phdprimehelp@gmail.com
+91-97 91 62 64 69

Ph.D. Research Proposal

Doctoral Program in "Department Name"

Dynamic Cluster based WSN-IoT for Secure and Energy aware Data Aggregation – A Deep Approach

by

<Name of the Candidate>

<Reg. No of the Candidate>

<Supervisor Name>

<Date of Submission (DD MM 20YY>

1. INTRODUCTION

Wireless Sensor Network (WSN) is an developing network paradigm that comprises huge number of sensor nodes that are dedicated to perform certain task [1]. The nodes deployed in the WSN are resource constrained (i.e.) has limited resource but have to perform sensing, transmitting, and receiving [2]. This computations leads to energy hole problem in WSN environment. Internet of Things (IoT) has been witnessed as a promising technology to enable future smarter world [3]. In many application cases, WSN is integrated with IoT in order extend its application scenarios. For example, WSN-IoT environment can be applicable for smart city applications [6]. However, security and energy efficiency are the major concerns in WSN integrated IoT environment [4]. The data transmitted from the sensor nodes must be secured with necessary security mechanisms in order to minimize the vulnerability. Since security is major constraint in WSN-IoT, it also introduces energy efficiency problems [5]. Thus it is necessary to tradeoff security and energy consumption in the network. In order to mitigate energy consumption, clustering, data aggregation, routing, MAC scheduling, and mobile sink deployment are considered as optimal solutions [7], [8].

Artificial Neural Network with Fuzzy Inference System (ANFIS) model was presented for optimal cluster formation and route selection in WSN [9]. Particle Swarm Optimization (PSO) algorithm is utilized for training of ANFIS which has local optima problems. A trust based approach is proposed used to enable data transmission in WSN-IoT [10]. However, trust computation with the involvement of BS increases complexity. An adaptive fuzzy rule based clustering approach is proposed in WSN assisted IoT along with immune inspired routing algorithm [11]. Execution of Fuzzy-AHP and Fuzzy-TOPSIS increases the time consumption for CH selection. A hybrid hierarchical clustering approach (HCCA) is presented for WSN assisted IoT [12]. Selection of grid head leads to node early dead for grid head. In routing, survivable path is selected for data transmission [13]. Network management and energy consumption balancing is critical in this work. For security purpose, a logical tree based rekeying mechanism

was proposed [14]. However, tree based rekeying method increases time consumption and complexity in the network.

2. PROBLEM STATEMENT

2.1 Overall Problem Statement

- ☑ Cluster formation and CH selection must be optimal without increase in time consumption
- ☑ Data transmission route must be selected by considering multiple constraints to ensure QOS and security level
- ☑ Data security must be provided with lightweight cryptography scheme without loss in security
- ☑ Another major issue is that IoT device authentication is also a major concern to be considered in WSN-IoT environment

2.2 Specific Research problems

Paper 16

Title: Energy Aware Cluster and Neuro-Fuzzy Based Routing Algorithm for Wireless Sensor Networks in IoT

Concept

This paper deals with optimal clustering and routing in WSN-IoT networks. Here the authors have designed a neuro-fuzzy model for attaining aforesaid objectives. Neuro-fuzzy is modeled by using Convolutional Neural Network (CNN) which is one of the deep neural networks. Initially the sensor network is clustered by k-means algorithm. In cluster formation, the cluster joining decision is made by executing 256 rules in neuro-fuzzy model.

Problems

→ 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 CMs compared to others).

→ Cluster formation consumes large energy and time since CNN has to be executed in every sensor node for decision making.

Proposed Solutions

→ CH selection by QPA approach considers all significant metrics.

→ Self-organized dynamic clustering is performed by static sensor nodes which minimizes energy consumption

Paper 17

Title: Secure Anti-Void Energy-Efficient Routing (SAVEER) Protocol for WSN-Based IoT Network

Concept

This paper considers 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. If void is identified in selected path, then it executes RUT mechanism for mitigating void problem. The data is secured by using a random number for encryption.

Problems

→ Route selection by greedy algorithm is not efficient and leads to void problem (optimal next-hop selection will avoid this issue).

→ Appending key (random number) with the transmitted data increases the vulnerability of data.

→ Encryption strength is not ensured and fully depends upon the random number generated.

Proposed Solutions

→ Route selection is performed by FitDRN which selects optimal route for data transmission

→ Group key is generated in each round and the sink node extracts the key based on CMs

→ Random group key generation and PRESENT based encryption ensures required security level

Paper 18

Title: Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks

Concept

This paper deals with the QoS improvement in WSN assisted IoT networks. The overall process is initiated with the path set-up phase. In path set-up phase, optimal path between each sensor node and BS is identified based on hop count. This process is started by BS through broadcasting hello packets over the network. After path set-up phase, CHs are selected based on energy level and distance with BS. Further cluster formation is performed based on RSSI value between CH and other nodes.

Problems

→ Route selection before cluster formation is not necessary because in cluster based network the data can be transmitted via CH.

→ Initial path set-up for every node increases packet overhead which affects bandwidth and energy efficiency.

Proposed Solutions

→ Inter-cluster routing is performed after cluster formation by FitDRN which improves the data transmission

Paper 19

Title: Residual energy based cluster-head selection in WSN for IoT application

Concept

This paper aims to improve energy efficiency and QoS in WSN based IoT applications. The network is clustered based on hybrid hierarchical cluster formation approach. The incorporated hierarchical clustering approach is LEACH and CH selection in first round is performed as in LEACH. From next rounds, CH selection is performed based on residual energy level.

Problems

→ CH selection based on single metric is not suitable for effective data transmission.
→ LEACH based cluster formation introduces large energy consumption because the CHs which are away from the network needs large energy for data transmission.
→ LEACH protocol is not suitable for large-scale networks. However, IoT applications demands protocols which support large network size.

Proposed Solutions

→ CH selection is performed based on multiple significant metrics
→ Cluster formation by self-organizing property minimizes energy consumption
→ Proposed work is suitable for large-scale network too

Paper 20

Title: Encryption Protocol for Resource-Constrained Devices in Fog-Based IoT using One-Time Pads

Concept

In this paper, an encryption scheme is proposed for resource constrained devices in fog-IoT. Authors have highlighted that the proposed algorithm is also suitable for resource constrained sensor nodes. Here encryption is performed based on one time pad (OTP) which is used as secret key. Each OTP can be used for single encryption and decryption. OTPs are

generated by random number generator (RNG). The security level of encryption scheme depends upon the randomness introduced by RNG.

Problems

→ Generation of one-time pads increases the complexity of the scheme

→ Security level depends upon the randomness of generated random number but it increases the computational as well as time complexity

Proposed Solutions

→ One time key is generated based on secret key of group members through XOR operations

→ Security level is ensured with group key (changed with cluster splitting and merging) and PRESENT algorithm

3. PROPOSED WORK

To mitigate aforesaid problems, we proposed a novel WSN model for secure IoT applications. Our proposed WSN-IoT model comprises both dynamic and static sensor nodes, mobile sink node, Wi-Fi gateway, and IoT users. Our research objectives are,

☑ To improve QoS in WS-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

To achieve above objectives, we propose following processes,

(i) Dynamic Cluster Formation

We construct our network with **Two-Concentric Hexagons (TC-Hex)** in order to define the ***visiting points (VPs)*** for mobile sink movement. Further, the network is divided into three regions by 120^0 which produces six sectors. Then we form multiple clusters within the network region. Initially, optimal CH is selected by using a new concept of **Quality Prediction**

Approach (QPA) approach. Here the static nodes in each sector are considered and optimal CHs are selected for cluster formation. QPA approach considers ***Energy level, Distance with VP, Node Degree, and Centrality factors.*** Cluster formation is performed based on distance and number of neighbor nodes. Further, in order to ménage the clusters, dynamic cluster splitting and merging processes are enabled.

(ii) Dual Data Aggregation

Our objective is to attain QoS and energy efficiency. Thus we perform data aggregation in CH level. We proposed a **Bi-Data Elimination then Reduction (BDETR)** scheme in which we concentrate on both redundant data elimination as well as data aggregation. Proposed BDETR scheme reduces the data size considerably which results in minimum energy consumption and improved QoS.

(iii) Lightweight Data Encryption

After data aggregation, CH encrypts the data to ensure data security. We propose a novel **One Time-Hummingbird (OTH)** algorithm for encryption. Proposed OTH algorithm is relatively lightweight which is suitable for resource constrained environment. Here One Time Key is generated through group key generation process which improves the security level. Thus the one time key is dynamic as well as strong enough for data encryption.

(iv) Secure Data Transmission

CH sends the encrypted data to mobile sink node through optimal path. We design a novel **Fitted Deep Reinforcement Network (FitDRN)** for optimal route selection between current CH and sink node. Here we apply crossover operator to generate multiple available paths initially and then we apply fitness computations for optimal route selection. In order to ensure security and QoS, we consider ***trust value, residual energy level, Congestion Level, Link Bandwidth, Delay, and Number of Hops*** constraints are considered in fitness computation.

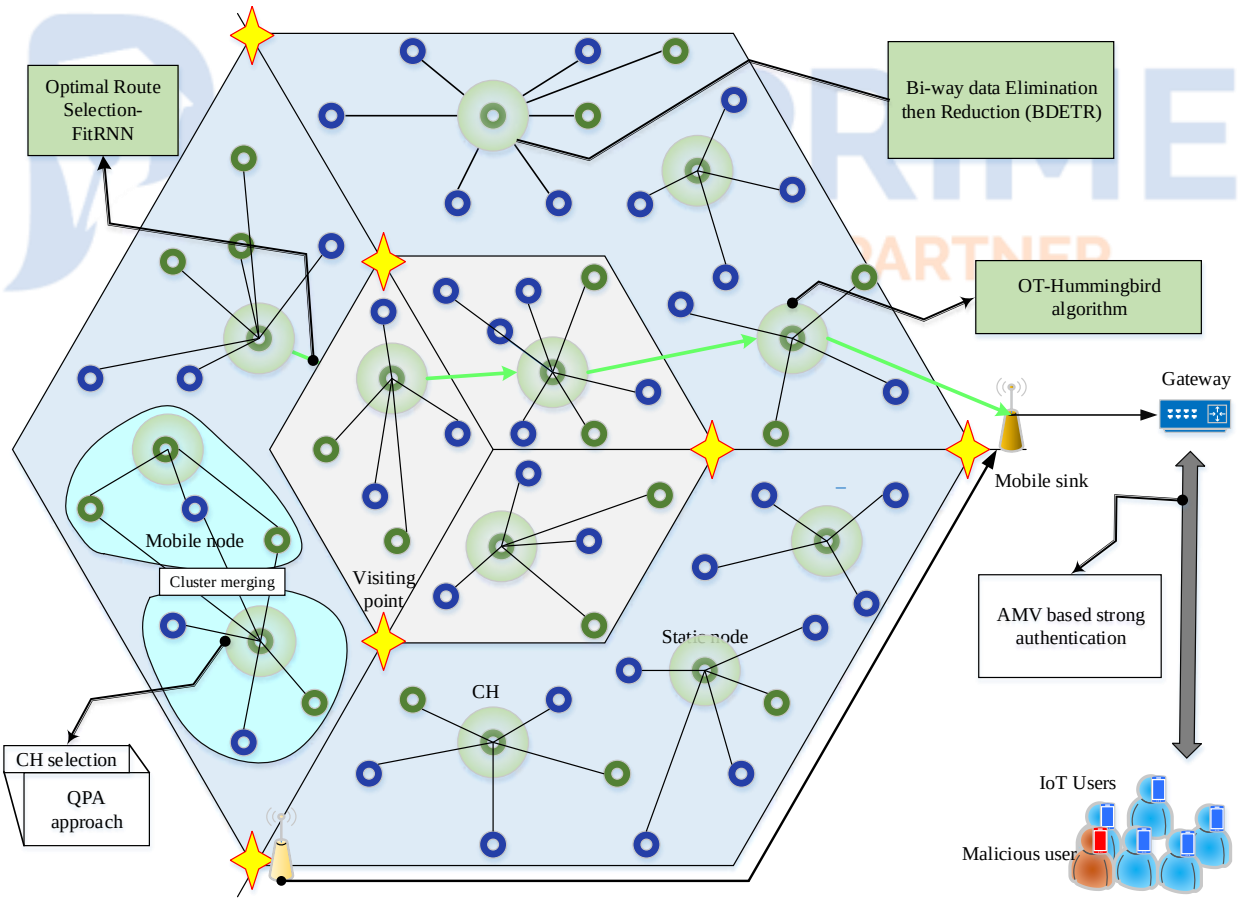
(v) IoT User Authentication

We also concentrate on user authentication to prevent the unauthorized user access. Initially, all legitimate users register their ID and password (PW) to gateway along with the secret key (SK). For further authentication, historical authentication information is utilized for every user which ensures high level security. We propose a novel **Apriori Multi-factor Validation (AMV)** algorithm. Herein apriori algorithm selects ideal attribute set for each user from the historical data and then authenticates the users at different levels. In first level, user ID is validated. In second level, user ID and PW is validated. In third level, user ID, PW, and SK are validated.

Proposed work ensures security as well as energy efficiency with necessary QoS. Finally, the proposed work is evaluated based on following metrics,

- ☑ Network lifetime
  - With respect to network size
  - With respect to packet size
- ☑ Throughput
  - With respect to network size
  - With respect to packet size
- ☑ Packet delivery ratio
  - With respect to network size
  - With respect to packet size
- ☑ Delay
- ☑ Encryption time

OVERALL NETWORK ARCHITECTURE



REFERENCE EXPLANATION

Paper 1

Title: Proposing a method to solve energy hole problem in wireless sensor networks

Concept

Wireless sensor network (WSN) comprises huge number of sensor devices and sink node. The sensor nodes are resource constrained which have limited computational, energy and power resources. Thus energy conservation is the major issue in WSN. This paper deals with energy hole problem which is introduced due to static sink node. In the presence of static sink node, the node that is presented nearer to the sink node consumes more energy for data transmission and aggregation from other node.

Paper 2

Title: Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN

Concept

This paper deals with cluster formation and cluster head selection in WSN to maximize the network lifetime. This work utilizes the hybrid optimization algorithm for optimal CH selection. The hybrid algorithm combines Fruitfly Optimization algorithm (FFOA) and Glowworm Swarm Optimization (GSO) algorithm. The CH is selected based on delay and energy consumption constraints.

Paper 3

Title: Models for integrating wireless sensor networks into the Internet of Things

Concept

Internet of Things (IoT) is an emerging paradigm that introduces many applications towards smarter world. This paper presents a model for IoT and WSN integration. In WSN IoT integration, scalability, interoperability, energy efficiency, and security are the major challenging issues. Integration of WSN and IoT can be applied over applications as smart city, healthcare, transportation, smart homes, and so on.

Paper 4

Title: IoT Security Techniques Based on Machine Learning

Concept

IoT comprises of millions of sensors, actuators, and other smart devices. Due to the variations in data and devices IoT is vulnerable to several attacks. In WSN-IoT environment, the sensed data can be sensitive or periodical data. In case of sensitive data it is necessary to provide required security level which can be ensured by security mechanisms. However, in general the data from IoT must be secured to protect the data from adversaries.

Paper 5

Title: Power Consumption and Calculation Requirement Analysis of AES for WSN IoT

Concept

This paper analyzes the power consumption of Advanced Encryption Standard (AES) in WSN assisted IoT. The objective this work is to detect the tradeoff between power consumption and required security level in WSN-IoT. AES is a symmetric key encryption algorithm which uses same key for encryption and decryption. In this paper, AES-CB, AES-CCM and AES-ECB algorithms are implemented and compared.

Paper 6

Title: Joint Balanced Routing and Energy Harvesting Strategy for Maximizing Network Lifetime in WSNs

Concept

This paper deals with joint routing and energy harvesting strategy to extend the network lifetime in WSN. In this work, the network is considered as a grid and split into multiple equal cells with the BS located in center of the network. For optimal routing, a shortest path tree with energy balance routing strategy (SPT-EBR) is proposed. Here optimal forwarder node is selected based on the link weight value and energy harvesting capability is incorporated.

Paper 7

Title: Novel Two-Fold Data Aggregation and MAC Scheduling to Support Energy Efficient Routing in Wireless Sensor Network

Concept

This paper presents a two-fold data aggregation scheme to achieve energy efficiency in WSN. In this paper, cluster formation is performed by voronoi diagram and then CH is selected based on weight value. To minimize energy consumption, authors have proposed cluster formation, optimal MAC scheduling, inter-cluster routing, and data aggregation. Particularly, mobile sink is utilized in this work to achieve better energy efficiency.

Paper 8

Title: Enhancement of RWSN Lifetime via Firework Clustering Algorithm Validated by ANN

Concept

This paper designs a rechargeable WSN to improve network lifetime. In this paper, the nodes are considered to be rechargeable by an external source. In this rechargeable WSN, the cluster formation is presented to improve the network lifetime. Firework optimization algorithm with adaptive transfer function (FWA-ATF) is proposed for optimal routing and cluster formation.

Paper 9

Title: A forwarding strategy based on ANFIS in internet-of-things-oriented wireless sensor network (WSN) using a novel fuzzy-based cluster head protocol

Concept

This paper presents a multi-sensor data fusion strategy by using artificial neural network and fuzzy inference systems (ANFIS). Here ANFIS Model is utilized for route selection and fuzzy based CH selection (FBCHS) algorithm is used for optimal CH selection. The main objective is to improve the network performance in IoT oriented WSN. Multiple parameters such as link bandwidth, centrality, latency, channel state information, SNR, and packet loss ratio are considered for route selection and ANFIS model is trained by MOPSO algorithm.

Problem

→ PSO algorithm has convergence issues which falls in local optima solutions. Thus ANFIS that is trained by PSO algorithm degrades the route selection efficiency.

Proposed Solution

→ FitDRN algorithm is presented for optimal route selection which improves the network perfromance

Paper 10

Title: Trust Based Scheme for IoT Enabled Wireless Sensor Networks

Concept

This papers deals with trust based data transmission in IoT enabled 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.

Problem

→ Trust computation needs the involvement of BS all time. Thus the complexity is high in this method.

Proposed Solution

→ Trust computation is performed based on direct and indirect trust values without involvement of sink node

Paper 11

Title: An adaptive fuzzy rule based energy efficient clustering and immune inspired routing protocol for WSN-assisted IoT system

Concept

This paper presents a adaptive fuzzy model for cluster formation in WSN assisted IoT systems. Here optimal CH selection is performed by Adaptive Fuzzy Multi-Criteria Decision Making (AF-MCDM) approach. AF-MCDM is designed with the combination of fuzzy AHP and fuzzy TOPSIS methods. Authors have highlighted that the proposed AF-MCDM based cluster formation improves energy efficiency.

Problems

→ Execution of fuzzy AHP and fuzzy TOPSIS algorithm for CH selection increases time consumption

→ It also increases complexity which results in energy consumption

Proposed Solutions

→ CH selection by QPA approach selects optimal cluster without increase in time consumption and complexity

Paper 12

Title: Enhanced Three Layer Hybrid Clustering Mechanism for Energy Efficient Routing in IoT

Concept

This paper proposes a hybrid hierarchical clustering approach (HHCA) for WSN assisted IoT networks. This HHCA is a distributed approach in which the nodes are organized in three layer architecture. The upper layer heads are selected by BS and are known as grid heads. The lower layer heads are selected by grid heads and known as CH. Grid heads are responsible to manage their CHs and CHs are responsible to manage their CMs.

Problem

→ 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.

Proposed Solution

→ We propose TC-Hex network architecture which mitigates the issue of energy consumption

Paper 13

Title: Survivable Path Routing in WSN for IoT applications

Concept

This paper concentrates on optimal routing in WSN for IoT applications. A survivable path based routing algorithm has been proposed for optimal route selection. Routing is performed based on multi criterion as: SNR of the link, survivability factor, and the congestion level. The survivability factor is defined 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.

Problems

→ Network management is not considered since the node located far away from sink experiences large energy consumption for data transmission

→ Security which is an important aspect of IoT is not considered in this work.

Proposed Solutions

→ Network is constructed as TC-Hex format and clustered to manage the network

→ Security is provisioned by OTH and AMV algorithm

Paper 14

Title: Logical Tree Based Secure Rekeying Management for Smart Devices Groups in IoT Enabled WSN

Concept

This paper presents 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.

Problem

→ Tree based keying method increases time consumption and complexity in the network

Proposed Solution

→ Proposed OTH algorithm is relatively lightweight

Paper 15

Title: Secure and Energy-Efficient Route Adjustment Model for Internet of Things

Concept

This paper presents a secure and energy efficient routing model for WSN assisted IoT. Here the network is designed with sensors, coordinators, mobile sink, IoT gateway, and IoT users. Initially, the IoT users are authenticated by bio-metric based authentication scheme. Then sensed data is aggregated by coordinator in threshold-TDMA (TTDMA) manner. To ensure data security, the sensed data is encrypted by RSA and authentication code is generated by SHA-1 algorithm. Optimal route selection is performed by type-2 fuzzy logic.

Problems

→ RSA requires large time and key size to ensure required security level. However, WSN involves resource constrained nodes which demands lightweight cryptography schemes.

→ Route selection by type-2 fuzzy and then reliability verification increases time consumption (in fuzzy logic 125 rules are executed for first level route selection).

Proposed Solutions

→ Proposed OTH algorithm is ultra-lightweight which ensures high security level

→ Optimal route selection is performed by FitDRN which processes all available routes in parallel

REFERENCES

SalehiPanahi, M., & Abbaszadeh, M. (2018). Proposing a method to solve energy hole problem in wireless sensor networks. Alexandria Engineering Journal, 57, 1585-1590.

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

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.

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.

Hung, C., & Hsu, W. (2018). Power Consumption and Calculation Requirement Analysis of AES for WSN IoT. Sensors.

Yu, C., Tala't, M., Chiu, C., & Huang, C.L. (2019). Joint Balanced Routing and Energy Harvesting Strategy for Maximizing Network Lifetime in WSNs. Energies, 12.

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.

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.

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.

Ali, B.A., Abdulsalam, H.M., & AlGhemlas, A. (2018). Trust Based Scheme for IoT Enabled Wireless Sensor Networks. Wireless Personal Communications, 99, 1061-1080.

Preeth, S., Dhanalakshmi, R., Kumar, R.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.

Ullah, M.F., Imtiaz, J., & Maqbool, K.Q. (2019). Enhanced Three Layer Hybrid Clustering Mechanism for Energy Efficient Routing in IoT. Sensors.

Elappila, M., Chinara, S., & Parhi, D.R. (2018). Survivable Path Routing in WSN for IoT applications. Pervasive and Mobile Computing, 43, 49-63.

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.

Jain, J.K. (2019). Secure and Energy-Efficient Route Adjustment Model for Internet of Things. Wireless Personal Communications, 1-25.

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.

Tabassum, A., Sadaf, S., Sinha, D., & Das, A.K. (2020). Secure Anti-Void Energy-Efficient Routing (SAVEER) Protocol for WSN-Based IoT Network.

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 Comp. Syst., 81, 372-381.

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.

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.