)$
    $RoundKey[76 - 79] \leftarrow SBoxLayer(Key[76 - 79])$
    $RoundKey[15 - 19] \leftarrow OT - \Psi[16 - 19]$
  End **do**
  End **If**
  If $Round = 31$, Then
    $lastRoundKey \leftarrow generateKey(Key, R)$
    $State \leftarrow State \oplus lastRoundKey$
    $\phi[A(P)] \leftarrow State$
  End **If**
End

Pseudocode 1 Description—The algorithm 1 presents pseudocode of proposed OT-PRESENT algorithm. The first four lines explain the process of $OT - \Psi$ generation. Then the subsequent lines explain the procedure of encryption and RoundKey generation by OT-PRESENT algorithm. At last, the $\phi[A(P)]$ is generated for the plaintext of $A(P)$. In this manner, the aggregated data is encrypted by OT-PRESENT algorithm.

As the proposed OT-PRESENT uses simple XOR operations, it is relatively lightweight. At the same time, generation of $OT - \Psi$ in each round increases the security level of OT-PRESENT algorithm.

4.7 Optimal Data Transmission

After completion of encryption, the CH transmits the aggregated ciphertext $\phi[A(P)]$ to the *MS*. As stated earlier, the *MS* follows the moving strategy as,

$$Strategy = \left[VP_1 \rightarrow VP_2 \rightarrow VP_3 \rightarrow VP_4 \rightarrow VP_5 \rightarrow VP_6 \rightarrow VP_1\right] \tag{15}$$

All CHs have the knowledge of current *VP* of the MS. Thus, the CH selects trusted optimal route for data transmission. Selection of optimal path results in QoS

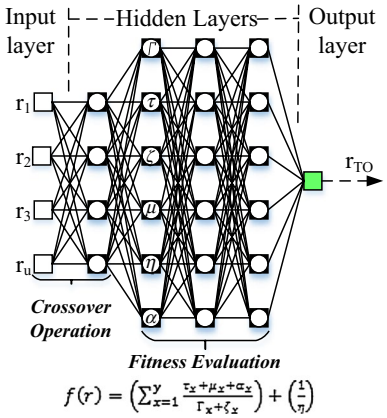

Fig. 3 Structure of proposed Co-FitDNN

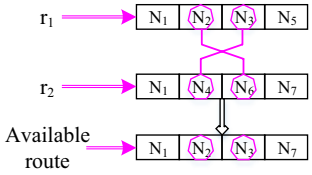

Fig. 4 Function of crossover operator

improvement as well as energy efficiency. Besides, selection of trusted route will improve the security level. Thus, we propose Co-FitDNN algorithm that selects trusted optimal route for data transmission. The proposed Co-FitDNN uses deep learning [56] approach for acquiring most suitable route from the set of available paths based on multiple metrics. Processing route selection in deep structure will results in better performance. We apply crossover operator over the first layer of deep neural network to generate all available paths between CH and sink node. Then, each route is evaluated based on the fitness function in hidden layers. In the output layer, the optimal route is selected for data transmission. The overall structure of proposed Co-FitDNN is shown in Fig. 3.

The process of proposed Co-FitDNN can be explained as follows,

Input layer—This layer is composed of input neurons. In this layer, the candidate routes $\boldsymbol{\Phi} = \{r_1, r_2, \ldots, r_u\}$ are initialized. The candidate routes are direct route between source CH (CH_S) and the MS.

Hidden layers—The Co-FitDNN comprises multiple hidden layers (up to L) as $h_1, h_2, \ldots, h_L$. In the first layer applies crossover operator on the input routes.

The crossover is a genetic operator that generates new combination of routes from the $\boldsymbol{\Phi}$. The process of crossover operator is shown in Fig. 4. From the crossover layer, all available routes are discovered. It can be denoted as $\boldsymbol{\Pi\Phi} = \{r_1, r_2, \ldots, r \}$ and $\mathbb{u} > u$. Then, each route is provided with a weight value in hidden layers. In Co-FitDNN, the weight value is computed in terms of fitness function ($f(r)$).

The $f(r)$ is computed by considering the following routing metrics,

1. *Trust value (τ)*—Trust value is computed as the forwarding ability of the nodes in a route. For a node N_i, the trust value can be computed as follows,

$$\tau_i = \sum_{j=1}^{n} \frac{\mathfrak{B}_{ij} + 1}{\mathfrak{B}_{ij} + \mathfrak{M}_{ij} + 2} \tag{16}$$

Here $\mathfrak{B}_{ij}$ represents the normal behavior of node N_i that is observed by node N_j. Likewise, $\mathfrak{M}_{ij}$ represents the malicious behavior of N_i that is observed by N_j. The normal behavior counts the number of packets forwarded by the node successfully and malicious behavior counts the number of packets dropped by the node. In this manner, each node computes the τ and share its trust value with others. In general, the malicious nodes involve in packet dropping which can be overwhelmed by our work.

2. *Congestion Level (Γ)*—It defines the number of packets available in the buffer. When congestion level is high, then the data will get delay to reach the destination.

3. *Link bandwidth (μ)*—It measures the available bandwidth between the nodes. When bandwidth is lower, then data loss will occur.

4. *Delay (ζ)*—The expected delay is computed based on the propagation, processing, and queuing delay introduced in that node.

5. *Number of hops (η)*—It counts the number of hops between CH_S and MS.

Along with the above metrics, α of the route is also considered. By combining all six parameters, the $f(r)$ function is formulated as follows,

$$f(r) = \left(\sum_{x=1}^{y} \frac{\tau_x + \mu_x + \alpha_x}{\Gamma_x + \zeta_x} \right) + \left(\frac{1}{\eta} \right) \tag{17}$$

Here x represents the x-th node in r and y represents the number of nodes in the route r. In typical DNN, the weight function provides the importance of the corresponding input. In Co-FitDNN, the importance of each route is determined in term of $f(r)$.

Output layer—This layer selects the optimal route from all available routes generated in hidden layers. The output is computed as follows,

$$\Theta = \sigma\big(f(r)_L \sigma\big(f(r)_{L-1} \sigma\big(\ldots \sigma\big(f(r)_1\big)\big)\big)\big) \tag{18}$$

where σ is the activation function. In this way, the output layer selects a trusted optimal route r_{TO} for data transmission. Through this r_{TO}, the CH_S transmits the $\phi[A(P)]$ to MS.

Pseudocode 2 Description—Algorithm 2 describes the pseudocode for route selection by Co-FitDNN. At first, the candidate routes are fed into input layer. Then, crossover operation is applied to generate available routes. The number of generated available routes is always higher than candidate routes. The hidden layer learns major metrics for each route in the available route set. Then, these metrics are fused to obtain the fitness value. This fitness value is assigned as the weight value for each route. Finally, the most fitted routed is selected for data transmission. Then optimal route is selected based on the fitness function.

Pseudocode 2: Co-FitDNN algorithm

Input: $\Phi = \{r_1, r_2, .., r_u\}$
Output: r_{TO}
Begin
  Initialize all $r_i \in \Phi$ in input layer
  For $\forall r_i \in \Phi$ do
    Apply crossover
    Generate $\leftarrow \Pi\Phi = \{r_1, r_2, .., r_{\mathbb{m}}\}$
  End **For**
  For $\forall r_i \in \Pi\Phi$, do
    Learn $\leftarrow \tau, \Gamma, \mu, \zeta, \eta, \alpha$
    Compute $f(r_i)$
    Assign $f(r_i) \rightarrow wieghtfunction$
  End **For**
  Collect $f(r_i)$ from all neurons
  Compute Θ
  Return (r_{TO})
End

Through dynamic clustering, data aggregation, and routing the network performance is optimized. The data is collected by MS and stored in the cloud for end users. To enable internet connectivity, gateway is used. The MS transmits the data to gateway to serve the end users.

4.8 IoT User Authentication

Proposed SecDL based WSN-IoT allows the end users to access the sensory data through gateway. Before access, the gateway validates the legitimacy of the users in order to secure the data from unauthorized access. SecDL proposes ARMV algorithm for user authentication. The ARMV algorithm uses the data mining concept for user authentication in a novel manner. The idea of ARMV algorithm is to map the idea set of authentication credentials of the user through frequent itemset analysis. At first, each user register their credentials as user ID ($\mathbb{U}_{ID}$) and password ($PW\_$) to the gateway. For all registered users, the secret key (SK) is generated and given that can be used in authentication process. We assumed that the gateway stores all historical information for each user from the time of registration. For instance, for a user $\mathbb{U}_{ID}(i)$ the past history include $A_1, A_2, A_3, \ldots, A_A$. Here A denotes the attribute and a history includes A number of attributes for each user. In ARMV algorithm following attributes are considered: Location ($Loc\_$), Timestamp ($T\_$), internet information ($Int\_$) and channel state information ($CSI\_$). In most of the times, the temporal differences in $CSI\_$ of the mobile users can be used for authentication [49]. The idea behind this consideration is that, $CSI\_$ measurements for the same user within coherence time period will be moreover same. Likewise, the $Int\_$ defines the ratio between number of access requests and number of successful requests through the internet. The Apriori algorithm is an important data mining approach that finds the frequent itemset from the several transactions. We use this technique to mine frequent attribute set for each user for authentication.

Let consider a set of attributes for $\mathbb{U}_{ID}(i)$ over a time period $T = \{t_1, t_2, t_3, \ldots, t_{10}\}$. For $\mathbb{U}_{ID}(i)$, the ARMV algorithm first mines the frequent attribute set as ideal attribute set (Att_{Ideal}) as follows,

1. First, it scans the history of $\mathbb{U}_{ID}(i)$ to get support of s each instance.
2. Then set of candidate attributes are generated and prune the unfrequent instance.
3. Then, this candidate is set is scanned to find the frequent attribute set and store it in the candidate set.

This process is performed for all instances in the candidate set.

Finally, the support and confident values are determined to find the ideal set. Based on the support and confident value, the Apriori algorithm maps the ideal set for each user. This process is performed for all registered users (Table 3).

For our considered example, the ideal attributes are $Loc\_ \rightarrow XXX, Int\_ \rightarrow 1, CSI\_ \rightarrow 10db$. Thus the Att_{Ideal} for $\mathbb{U}_{ID}(i)$ is $\{\text{XXX}, 1, 10\}$. When, the user sends authentication request, the gateway extracts the current attributes (Att_{cur}) values from the request. Then, the correlation (ΔC) between Att_{cur} and Att_{Ideal} is determined as follows,

$$\Delta C = \Delta Loc\_ + \Delta Int\_ + \Delta CSI\_ \tag{19}$$

where,

$$\Delta Loc\_ = 1, if\ Loc\_ = XXX \tag{20}$$

$$\Delta Int\_ = |1 - Int| \tag{21}$$

$$\Delta CSI\_ = |10 - CSI\_| \tag{22}$$

Then the authentication is performed based on different levels according to the ΔC value. The ARMV authenticates the user as follows,

- *Level 1*—if $\Delta C = 3$, then the user id is verifies to validate the user
- *Level 2*—if $2 < \Delta C < 3$, then the $\mathbb{U}_{ID}(i)$ and the $PW\_$ is verified to authenticate the user
- *Level* 3—if $1 < \Delta C < 2$, then the $\mathbb{U}_{ID}(i)$, $PW\_$ and the $SK\_$ are verified to validate the user

Table 3 Attribute set of $\mathbb{U}_{ID}(i)$

History number	$Loc\_$	$T\_$	$Int\_$	$CSI\_$
1	XXX	t_1	1	10 db
2	XXX	t_2	1	9db
3	XXX	t_3	0.8	10 db
4	YYY	t_4	0.9	10.5 db
5	YYY	t_5	1	9db
6	XXX	t_6	0.9	10 db
7	XXX	t_7	1	10 db
8	XXX	t_8	1	9 db
9	XXX	t_9	0.9	11 db
10	XXX	t_{10}	1	10 db

If $\Delta C < 1$, then the user request is denied. Thus the ARMV algorithm users both user credentials and channel credentials for user authentication. Involvement of ARMV algorithm prevents the unauthorized user access in the network.

Pseudocode 3 description—The pseudocode of proposed ARMV algorithm is presented. Initially, the users are registered and then the ideal attribute set is learned for each user. When the user sends $Auth_{Req}$, the algorithm extracts the current attribute set. Then, the correlation is determined between ideal and current attribute set. Upon the ΔC value the authentication is performed.

Therefore, the proposed SecDL presents a novel approach for achieving better QoS, energy efficiency, and security in WSN-IoT networks. Proposed clustering, data aggregation, encryption, routing and authentication schemes support the objectives in WSN-IoT. The proposed SecDL improves QoS and energy efficiency without loss in security.

Pseudocode 3: Pseudocode for ARMV algorithm

```
Input: 𝕌1, 𝕌2, 𝕌3, ...
Output: Authentication results
Begin
  For each 𝕌
    Register← 𝕌ID, PW_, SK_
    Learn ← Loc_,T_,Int_,CSI_
    Compute s
    Prune unfrequent set
    Find← Att_Ideal
  End For
  Receive Auth_Req(𝕌ID(i))
  Learn ← Att_cur
  Compute ΔLoc_,ΔInt_,ΔCSI_
  Find ΔC
  If (ΔC = 3), Then
    Verify 𝕌ID(i)
    If (2 < ΔC < 3), Then
      Verify (𝕌ID(i)&&PW_)
      If (1 < ΔC < 2), Then
        Verify (𝕌ID(i)&&PW_&&SK_)
        Deny the Auth_Req
      End If
    End If
  End If
End
```

At last, the proposed SecDL is evaluated based on performance metrics. For that QoS and energy efficiency metrics are considered.

5 Experimental Analysis

In this section, the proposed SecDL is analyzed through experimentations. This section introduces the simulation environment and then provides brief comparative analysis.

5.1 Simulation Setup

The proposed SecDL based WSN-IoT network is modeled in network simulator-3.26 (ns-3.26). The ns-3.26 is the event based simulation tool that supports various network simulations [57]. Firstly, the ns-3.26 is installed in the PC that uses Ubuntu 14.04 operating system. Then, the network parameters are set according to our work. The algorithms are written in C++ programming languages then executed with the support of Python language. Before starting the simulation, we set the n value, initial energy, positions of the nodes in ns-3.26. According to this setup, the overall simulation is performed and the results are observed.

In Table 4, the significant simulation parameters considered to model the SecDL is depicted. Each node is configured upon these parameters. Here we consider 100 sensor nodes with 70% of static nodes and 30% of mobile nodes (i.e.) 7o static nodes and 30 mobile nodes. Thus, $n_1 > n_2$ condition is satisfied. However, our work supports even large number of nodes. Transmission rage of each node is set to 200 m. Further, the mobility of the sink node is set to 10 m/s (maximum). By considering these parameters, the SecDL is modeled in the simulator and experimentally analyzed to obtain the results.

The Fig. 5a, b illustrate the simulation topology and environment of proposed SecDL in ns-3.26 and netanim. From this setup, the results are observed and analyzed with existing works. Here the nodes in red color represent the static nodes, blue denotes the mobile nodes, and green represents the IoT users. With the above configuration, we start the implementation.

Real-world Use Case of SecDL WSN-IoT—The proposed WSN-IoT network has many real-time applications. Here we demonstrate one apt use case of smart city application. The major aspect of smart city application is that in covers both static as well as mobile nodes for various purposes. As our work supports both types of nodes, SecDL is more suitable for WSN-IoT environment.

In Fig. 6, the proposed SecDL approach is validated for pollution monitoring in smart city applications. In smart cities, pollution monitoring is the prime process. For pollution monitoring, the sensor nodes are deployed on the smart buildings (static sensors). Growing technology in transportation allows us to use vehicles for monitoring applications. Thus, the mobile sensor nodes are deployed on the moving smart vehicles. In this case, all sensor nodes are specified to perform monitoring task. We consider the following sensors for real-time monitoring,

- MQ 135—It is used to monitor the combustible gases. It is highly sensitive to *Ammonia, Sulphide and Benzene steam*.
- HR202—It measures the *humidity level* in the air. It detects the ambient humidity in three levels.
- Liquid pH Value detection sensor—It measures the *pH value* in the air. The pH value ranges from 0 to 14.
- DHT-11—It detects the *temperature* with $\pm 2°$ accuracy. Typically, it measures the temperature from 0° to 50°.

All these sensor nodes are deployed in static as well as in vehicles. Then, the sensed data is aggregated from sensor nodes by CHs and the redundant data is eliminated.

The aggregated data is encrypted then stored in remote server. For the connectivity, we use WiFi gateway. In smart city applications, the data is accessed by the citizens and also

Table 4 Simulation parameters

Parameter	Value
Simulation area	1000 ×. 10 m
Network topology	BiC-Hex
Network standard	WiFi
Sensor parameters	
Number of static nodes	70
Number of mobile nodes	30
Number of sectors	6
Number of sink nodes	1
Initial energy level	750 J
Mobility model	RandomWay
Mobility speed	10 m/s (max)
User parameters	
Number of users	25
Number of attributes	4
Number of instances	50
CSI interval	10 ms
Channel and packet parameters	
Bandwidth	20 MHz
Data rate	54 Mbps
Number of packets	1000
Packet size	1024 bits
Packet interval	10 µs
Number of Retransmissions	7 (max)
Packet interval	1 ms
Header size	24 bits
CoFit-DNN parameters	
Number of hidden layers	10
Number of neurons in output layer	1
Learning rate	0.001
Crossover rate	0.5
Activation function	Sigmoid
Simulation time	100 s

Fig. 5 **a** Topology of SecDL. **b** Simulation environment of SecDL

Fig. 6 SecDL-based smart city application (pollution monitoring)

by authorities. Thus, the data is vulnerable to many security threats. The SecDL allows the users to access the data only after strong authentication. That is the proposed SecDL is more suitable for smart city applications.

5.2 Comparative Study

In order to validate the efficiency of SecDL, this section performs comparative analysis. The proposed work is evaluated under QoS, energy efficiency and security metrics. The observed results are compared with existing CNN [46], QoS routing [47], LEACH-CH [48], OTP [45] and Secure WSN-IoT [44]. All these works are compared in the major aspects in Table 5.

5.3 Analysis on Network Lifetime

Network lifetime is defined as the amount of time in which the network is fully active. In other words, it is defined as the maximum operational duration of the network to perform specified task. We compare the network lifetime with respect to network size (i.e.) number of nodes and packet size. Figure 7 shows the comparative analysis on the network lifetime with respect to network size and packet size. The analysis shows that the proposed SecDL improves the network lifetime even with large number of nodes and packet size. When the number of nodes increases then the network lifetime is also increased. This is because the in the presence of large number of nodes, there will be high possibility for minimized retransmissions. In addition, optimal CH selection is also improved with large n. Thus, network lifetime is gradually increases in all works. However, the SecDL achieves highest lifetime up to 220 rounds while LEACH-CH achieves lowest lifetime up to 100 rounds. Thus, the nodes in LEACH-CH based network sustain only for 100 rounds which is 50% lower than SecDL. Besides, other works as CNN (112), QoS routing (107), and secure WSN-IoT (135) also have lower lifetime when compared to SecDL.

Similarly, Fig. 7b shows the analysis with respect to packet size. When packet size is increased, then more energy is required to transmit the data from source to destination. Thus, the lifetime is decreased with the increase in packet size. As well, proposed SecDL achieves better network lifetime even with the large packet size. Even with the 1000 bits of packets, the SecDL sustains for 200 rounds. But the existing works drop between 150 rounds. In particular,

Table 5 Limitations of Prior Works

Method	Security	QoS	Energy efficiency	Limitations
CNN	Not provided	Provided by optimal route selection		Lack in security Increases time and energy consumption
QoS-routing	Not provided	Achieved by optimal routing	Energy constraint is considered for routing	Increases bandwidth consumption Poor algorithm design
LEACH-CH	Not provided	Not focused	Energy efficient CH is selected	Not suitable for large scale networks Fail to achieve energy efficiency
OTP	One-time Pad based encryption is proposed	Not focused	Not focused	Security level is low Increases complexity
Secure WSN-IoT	RSA and SHA-1 are used	Type-2 Fuzzy based routing is proposed	Data Scheduling is performed	High energy and bandwidth consumption Security level is low but complexity is high

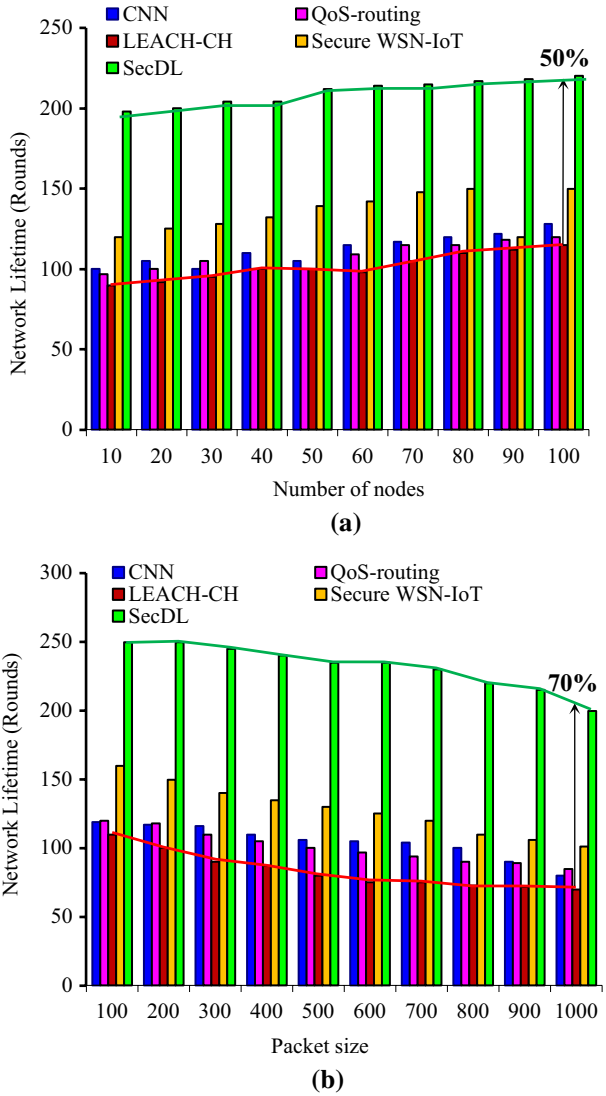

Fig. 7 Analysis on network lifetime **a** based on network size, **b** based on packet size

LEACH-CH method provides 70 rounds for the packet size of 1000 bits. That is, optimal CH selection alone is not sufficient for improving network lifetime. Proposed SecDL uses TDETR for data aggregation which eliminates the redundant data and also minimizes the number of transmissions. Thus, the proposed work achieves better network lifetime.The major reason behind this huge difference is that, proposed work concentrates on all three major aspects such as QoS, energy efficiency and security. In the presence of better QoS, and strong security the network lifetime will be improved.

5.4 Analysis on PDR

PDR is defined as the amount of packets generated by the network to the number of packets successfully delivered to the destination.

In Fig. 8, the PDR is compared between proposed and previous research works. With the increase in number of nodes, the PDR is also increased. SecDL provides PDR above 90% without regarding to the network size. That is, ≅. 9 of packets have reached the destination successfully. At the same time, LEACH-CH transmits only 70% of packets without loss. The reason behind this huge loss is, LEACH-CH transmits the data through non-optimal route. However, QoS-routing scheme also has 24% of packet loss. This routing algorithm considers the initial path set-up stage which consumes more energy and bandwidth. Further, data transmission through initial optimal path is efficient. Likewise, all

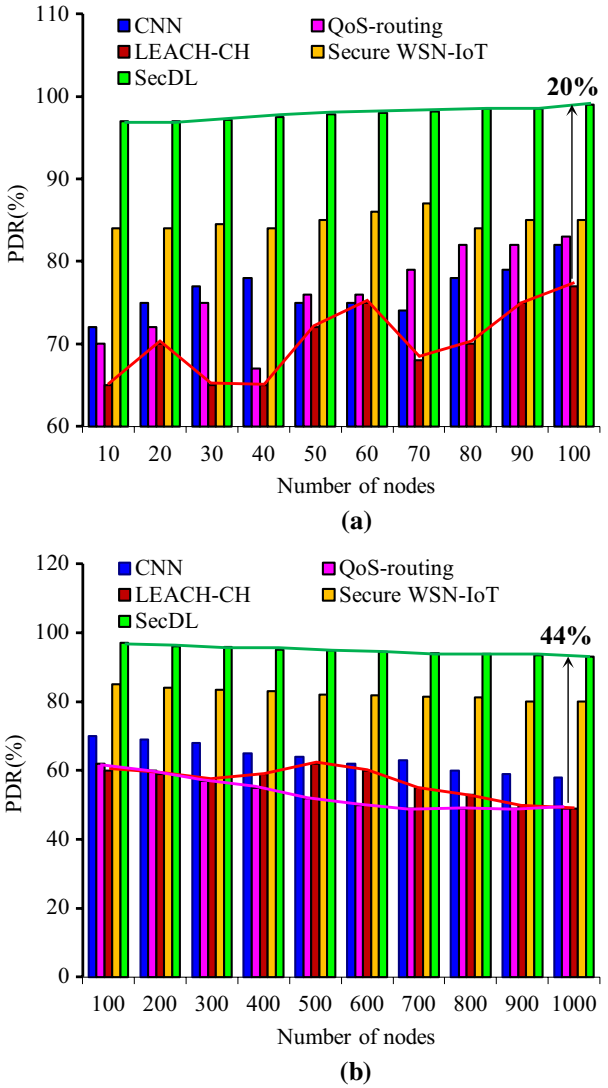

Fig. 8 Analysis on PDR **a** based on network size, **b** based on packet size

other works like CNN (25%) and Secure WSN-IoT (15%) also have huge packet loss. The analysis shows that any previous works is able to achieve better PDR.

Likewise, Fig. 8b compares the proposed SecDL with respect to packet size. When the packet size is large then there will be additional need of energy and bandwidth. Thus, the PDR is inversely proportional to packet size. The proposed SecDL transmits 93% of packets (has the size of 1000 bits) successfully. For the same packet size, the LEACH-CH and QoS routing algorithm transmits inly 49% of packets. This is 44% lower than SecDL. In data transmission, security is also major aspect since most of the attackers drop the packets to degrade the network performance. For this reason, we Co-FitDNN with trust value. Thus, the proposed SecDL achieves better PDR regardless packet size. Further, we compress the $A(P)$ into single packet which minimizes the packet loss.

In WSN-IoT, PDR will be high when the network has the ability to handle huge number of nodes and packets. For that, it needs a new architecture since the existing works are unable to achieve better data transmission. Consideration of QoS, energy efficient, and security parameters improves the PDR and optimizes the data transmission in SecDL.

5.5 Analysis on Throughput

Throughput is defined as the amount of data transmitted successfully to the specific destination at given period of time. In WSN-IoT, it estimates the amount of data received by the sink node successfully.

In Fig. 9a, b, the throughput achieved by proposed SecDL in compared with prior research works. The analysis shows that, the throughput is increased with increase in network size and decreased with the increase in packet size. But in both cases, SecDL outperforms with other works. The major reason behind this huge deviation is that, the proposed work considers the major three objectives as QoS, energy efficiency and security in WSN-IoT. Thus, proposed work achieves better throughput. At given period of time, the proposed SecDL achieves throughput higher than 90% with respect to both network size and packet size. When $n = 100$, then SecDL achieves throughput up to while the LEACH-CH have throughput of 65%. This is 34% lower than SecDL. That is, the prior works are unable to perform well in all the time. But the SecDL has the ability to outperform at any given period of time.

When the packet size is high, then the previous works have much lower throughput. Specifically, LEACH-CH method provides throughput of 55%. The major reason is the prior works not able to handle large packet size. For instance, LEACH-CH uses non-optimal path for data transmission, CNN has higher energy consumption, QoS routing has higher bandwidth consumption and Secure WSN-IoT has time and energy consumption. Therefore, the previous research works are not suitable for resource constrained WSN-IoT environment. At the same time proposed SecDL achieves better throughput by extending QoS, security and energy efficiency. Thus, the proposed SecDL is suitable for WSN-IoT environment.

5.6 Analysis on Delay

Delay is measured as the time taken by a data packet to reach its destination rom the source. It includes, propagation delay, processing delay and queuing delay.

Figure 10 shows the comparative analysis for delay. When the data packet is transmitted through the non-optimal route, then the delay will be high. However, we transmit the

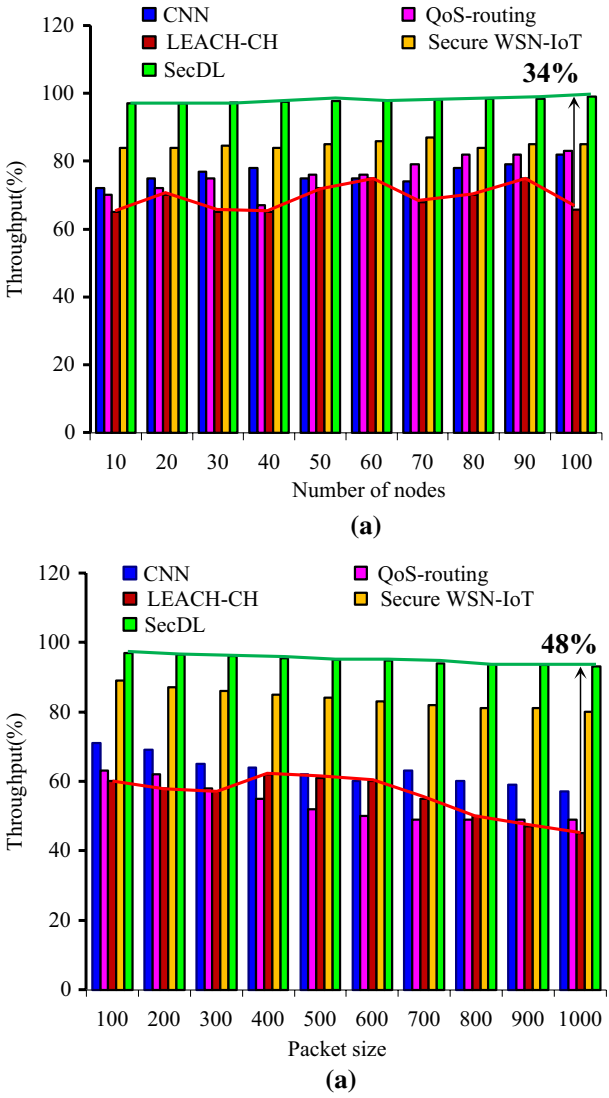

Fig. 9 Analysis on throughput **a** based on network size, **b** based on packet size

data through fittest route selected by Co-FitDNN by considering six major matric. In that, we also consider the delay as the metric for $f(r)$ computation. Thus we transmit the data through the route which provides lower delay. This idea is reflected in the results also. In the comparison graph, the proposed SecDL has lower delay than prior works. The previous research works are not able minimize delay due to improper algorithm and initial path set-up phase. In that, the LEACH-CH protocol has delay up to 16 s as it transmits the data through non-optimal path. Even QoS-routing algorithm also fails to minimize the delay since it consumes time to set the initial path. In secure WSN-IoT route selection itself consumes large time and energy. Thus the prior research works are not able to handle the delay. Besides, the proposed work introduces 1 s of delay even in the presence of 100 nodes. This is due to our work elects optimal CH and aggregates the data. Further, a trusted

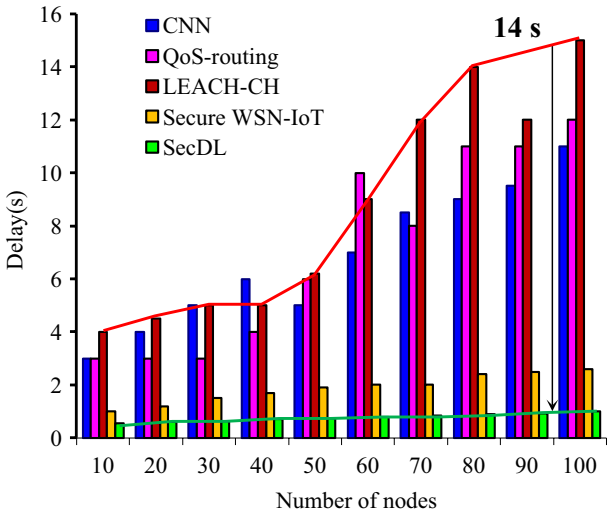

Fig. 10 Analysis on delay

and energy efficient route is selected for data transmission. Thus, the proposed work minimizes the delay.

5.7 Analysis on Encryption time

Encryption time measures the time taken to encrypt the data before transmission. This metric evaluates the efficacy of OT-PRESENT algorithm.

In Fig. 11, the comparison on encryption time is depicted. Here, OTP method and secure WSN-IoT are considered for comparison. In OTP method, the key length and randomness ensures the security level and time consumption. In secure WSN-IoT, RSA is used for encryption which is not suitable for resource constrained environment. When $n = 100$, then the OTP algorithm takes 10 s to encrypt the data and RSA algorithm takes 5 s for encryption. For the same network size, proposed OT-PRESENT algorithm takes only 1.1 s

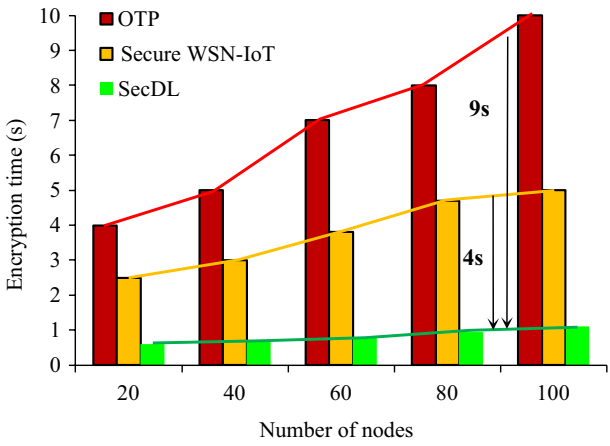

Fig. 11 Analysis on encryption time

Table 6 Time complexity comparison

Process	Secure WSN-IoT	SecDL
Data Aggregation	$O(3N + N^2)$	$O(N)$
Encryption	$O(\log(N)^2)$	$O(N^2)$
Routing	$O\left(N + \frac{N}{2}\right)$	$O(2N)$
Authentication	$O(N + 2^{52})$	$O(N^2)$
Overall complexity	$O\left(\frac{7N}{2} + \log(N)^2 + 2^{52}\right)$	$O(3N + 2N^2)$

Table 7 Numerical analysis on results

QoS and energy efficiency metric	Main results ± SD				
	CNN	QoS-routing	LEACH-CH	Secure WSN-IoT	SecDL
Network lifetime (rounds)					
Upon network size	112 ± 0.2	107 ± 0.9	101 ± 0.7	135 ± 0.4	210 ± 0.2
Upon packet size	104 ± 0.7	100 ± 0.8	83.2 ± 0.2	127 ± 0.7	232 ± 0.01
PDR (%)					
Upon network size	76 ± 0.5	76 ± 0.2	70 ± 0.2	84 ± 0.9	98 ± 0.2
Upon packet size	63 ± 0.8	53 ± 0.2	56 ± 0.4	82 ± 0.2	95 ± 0.25
Throughput (%)					
Upon network size	76 ± 0.5	76 ± 0.2	69 ± 0.08	84 ± 0.8	98 ± 0.13
Upon packet size	63 ± 0.1	53 ± 0.6	55 ± 0.5	83 ± 0.8	95 ± 0.1
Delay (s)	6 ± 0.8	7 ± 0.1	8 ± 0.67	2 ± 0.02	0.7 ± 0.5

which is much lower than prior works. As the PRESENT algorithm is ultra-weight, we achieve this much of results. Thus, the proposed work is suitable for resource constrained environment too.

5.8 Complexity Analysis and Results Discussion

Time complexity is compared between proposed SecDL and secure WSN-IoT in Table 6. Time complexity is computed for cluster formation, data aggregation, route selection, encryption and authentication. The comparison shows that the proposed SecDL has lower complexity that previous work.

As we minimize the frequent clustering and routing, the time complexity is much minimized. Further, routing is performed between CHs and MS. This reduces the complexity in route selection.

From the obtained results, it is assured that the proposed SecDL achieves better QoS, energy efficiency, and security. The major reason behind this work is a novel construction of WSN-IoT network with the necessary considerations. Table 7 summarizes the numerical observations on mean and standard deviation achieved by the proposed and existing works.

The analysis shows that the proposed work outperforms with prior research works in all aspects. That is, the proposed cluster formation, data aggregation, routing, encryption and authentication schemes enhance the performance of SecDL. The analysis shows that the

proposed work achieves better mean values for each performance metric. Furthermore, the standard deviation (SD) is also minimum in the proposed work. Thus the proposed work is suitable for WSN-IoT environment.

In Table 8, the theoretical facts behind the numerical results are summarized. The table analyzes each and every aspect of proposed approaches and its contributions in the results.

Overall, the proposed SecDL satisfies all requires of QoS, energy efficiency and security in WSN-IoT. Besides, the complexity analysis confirms that the proposed SecDL is apt for resource constrained environment.

6 Conclusion

In this paper a novel SecDL approach is designed to improve QoS, energy efficiency and security in WSN-IoT environment. At first, the network is constructed as BiC-Hex and divided into six sectors. In each sector, dynamic clusters are formed and reformed in a self-organized manner. In each cluster, CH selection follows QP^2 algorithm that selects optimal CH according to multiple parameters. Data aggregation follows TDETR algorithm that minimizes redundant data and compress the data. The aggregated data is encrypted by OT-PRESENT algorithm which is lightweight and also provides strong security. For data transmission, optimal route is selected based on six major parameters. The optimal route is selected in Co-FitDNN with trust, QOS, and energy parameters. In order to secure the data from unauthorized user access, IoT users are authenticated at gateway. For strong authentication, ARMV algorithm is proposed. Finally, the SecDL approach is modeled in ns-3.26 and analyzed in terms of performance metrics. The results show promising research

Table 8 Theoretical Assessment

Proposed method	Impact on results
BiC-Hex Topology	Improves energy efficiency Supports data aggregation Provides better QoS
QP2 algorithm	Minimizes frequent CH selection Increases network lifetime Improve PDR and throughput
Dynamic Clustering	Supports data aggregation Increases energy efficiency Improves the network lifetime Supports effectual data transmission
TDETR algorithm	Eliminates redundant data Reduces number of transmission Improves energy efficiency Minimizes packet loss
OT-PRESENT	Ensures high level security Mitigates the energy consumption problem Reduces time complexity
Co-FitDNN	Selects optimal route Improves PDR and throughput Minimizes delay Improve QoS, security, and energy efficiency
ARMV algorithm	Improves the security level Prevents unauthorized user access

directions in WSN-IoT. In future, we have planned to extend this work with more than one sink nodes to further reduce the energy consumption. We have also interested to evaluate SecDL in large-scale environment.

References

1. SalehiPanahi, M., & Abbaszadeh, M. (2018). Proposing a method to solve energy hole problem in wireless sensor networks. *Alexandria Engineering Journal, 57,* 1585–1590.
2. Kalyani, S. N., & Sujanthi, S. (2018). Dynamic clustering approach in wireless sensor networks. *International Journal of Management, Technology and Engineering, 8*(XI), 781–785.
3. Abidoye, A. P., & Obagbuwa, I. C. (2017). Models for integrating wireless sensor networks into the Internet of Things. *IET Wireless Sensor Systems, 7,* 65–72.
4. Movva, P., & Rao, P. T. (2019). Novel two-fold data aggregation and mac scheduling to support energy efficient routing in wireless sensor network. *IEEE Access, 7,* 1260–1274.
5. Ali, A., Ming, Y., Si, T., Iram, S., & Chakraborty, S. (2018). Enhancement of RWSN lifetime via firework clustering algorithm validated by ANN. *Information, 9,* 60.
6. Shen, J., Wang, A., Wang, C., Hung, P. C., & Lai, C. (2017). An efficient centroid-based routing protocol for energy management in WSN-assisted IoT. *IEEE Access, 5,* 18469–18479.
7. Priyadarshi, R., Singh, L., Kumar, S., Sharma, I., & Randheer, (2018). A hexagonal network division approach for reducing energy hole issue in WSN. *International Journal of Pure and Applied Mathematics, 118*(20), 1003–1008.
8. Shrivastav, K., & Kulat, K. D. (2018). Energy efficient scalability of three level hexagonal heterogeneous broad transmission distance protocol (3L-HEXA-HTBTDP) for WSN-IoT networks. *International Journal of Communication Systems, 31,* 1–27.
9. Shrivastav, K., & Kulat, K. D. (2020). Scalable energy efficient hexagonal heterogeneous broad transmission distance protocol in WSN-IoT Networks. *Journal of Electrical Engineering & Technology, 15,* 95–120.
10. Hanif, S., Khedr, A. M., Aghbari, Z. A., & Agrawal, D. P. (2018). Opportunistically exploiting internet of things for wireless sensor network routing in smart cities. *Journal of Sensor and Actuator Networks, 7,* 46.
11. Jabbar, W. A., Saad, W. K., & Ismail, M. (2018). MEQSA-OLSRv2: A multicriteria-based hybrid multipath protocol for energy-efficient and QoS-aware data routing in MANET-WSN convergence scenarios of IoT. *IEEE Access, 6,* 76546–76572.
12. Ahmed, A., Pasha, M.A., Ahmad, Z., Masud, S., & Sikora, A. (2017). Energy efficient sensor network routing (EESNR) protocol for large distributed environmental monitoring applications. In *2017 9th IEEE international conference on intelligent data acquisition and advanced computing systems: Technology and applications (IDAACS)*, Vol. 2, pp. 740–745.
13. Kaur, T., & Kumar, D. (2019). A survey on QoS mechanisms in WSN for computational intelligence based routing protocols. *Wireless Networks*. https://doi.org/10.1007/s11276-019-01978-9.
14. Buchanan, William J., Li, Shancang, & Asif, Rameez. (2017). Lightweight cryptography methods. *Journal of Cyber Security Technology, 1*(3–4), 187–201.
15. Tsai, K., Leu, F., Su, T., & Chang, Y. (2017). A light weight data encryption method for WSN communication. In *BWCCA*.
16. Hung, C., & Hsu, W. (2018). Power consumption and calculation requirement analysis of AES for WSN IoT. *Sensors, 18,* 1675.
17. Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2017). A lightweight IoT security protocol. In *2017 1st cyber security in networking conference (CSNet)*, pp. 1–8.
18. Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine, 35,* 41–49.
19. Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2017). A lightweight mutual authentication protocol for the IoT.
20. El-hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors, 19,* 1141.
21. Mishra, D., Vijayakumar, P., Sureshkumar, V., Amin, R., Islam, S. H., & Gope, P. (2017). Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. *Multimedia Tools and Applications, 77,* 18295–18325.

22. Ang, K. L., & Seng, J. K. P. (2019). Application specific internet of things (ASIoTs): Taxonomy, applications, use case and future directions. *IEEE Access, 7,* 56577–56590.
23. Ray, P. P. (2018). A survey on internet of things architectures. *Journal of King Saud University Computer and Information Sciences, 30,* 291–319.
24. Boubiche, S., Boubiche, D. E., Bilami, A., & Toral-Cruz, H. (2018). Big data challenges and data aggregation strategies in wireless sensor networks. *IEEE Access, 6,* 20558–20571.
25. Čolaković, Alem, & Hadzialic, Mesud. (2018). Internet of things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks, 144,* 17–39.
26. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks, 141,* 199–221.
27. Kulkarni, S., Vani, R. M., & Hunagund, P. V. (2018). Review on IoT based case study: Applications and challenges. In *ICICI-2018*.
28. Khan, F. I., & Hameed, S. (2018). Understanding security requirements and challenges in internet of things (IoTs): A review. *Journal of Computer Networks and Communications*.
29. Kumar, S., Lal, N., & Chaurasiya, V. K. (2018). A forwarding strategy based on ANFIS in internet-of-things-oriented wireless sensor network (WSN) using a novel fuzzy-based cluster head protocol. *Annals of Telecommunications, 73,* 627–638.
30. Elappila, M., Chinara, S., & Parhi, D. R. (2018). Survivable path routing in WSN for IoT applications. *Pervasive and Mobile Computing, 43,* 49–63.
31. Amjad, M., Afzal, M., Umer, T., & Kim, B. (2017). QoS-aware and heterogeneously clustered routing protocol for wireless sensor networks. *IEEE Access, 5,* 10250–10262.
32. Zhang, W., Liu, Y., Han, G., Feng, Y., & Zhao, Y. (2018). An energy efficient and QoS aware routing algorithm based on data classification for industrial wireless sensor networks. *IEEE Access, 6,* 46495–46504.
33. Deepa, O. S., & Suguna, J. (2017). An optimized QoS-based clustering with multipath routing protocol for Wireless Sensor Networks. *Journal of King Saud University – Computer and Information Sciences*.
34. Preeth, S., Dhanalakshmi, R. V., Kumar, R., & Shakeel, P. M. (2018). An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system. *Journal of Ambient Intelligence and Humanized Computing*, 1–13.
35. Ullah, M. F., Imtiaz, J., & Maqbool, K. Q. (2019). Enhanced three layer hybrid clustering mechanism for energy efficient routing in IoT. *Sensors, 19,* 829.
36. Rani, S., Ahmed, S. H., & Rastogi, R. (2019). Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications. *Wireless Networks*.
37. Xu, C., Xiong, Z., Zhao, G., & Yu, S. (2019). An energy-efficient region source routing protocol for lifetime maximization in WSN. *IEEE Access, 7,* 135277–135289.
38. Srinidhi, N. N., Lakshmi, J., & Kumar, S. M. (2019). Hybrid energy efficient and QoS aware algorithm to prolong IoT network lifetime.
39. Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Journal of Network and Computer Applications, 103,* 194–204.
40. Sathyadevan, S., Achuthan, K., Doss, R., & Pan, L. (2019). Protean authentication scheme—A time-bound dynamic KeyGen authentication technique for IoT edge nodes in outdoor deployments. *IEEE Access, 7,* 92419–92435.
41. Ali, B. A., Abdulsalam, H. M., & AlGhemlas, A. (2018). Trust based scheme for IoT enabled wireless sensor networks. *Wireless Personal Communications, 99,* 1061–1080.
42. Mughal, M. A., Shi, P., Ullah, A., Mahmood, K., Abid, M., & Luo, X. (2019). Logical tree based secure rekeying management for smart devices groups in IoT enabled WSN. *IEEE Access, 7,* 76699–76711.
43. Tabassum, A., Sadaf, S., Sinha, D., & Das, A. K. (2020). Secure anti-void energy-efficient routing (SAVEER) protocol for WSN-based IoT network.
44. Jain, J. K. (2019). Secure and energy-efficient route adjustment model for internet of things. *Wireless Personal Communications, 108,* 633–657.
45. Boakye-Boateng, K., Kuada, E., Antwi-Boasiako, E., & Djaba, E. (2019). Encryption protocol for resource-constrained devices in fog-based IoT using one-time pads. *IEEE Internet of Things Journal, 6,* 3925–3933.
46. Thangaramya, K., Kulothungan, K., Logambigai, R., Lavina, L. S., Ganapathy, S., & Kannan, A. (2019). Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. *Computer Networks, 151,* 211–223.
47. Shah, S. B., Chen, Z., Yin, F., Khan, I. U., & Ahmad, N. (2018). Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks. *Future Generation Computing Systems, 81,* 372–381.
48. Behera, T. M., Mohapatra, S. K., Samal, U. C., Khan, M. S., Daneshmand, M., & Gandomi, A. H. (2019). Residual energy-based cluster-head selection in WSNs for IoT application. *IEEE Internet of Things Journal, 6,* 5132–5139.

49. Liu, H., Wang, Y., Liu, J., Yang, J., Chen, Y., & Poor, H. V. (2018). Authenticating users through fine-grained channel information. *IEEE Transactions on Mobile Computing, 17*(2), 251–264.
50. Kalyani, S. N., Sasikala, E., & Gopinath, B. (2015). Collaborative data processing in WSN using Voronoi fuzzy clustering. *International Journal of Computers Communications & Control, 10*(3), 348–356.
51. Dattatraya, K. N., & Rao, K. V. (2019). Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN. *Journal of King Saud University-Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2019.04.003.
52. Kalyani, S. N., & Mary, P. R. (2018). Energy efficient by piezoelectric effect synchronous multicast protocol (PESM) in wireless sensor networks. *Journal of Electrical Engineering, 18*(1), 1–7.
53. Zeng, B., & Dong, Y. (2016). An improved harmony search based energy-efficient routing algorithm for wireless sensor networks. *Applied Soft Computing, 41,* 135–147.
54. Tan, J., Liu, W., Xie, M., Song, H., Liu, A., Zhao, M., et al. (2019). A low redundancy data collection scheme to maximize lifetime using matrix completion technique. *EURASIP Journal on Wireless Communications and Networking, 2019,* 1–29.
55. Singh, P., & Chauhan, R. K. (2017). A survey on comparisons of cryptographic algorithms using certain parameters in WSN. *International Journal of Electrical and Computer Engineering, 7*(4), 2232–2240.
56. Wang, L., & Xia, K. (2019). Data fusion algorithms for wireless sensor networks based on deep learning model. In *HP3C '19*.
57. Yang, J., Akyurek, A. S., Tilak, S., & Rosing, T. S. (2018). Design of transmission manager in heterogeneous WSNs. *IEEE Transactions on Emerging Topics in Computing, 6,* 395–408.
58. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., Seurin, Y., & Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. In *CHES*.

S. Sujanthi received the B.E. degree in CSE from Anna University Chennai in 2009, the M.E. degree in CSE from Anna University of Technology Coimbatore in 2011 and she is Pursuing Ph.D. in Information and Communication Engineering from Anna university Chennai, she is Assistant Professor with Ariyalur Engineering College Ariyalur. Her current research interests are WSN, data aggregation techniques and security with IOT. Her research has been Published International Journals.

Dr. S. Nithya Kalyani received the B.E. degree in IT from Deemed University in 2000, the M.E. degree in CSE from Anna University Chennai in 2004 and the Ph.D. degree in Information and Communication Engineering Chennai in 2014, she is Associate Professor with K.S.R College of Engineering Tiruchengode. She has Authored over 80 papers in related International Conferences and Jounarls. Her current research interests are WSN with IOT, security with IOT, dynamic clustering approach with WSN, data aggregation methods. She was Supervisor with 8 scholars, 7 scholars are pursuing and 1 had completed.