AI-enabled distributed energy conservative model for SDN based mobile IoT devices

Khalid Haseeb[1], Naveed Islam[1], Imran Ahmed[2,3], Mohammad Mehedi Hassan[4], Gwanggil Jeon[5]

[1] Department of Computer Science, Islamia College Peshawar, Peshawar, Pakistan;
e-mail: khalid.haseeb@icp.edu.pk, naveed.islam@icp.edu.pk
[2] School of Computing and Information Science, Anglia Ruskin University, Cambridge, UK;
e-mail: imran.ahmed@aru.ac.uk
[3] Institute of Management Sciences, Peshawar, Pakistan; e-mail: imran.ahmed@imsciences.edu.pk
[4] Information Systems Department, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia; e-mail: mmhassan@ksu.edu.sa
[5] Department of Embedded Systems Engineering, Incheon National University, Incheon, Korea;
e-mail: gjeon@inu.ac.kr

Abstract: The Internet of things (IoT) is an emerging technology for many smart applications due to efficient resource utilization, scalability, and fast interaction with the physical world. Software-defined network (SDN), on the other hand, provides dynamic services for controlling and managing real-time systems. However, collected data is sent to a central location, which requires balancing energy resources with redundant channels to maximize the availability of smart functions. Furthermore, the IoT network faces numerous security vulnerabilities as a result of its open communication space, including fraudulent messages and privacy concerns. Thus, this paper presents a distributed and artificial intelligence-based energy-efficient model for IoT-SDN architecture, which aims to improve data aggregation and power distribution. It also provides security and authentication for smart communication systems. Firstly, the proposed model introduces the heuristic evaluation using artificial intelligence and decreases the power consumption for sensor nodes in a real-time system. Moreover, optimizes the paradigm of distributed processing and efficiently increases the green energy technology with nominal management costs using the mobile edges. Secondly, the aggregated data of the environment is secured using a centralized controller to attain the most trustworthy data availability. The experimental results show a comparative analysis of the proposed model in terms of energy efficiency, packet drop ratio, and waiting time by 22%, 23%, 40%, and 49% as compared to existing studies.

Keywords: energy management; artificial intelligence, internet of things, smart systems, software-defined network

1. List of abbreviations

IoT	Internet of Things
SDN	Software-Defined Network
WSN	Wireless Sensor Network
BS	Base station
AI	Artificial Intelligence
TDR	Traffic-Differentiated Routing
SDDCs	Software-Defined Data Centers
VM	Virtual Machine
DAI	Distributed Artificial Intelligence
P2P	Peer-to-peer

2. Introduction

Wireless sensor networks (WSNs) and smart things are widely used for remote monitoring and tracking scenarios due to their exceptional advantages in terms of versatility, durability, and cost-effectiveness [1-4]. Many crucial real-time applications, such as smart agriculture, intelligent transportation, etc have limited resource budgets and strict security requirements. IoT networks connect a variety of heterogeneous gadgets with the capability of sensing data and assisting societies [5-7]. Due to the limited capabilities of low-powered devices, the majority of IoT solutions rely on artificial intelligence. WSN's compatibility with developing technologies allows it to support a wide range of mobile networks and collect data from a variety of sources [8, 9]. Such data is delivered to connected systems for further analysis. Emerging technologies such as artificial intelligence and machine learning are introducing complex algorithms for protecting IoT networks and smart systems by observing their local and global features [10-12]. Such techniques are frequently used in communication systems to improve their performance and efficiency. Moreover, SDN is utilized for the design and management of network configurations. It simplifies data gathering and processing for resource-constrained devices and provides intelligent behavior. SDN provides a bridge among IoT devices and communication systems with dynamic characteristics [13-15]. However, most SDN-based WSN solutions are insufficient to handle all types of smart operations with precision, speed, and security. Furthermore, because smart devices and sensors collect a large amount of data from many sources and physical objects, therefore optimal data processing and analysis methods are required [16, 17]. Presently, the internet and mobile communication networks evolve rapidly as wireless platforms and have complicated architecture, diverse devices, resources, and highly dynamic network forms. Many IoT-based smart cities often use sensor nodes for data gathering and relaying to remote users via autonomous structures. However, because sensors are used in unpredictable contexts, optimizing system resources and protecting real-time data from many security incidents significant research challenges for IoT systems [18-20]. As a result, with the integration of an SDN controller, this article offered an artificial intelligence-based distributed IoT architecture with energy savings and data security. The major objectives of the proposed model are as follows.

i. Proposing an AI-based approach for generating smart system routing strategies with effective energy management and power distribution.
ii. It provides a scalable solution that takes controllers into account and keeps track of data flow statistics to identify congested and faulty communications.
iii. Furthermore, security analysis for open communication systems has been adapted to give trustworthiness and assistance to privacy-preserving data aggregation.
iv. The simulation-based experiments illustrate that the proposed model significantly improved energy management and data availability.

The rest of the research paper is organized in the following sections. Section 3 presents the discussion of existing schemes. Section 4 explains the proposed model in detail. Section 5 discusses the experimental results. In the end, Section 6 concludes this research study with future work.

3. Related Work

WSNs and IoT technologies have been widely deployed in a wide range of smart applications, including healthcare, agriculture, grid computing, etc. Such applications make it easier for connected devices to obtain required data without human interaction [21-23]. The primary purpose of the IoT-based WSN

is to intelligently monitor, process, and analyze the embedded objects and share the data over the Internet. The connected objects form a distributed network system to balance a load of communication services with minimum overheads. However, due to tight constraints on such IoT devices, especially in terms of energy, memory, and transmission power, most of the solutions are not able to produce desirable outcomes with high performance. As a result, minimizing the enormous number of network challenges related to connectivity, reliability, data security, and trust are important aspects [24-26]. The authors [27] discuss two aspects of SDN-based load-balanced opportunistic routing for duty-cycled WSNs. In the control plane, the candidates are first computed and controlled. Second, the metric used to prioritize the candidates takes into account the average of three distributions: transmission distance, predicted number of hops, and residual energy, such that more traffic is directed through the nodes with higher priority. In comparison to the benchmarks, simulation results show that the proposed protocol considerably improves network lifetime, routing efficiency, energy usage, sender waiting time, and duplicate packets.

A novel SDN architecture is proposed in [28], which consists of several components such as topology, the base station (BS) and controller discovery, link, and virtual routing, to lower load distribution and extend lifetime. As a result, a new load-balancing routing strategy based on SDN and virtualization is proposed. The used OpenFlow protocol may calculate load-balancing routing for each flow in various IoT applications by directly monitoring link load statistics and network running state. Various routes can be used to direct flows from various resource applications to a BS. In implementations, it was noticed that communication of network status and other critical information is also reduced by the proposed solution. The authors [29] developed a unique clustering FASNET architecture with SDN cluster controllers and a collaborative controller to enable hierarchical administration and unified dispatch. It also demonstrated a centralized traffic-differentiated routing (TDR) implementation in each cluster based on the designed architecture, to meet the specific QoS requirements of delay-sensitive and reliability-required services. Different weights are assigned to the various flows based on their sensitivity to delays. Furthermore, it provides TDR with a transmission reliability prediction model that considers both link availability and node forwarding ability. The results of simulations proven that the proposed TDR has good performance as compared to other techniques.

In [30] authors used software-defined data centers (SDDCs) to reduce energy demand. These centers directly customize logical computation, network routers, and storage resources in real-time to meet the needs of the workload. For heterogeneous computing infrastructures, authors showed how to 1) construct a consolidated SDDC-based model to simultaneously optimize the process of virtual machine (VM) deployment and network bandwidth allocation; 2) frame a multi-objective optimization problem to determine the ideal energy allocation for critical and noncritical applications; and 3) It proposes a poor initial fit decreasing method. To reduce energy usage in industrial 6G operations, the authors [31] proposed a huge IoT system with a dynamic network model. They employed distributed artificial intelligence (DAI) to cluster sensor nodes and locate the primary node. Their approach evaluated mutual cluster correlation to optimize resources for individual nodes within each cluster. The simulation results demonstrated that the suggested strategy lowered resource loss caused by redundant data, increased network energy savings, and preserved data. With blockchain and software-defined networking, authors [32] addressed security issues successfully. They demonstrated a blockchain-enabled SDN controller cluster architecture for IoT networks using a novel routing protocol

for both safety and energy efficiency. For peer-to-peer (P2P) communication between IoT devices and SDN controllers, the design uses public and private blockchains. Moreover, less latency and energy usage are shown by the empirical evidence of the cluster-based routing protocol. We highlight the following developments and advancements based on the related studies.

- Sensor technologies are commonly used to automate communication systems in real-time applications such as intelligent transportation, healthcare, smart grid, etc.
- The developed infrastructure using the IoT-based paradigm not only offers scalable and efficient relay systems but also supports collaborative processing.
- However, most of the existing techniques imposed communication overheads, increased power consumption, and security risks. As a result, for trustworthy network availability with an efficient network system, the achievement of data privacy and integrity should be considered.
- Furthermore, to improve the green communication of smart cities, the routing paths should be more dynamic in terms of intelligence and processing power.

As a result, this study offered a distributed and AI-supported model for IoT-based SDN architecture to achieve a high-quality communication system with energy-efficient and secure collaborative processing.

4. Proposed distributed and artificial intelligence-oriented secured model

This section explains the detail of the proposed model. Figure.1 illustrates the designed four components of the proposed model: routing evaluation with AI methods, mutual authentication, formation of routing states, and data availability with trust. By exploring local attributes, the proposed model utilizes the AI technique for the selection of appropriate routing nodes, and after their trusted connection they can interchange the data. Moreover, the routing tables are updating their entries with the intelligence of the proposed model. In the end, towards network users, only consistent and fully trusted data is forwarded. Initially, the smart system provides the quality assurance data transmission system with efficient energy management among distributed devices. Also, it lowers the management load and cost on the communicating devices with the integration of the artificial intelligence approach at network edges. In the routing process, the proposed model also creates a redundant path by exploring the congestion window and improves the response time of the communication system under critical conditions. Moreover, the SDN controller filters the malicious traffic from the data flow plane, and only authorized data is allowed to cross the network devices. The mobile edges evaluate the history and assigned a priority to the established routes. Accordingly, the route with low priority eliminates from the routing table, and updated information is continuously reflected to increase trust and data availability. The working flow of the proposed model is divided into the following two subsections.

A. Quality assurance data transmission system with efficient energy management

Before discussing this section, let's go through the following assumptions. We consider sensor nodes to be static and can sense the data of the environment within the preset radius. Each sensor has enough memory to store its neighbor list in a form of a routing table and reform it whenever any change occurs in its proximity. Sink nodes are mobile and offer services as edge devices to the SDN controller. The SDN controller operates in a centralized manner and controls the data plan of the distributed sensors with its intelligent and high computing capabilities. IoT sensors are distributed randomly in the environment and are structured in the form of Graph $G(E,V)$. If $n1, n2 \in V(G)$, then $n1 \rightarrow n2$ means that

both are joined to V by edge E. In the beginning, the proposed model forms the initial routing table for each node i. Accordingly, a set of routes R_i are extracted from the routing table as given in equation 1.

$$R_i = \sum_{i=0}^{n} r_i \quad (1)$$

The individual formed a route r_i is on the greedy principle and indicates the pair of consecutive nodes without any looping. Afterward, the proposed model uses an AI-assisted depth-first search (DFS) approach to find the spanning trees and generated subgraph G'.

Moreover, neighboring states are identified using heuristic cost $H(c)$ by extracting the nodes' information from G'. The decision of $H(c)$ is based on multi-criteria and offers the optimal choices to lead the sensor-edge communication system. The mobile edges periodically announced their newest positions, accordingly, sensors updated their routing table by incorporating received information. Let us consider that the transmission range of sensor i is denoted by t_i. If the distance between node and sink $(i, sink)$ falls between t_i, the data is forwarded immediately. Otherwise, the proposed model utilizes the $H(c)$ value for identifying the appropriate neighboring node. Equation 2 defined the computation of $H(c)$ value based on distance d_i and congestion window C_w.

$$H(c) = min\,(d_i + C_w) \quad (2)$$

In equation 2, d_i denotes the distance of source node towards extracted neighboring nodes from subgraph G', whereas C_w is congestion window. The source node i maintains the record of transmitted beacon packets P_t and round trip time RTT. Also, available data bandwidth α is incorporated in the computation of C_w value as defined in equation 3.

$$C_w = \frac{P_t}{RTT} + \frac{l_b}{\alpha} \quad (3)$$

where l_b denotes the bandwidth size of the link between the source node i to the neighbor j. The depth-first algorithm utilizes the computed $H(c)$ value and support to identify the optimal solution for the delivery of data towards the mobile sink. Firstly, it uses the subgraph G' to identify the set of nodes (S, N, G) in the initial routes, whereas S is the source node, N is the set of neighbors and G is the goal state. Each node maintains information in its routing table about visited vertices and keeps its order based on minimum $H(c)$ value.

Afterward, the edge devices are communicating with the SDN controller to offer low latency services for the IoT system. Edge devices continuously update the SDN controller about sensors' data flow and accordingly, the SDN controller keeps the latest information in its global table about routing topology. It manages the re-construction of routing paths using intelligent edges and exploring packets receiving information. If the packet drop ratio exceeds a certain threshold, the SDN controller sends a signal to the sink node to initiate the identification of an alternative route and marked it as the redundant route. The redundant route offers the service as a backup when the current route cannot be able to tackle the data flow of sensors' data.

B. Trusted data availability using SDN controller

The SDN controller also provides an ease for connected devices to obtain the IoT data with a high degree of trust and security against anonymous attacks. In the proposed model, the security phase is accomplished using two procedures. The first is executed between the network edges and sensors by utilizing a threshold scheme, and the second process is executed between network edges and the SDN controller by exploiting the RSA algorithm [33]. SDN controller performs high-cost computing to reduce the communication overheads for sensors, as a result, it offers energy-efficient and smart network management. Moreover, in the proposed model, the SDN controller provides the network intelligence in a centralized manner and keeps the global view for the entire IoT devices. In the proposed model, network edges are considered as a trusted party and compute secret shares k_i from initial share Y [34], as defined in equation 4.

$$s \rightarrow n_i: k_i, 1 \leq i \leq t \tag{4}$$

To secure transmission and reconstruction of the secret key, the following two conditions must be satisfied among edges and sensors. (i) any combination of t or a higher number of subkeys may easily rebuild the secret key K. (ii) less than t or fewer subkeys can not be cable to rebuild the secret key K. After securely transmission of secret key among network edges and sensors, both can utilize the encryption function e to attain data privacy for m_i , as defined using Xor operation in equation 5.

$$e = m_i \oplus k_i \tag{5}$$

To transmit the encrypted data from edge device edi towards the SDN controller S, the proposed model computes the path p with the fewest edges. If the edi is not directly connected with the S then it explores the distance threshold d to identify the nearest edge edj, as given in equation 6.

$$if\ p^{edi-edj}(len) \leq d\ then\ route\_data \tag{6}$$

In the last phase, the proposed model support trusted communication between mobile edges and the SDN controller by utilizing symmetric digital certificates. The mobile edges firstly make contact with the SDN controller for the issuance of secret keys. Upon receiving the requests from edges, the SDN controller verifies their identities from the global table, and with successful verification, the SDN controller initiates the process of issuing digital certificates to ensure mutual trust among edges, as given below.

$$req^{ed(i)-S} = ID_i, E_{is}(ID_j, D) \tag{7}$$

$$res^{S-ed(i)} = E_{js}(ID_i, D) \tag{8}$$

In equations 7 and 8, E is a symmetric algorithm for encryption, D is the data message, E_{is}, E_{js} are the shared key of edge i, j, and SDN controller. After obtaining the certificate from the SDN controller, edge i returns it to edge j for authentication, as given in equation 9.

$$ed(i) \rightarrow ed(j) : E_{js}(ID_i, D) \tag{9}$$

Figures 2(a) and 2(b) demonstrate the flowcharts of the proposed model. It was developed based on two main components. Firstly, using DFS evaluation spanning trees are generated, and compute the heuristic cost for extracting the forwarders' information. The cost should be minimum in terms of both the distance and congestion. The mobile edges not only support IoT data with low latency but also control the data plane with collaborative processing of the SDN controller. Secondly, the proposed model increases trust on two levels. It also secures the sensor's data from malicious traffic and offers reliable and secure routes with the support of edges by using a threshold sharing scheme. The symmetric digital certificates give the high computing solution to upper devices and maintain the data authenticity with privacy.

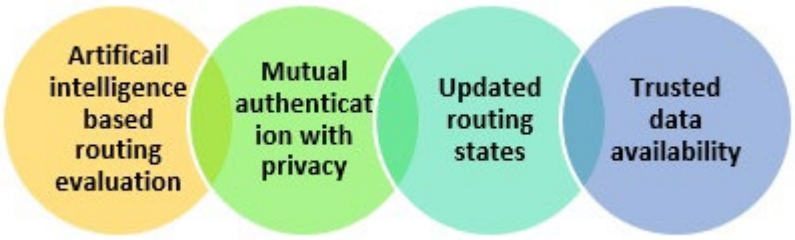
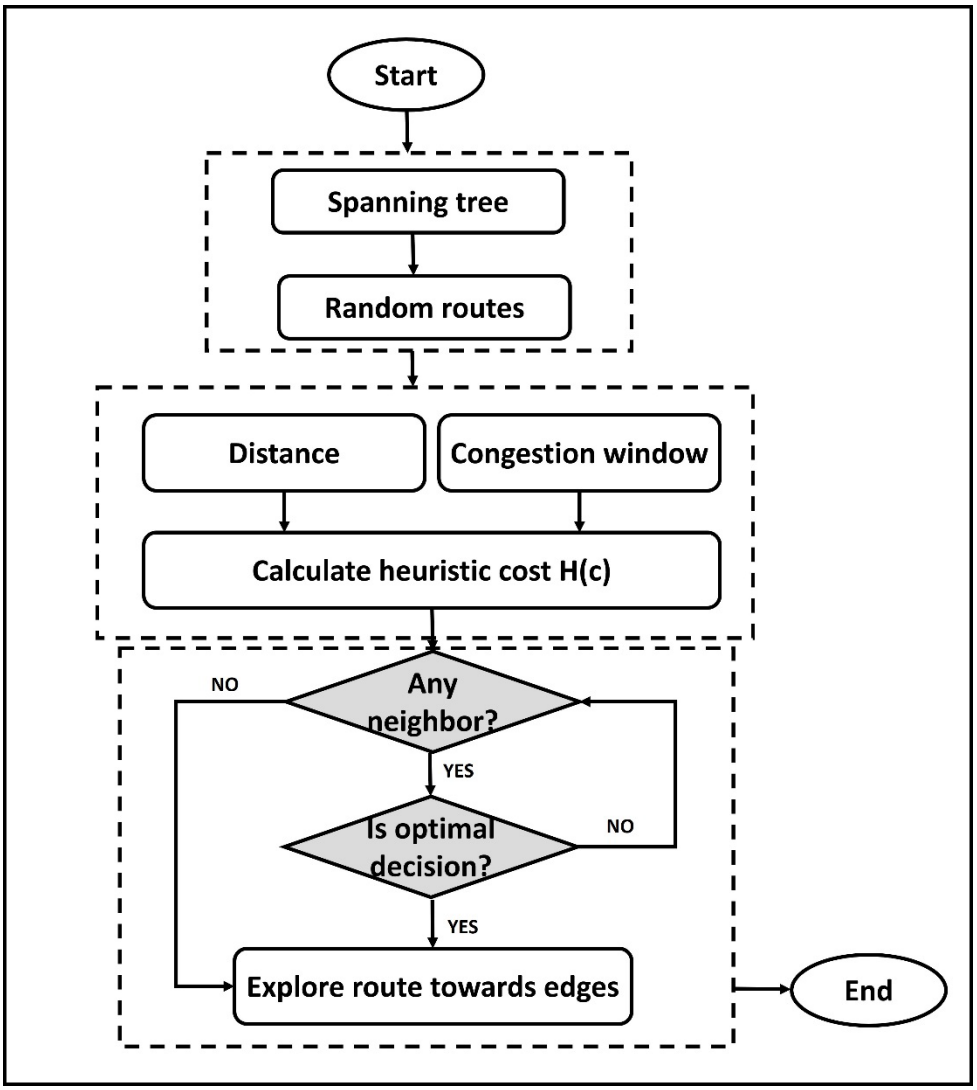
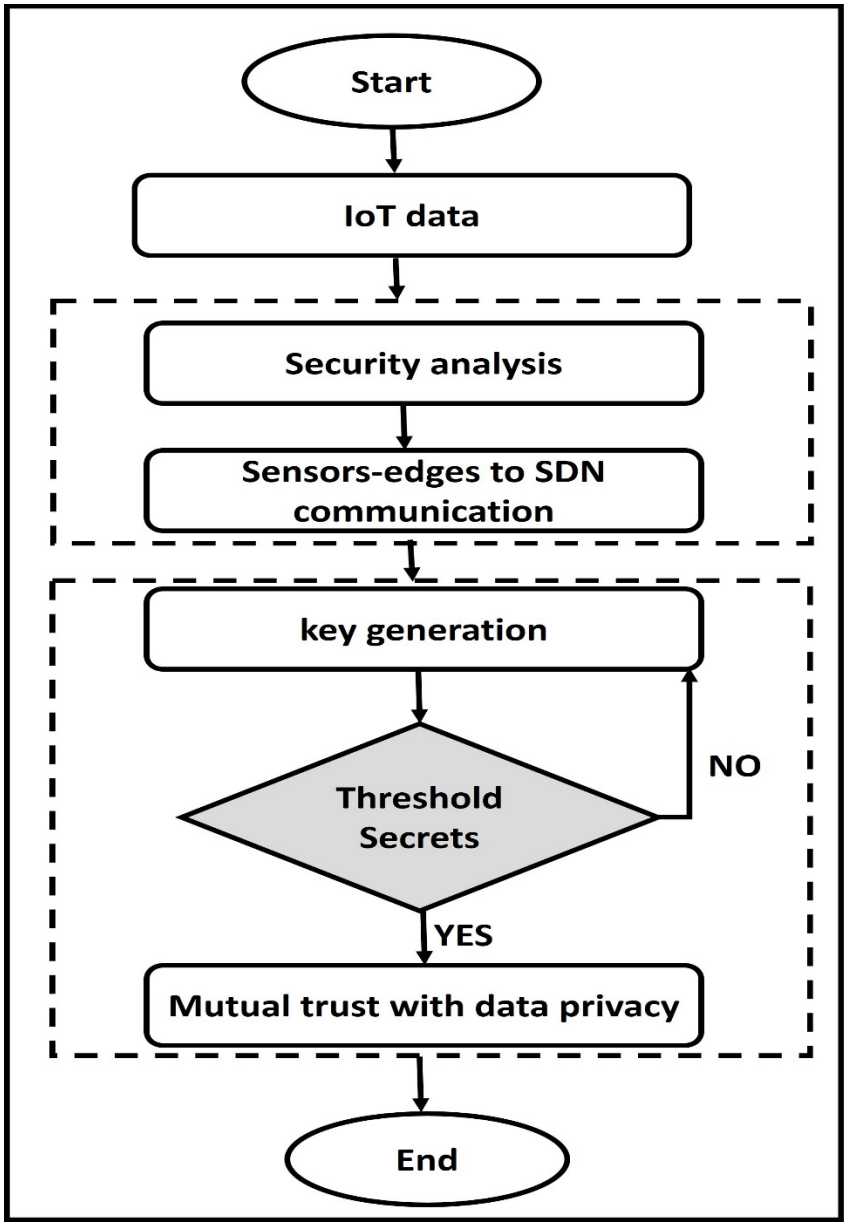


Figure 1. Developed components of the proposed model



(a) Formulation of data flow routes with mobile edges using heuristics computing



(b) Security for a smart communication system with edges-SDN

Figure 2. The flowchart of the proposed distributed and AI-based energy-efficient model for IoT-SDN architecture

5. Simulation environment

This section presents the experimental environment and discussion on results. The performance of the proposed method is computed and verified with simulation-based results in the comparison of existing work. IoT system is comprised of random deployment of sensors in the field of 300m × 300m. Sink nodes are mobile and considered edge devices. Initially, sensors have fixed with 2J of energy resource. The packet size is 20bytes and the transmission range is set to 5m. We deployed an SDN controller with varying malicious devices. The proposed model makes use of the Open Network Operating System (ONOS) [35], an open-source controller. The number of sensors are varying from 50 to 250. The simulations are run for a period of 10 to 50 mins. Table 1 defines the simulation metrics for the analysis of the proposed model against related work.

Table 1 Simulation parameters

Parameter	Value
Sensors	50-250
Deployment	Random
Sink nodes	5
Network diameter	300m x 300m
Transmission range	5m
Initial energy	2J
Packet size	20 bytes
Malicious devices	3-15
Time intervals	10-50 mins

A. Security analysis

In this section, we present the performance results of the proposed model with existing solutions. Table 2 shows numerous security concerns as well as proposed countermeasures in terms of authentication, data privacy, malicious node detection, and mutual trust. Proposed security procedures exploit the unique ID and session keys to ensure the device's authentication. The proposed security strategy uses the encryption keys to secure data privacy and generates encrypted code by performing a Xor operation on data bits. Additionally, it provides an efficient method of securing edge-SDN communication by exploring digital certificates and mutually assured trust. To detect the malicious nodes, the proposed solution verified the secret shares that are generated by network edges. In case, the invalid secret share is found with any nodes, then such node is marked as faulty and unauthentic.

Table 2. Security analysis

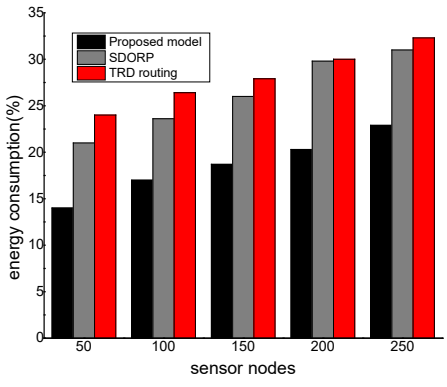
Security Attacks	**Procedures**
Device authentication	Unique ID Session keys
Sensors to edges security	Encryption keys
Edges to SDN security	Digital certificates
Privacy	Xor between messages and keys
Edges verification	Using SDN global table
Indirect routes	Computing distance threshold
Identification of malicious nodes	Invalid secret share
Mutual trust	Exchanging verified digital certificates

B. Results and Discussion

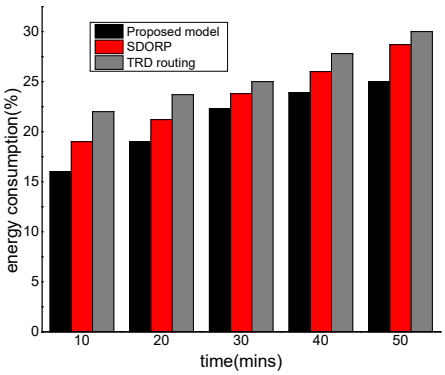
We evaluated the performance of the proposed model against the existing solution in terms of energy consumption. Figs. 3(a) and 3(b) illustrate the evaluation of the proposed model and existing solutions and it is observed to improve the efficiency of energy utilization of the proposed model by an average of 28% and 15%. It was seen that with increasing the number of nodes the rate of energy consumption is also increasing. However, the proposed model offers an intelligent energy solution using a cost heuristic function using the DFS algorithm and re-adjusting the routes for the network system. Due to the least control messages and retransmission, the proposed model balances the energy consumption

of the IoT system and increases the overall lifetime. Moreover, routing states are only updated whenever the SDN controller realizes the uncertain situation of the network. Accordingly, the proposed model supports the efficient power distribution system using mobile edges with manageable communication costs. We evaluated the performance of the proposed model against the existing solution in terms of end-to-end delay. The evaluation of the proposed model and existing solutions is shown in Figures 4(a) and 4(b), and it was discovered that the proposed model reduces waiting time by 49% and 26%, respectively. It's because mobile edges are integrated with SDN controllers and improve delivery performance. In addition, by re-evaluating the routing nodes, the mobile devices reduce the reaction time for gathering data from the IoT system and efficiently tackle wireless channels. Furthermore, the security solution prevents malicious devices from sending false diverting messages and lowers non-authentic data traffic across communication networks.

Accordingly, the proposed model increases the response time for the most critical operation with a nominal delay rate. Figs. 5(a) and 5(b) illustrate the performance evaluation of the proposed model against the existing solution in terms of network throughput. It is seen that the proposed model significantly increases network throughput under varying sensors and time intervals by 15% and 18%. This is due to the proposed model making use of an SDN controller for the monitoring of the IoT system and efficiently managing the energy distribution among forwarders. Whenever any communication channel links are identified by computing the packets and congestion window information, the proposed model re-evaluates the routing states. The routing states are re-computed based on certain criteria with the support of artificial intelligence techniques. The lightweight computing functions not only reduce the sensors' overhead but also offer high data reception rate using the intelligence of mobile edges. Figs. 6(a) and 6(b) depict the performance evaluation of the proposed model for varying numbers of sensors and varying time intervals in terms of packet drop ratio. It was observed that the proposed model significantly reduces the malicious traffic detection rate under the presence of faulty devices by 44% and 37%. It is due to mutual authentication of the devices using a threshold sharing scheme and secret keys. Also, the digital certificates and secret keys support the timely verification of malicious devices and attain the data availability of the smart network communication system. Moreover, the mobile edges are more robust and act as a supervisor for sensor data coming from the IoT network, after proper authentication the gathered data is forwarded to the application user with the intelligence of the SDN controller.

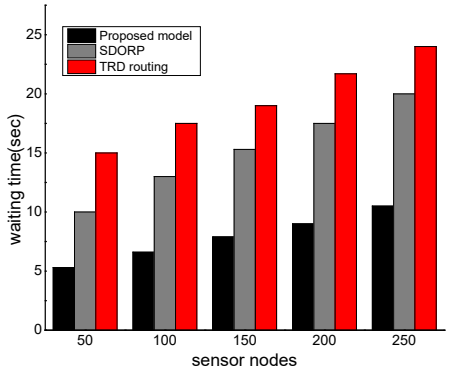


(a)

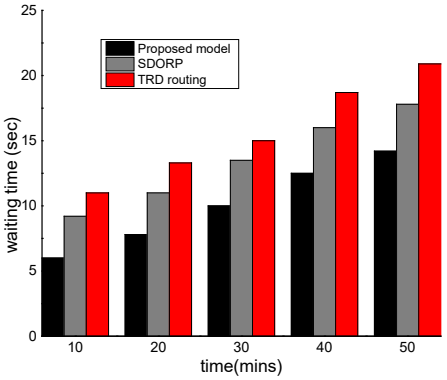


(b)

Figure 3. (a) energy consumption with varying sensors (b) energy consumption with varying time intervals

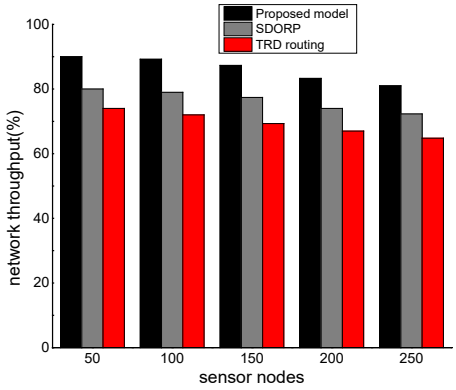


(a)

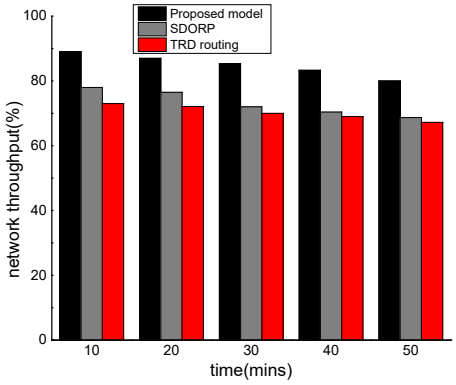


(b)

Figure 4. (a) waiting time with varying nodes (b) waiting time with varying time intervals

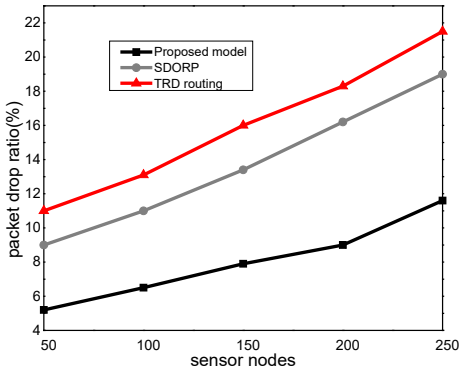


(a)

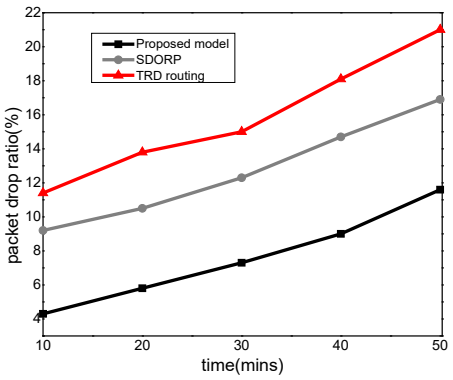


(b)

Figure 5. (a) network throughput with varying nodes (b) network throughput with varying time intervals



(a)



(b)

Figure 6. (a) packet drop ratio with varying nodes (b) packet drop ratio with varying time intervals

6. Conclusion

In this paper, we present a distributed and AI-based energy-efficient model for mobile IoT devices using SDN. Unlike most previous work, our proposed solution provides improved delay performance and a successful transmission rate with secured routing. Furthermore, even in the presence of malicious actions, network devices use secret sharing for mutual authentication and offer a secure environment. It enables real-time data collection and processing for smart objects, resulting in a green and efficient system. The proposed model, on the other hand, is unable to sustain the efficacy of nodes' information when their locations change frequently. As a result, it generated a large number of route request packets from the source node, causing the network unbalanced in terms of traffic flow. In the future, we intend to evaluate the efficacy of the proposed model in terms of both internal and external network threats. Moreover, we aim to incorporate cloud services for enhancing data computation and large-scale data storage.

Acknowledgment

This work was supported by King Saud University, Riyadh, Saudi Arabia, under Researchers Supporting Project number RSP-2021/18.

References

1. Jia, X.-C., *Resource-efficient and secure distributed state estimation over wireless sensor networks: a survey.* International Journal of Systems Science, 2021. **52**(16): p. 3368-3389.
2. Liang, Q., T.S. Durrani, J. Koh, J. Liang, Y. Li, and X. Wang, *IEEE Access Special Section Editorial: Mission-Critical Sensors and Sensor Networks (MC-SSN).* IEEE Access, 2021. **9**: p. 49457-49466.
3. Haseeb, K., S. Lee, and G. Jeon, *EBDS: An energy-efficient big data-based secure framework using Internet of Things for green environment.* Environmental Technology & Innovation, 2020. **20**: p. 101129.
4. Landaluce, H., L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, *A review of IoT sensing applications and challenges using RFID and wireless sensor networks.* Sensors, 2020. **20**(9): p. 2495.
5. Haseeb, K., N. Islam, A. Almogren, and I.U. Din, *Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things.* IEEE Access, 2019. **7**: p. 185496-185505.

6. Vardhana, M., N. Arunkumar, E. Abdulhay, and P. Vishnuprasad, *Iot based real time trafic control using cloud computing.* Cluster Computing, 2019. **22**(1): p. 2495-2504.
7. Gao, H., B. Qiu, R.J.D. Barroso, W. Hussain, Y. Xu, and X. Wang, *TSMAE: a novel anomaly detection approach for internet of things time series data using memory-augmented autoencoder.* IEEE Transactions on Network Science and Engineering, 2022.
8. Gupta, B.B. and M. Quamara, *An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols.* Concurrency and Computation: Practice and Experience, 2020. **32**(21): p. e4946.
9. Shahraki, A., A. Taherkordi, Ø. Haugen, and F. Eliassen, *A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms.* IEEE Transactions on Network and Service Management, 2020. **18**(2): p. 2242-2274.
10. Zhang, J., *Real-time detection of energy consumption of IoT network nodes based on artificial intelligence.* Computer Communications, 2020. **153**: p. 188-195.
11. Goswami, P., A. Mukherjee, R. Hazra, L. Yang, U. Ghosh, Y. Qi, and H. Wang, *AI based energy efficient routing protocol for intelligent transportation system.* IEEE Transactions on Intelligent Transportation Systems, 2021.
12. Gao, H., J. Xiao, Y. Yin, T. Liu, and J. Shi, *A Mutually Supervised Graph Attention Network for Few-Shot Segmentation: The Perspective of Fully Utilizing Limited Samples.* IEEE Transactions on Neural Networks and Learning Systems, 2022.
13. Abbas, S., N. Javaid, A. Almogren, S.M. Gulfam, A. Ahmed, and A. Radwan, *Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things.* IEEE Access, 2021. **9**: p. 139739-139754.
14. Shafique, A., G. Cao, M. Aslam, M. Asad, and D. Ye, *Application-aware SDN-based iterative reconfigurable routing protocol for Internet of Things (IoT).* Sensors, 2020. **20**(12): p. 3521.
15. Sayeed, M.A., R. Kumar, and V. Sharma, *Efficient data management and control over WSNs using SDN - enabled aerial networks.* International Journal of Communication Systems, 2020. **33**(1): p. e4170.
16. Mahdavinejad, M.S., M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A.P. Sheth, *Machine learning for Internet of Things data analysis: A survey.* Digital Communications and Networks, 2018. **4**(3): p. 161-175.
17. Ahmad, A., M. Khan, A. Paul, S. Din, M.M. Rathore, G. Jeon, and G.S. Choi, *Toward modeling and optimization of features selection in Big Data based social Internet of Things.* Future Generation Computer Systems, 2018. **82**: p. 715-726.
18. She, W., Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, *Blockchain trust model for malicious node detection in wireless sensor networks.* IEEE Access, 2019. **7**: p. 38947-38956.
19. Elhoseny, M., K. Haseeb, A.A. Shah, I. Ahmad, Z. Jan, and M. Alghamdi, *IoT Solution for AI-Enabled PRIVACY-PREServing with Big Data Transferring: An Application for Healthcare Using Blockchain.* Energies, 2021. **14**(17): p. 5364.
20. Gao, H., W. Huang, T. Liu, Y. Yin, and Y. Li, *PPO2: Location Privacy-Oriented Task Offloading to Edge Computing Using Reinforcement Learning for Intelligent Autonomous Transport Systems.* IEEE Transactions on Intelligent Transportation Systems, 2022.
21. Kumar, A., M. Zhao, K.-J. Wong, Y.L. Guan, and P.H.J. Chong, *A comprehensive study of IoT and WSN MAC protocols: Research issues, challenges and opportunities.* IEEE Access, 2018. **6**: p. 76228-76262.
22. Ullah, A., G. Said, M. Sher, and H. Ning, *Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN.* Peer-to-Peer Networking and Applications, 2020. **13**(1): p. 163-174.

23. Marjani, M., F. Nasaruddin, A. Gani, A. Karim, I.A.T. Hashem, A. Siddiqa, and I. Yaqoob, *Big IoT data analytics: architecture, opportunities, and open research challenges.* ieee access, 2017. **5**: p. 5247-5261.
24. Haseeb, K., N. Islam, A. Almogren, I.U. Din, H.N. Almajed, and N. Guizani, *Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs.* IEEE Access, 2019. **7**: p. 79980-79988.
25. Shahid, H., H. Ashraf, H. Javed, M. Humayun, N. Jhanjhi, and M.A. AlZain, *Energy optimised security against wormhole attack in IoT-based wireless sensor networks.* CMC-Computers Materials & Continua, 2021. **68**(2): p. 1966-1980.
26. Gao, H., C. Liu, Y. Yin, Y. Xu, and Y. Li, *A hybrid approach to trust node assessment and management for vanets cooperative data communication: Historical interaction perspective.* IEEE Transactions on Intelligent Transportation Systems, 2021.
27. Qaisar, M.U.F., X. Wang, A. Hawbani, L. Zhao, A.Y. Al-Dubai, and O. Busaileh, *SDORP: SDN based Opportunistic Routing for Asynchronous Wireless Sensor Networks.* IEEE Transactions on Mobile Computing, 2022.
28. Hajian, E., M.R. Khayyambashi, and N. Movahhedinia, *A Mechanism for Load Balancing Routing and Virtualization Based on SDWSN for IoT Applications.* IEEE Access, 2022. **10**: p. 37457-37476.
29. Qi, W., Q. Song, X. Kong, and L. Guo, *A traffic-differentiated routing algorithm in Flying Ad Hoc Sensor Networks with SDN cluster controllers.* Journal of the Franklin Institute, 2019. **356**(2): p. 766-790.
30. Kaur, K., S. Garg, G. Kaddoum, E. Bou-Harb, and K.-K.R. Choo, *A big data-enabled consolidated framework for energy efficient software defined data centers in IoT setups.* IEEE Transactions on Industrial Informatics, 2019. **16**(4): p. 2687-2697.
31. Mukherjee, A., P. Goswami, M.A. Khan, L. Manman, L. Yang, and P. Pillai, *Energy-efficient resource allocation strategy in massive IoT for industrial 6G applications.* IEEE Internet of Things Journal, 2020. **8**(7): p. 5194-5201.
32. Arshad, R., S. Zahoor, M.A. Shah, A. Wahid, and H. Yu, *Green IoT: An investigation on energy saving practices for 2020 and beyond.* Ieee Access, 2017. **5**: p. 15667-15681.
33. Zhou, X. and X. Tang. *Research and implementation of RSA algorithm for encryption and decryption*. in *Proceedings of 2011 6th international forum on strategic technology*. 2011. IEEE.
34. Shamir, A., *How to share a secret.* Communications of the ACM, 1979. **22**(11): p. 612-613.
35. Berde, P., M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, and W. Snow. *ONOS: towards an open, distributed SDN OS*. in *Proceedings of the third workshop on Hot topics in software defined networking*. 2014.