Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-021-02946-y

ORIGINAL RESEARCH

Machine learning based hybrid model for energy efficient secured transmission in wireless sensor networks

N. M. Saravana Kumar[1] · **E. Suryaprabha**[2] · **K. Hariprasath**[3]

Received: 28 July 2020 / Accepted: 1 February 2021
© The Author(s), under exclusive licence to Springer-Verlag GmbH, DE part of Springer Nature 2021

Abstract
Wireless Sensor Networks becomes robust while the nodes possessing the self-configuring capability by which they can be either keeping themselves as a part of the network or they can also simply leave. The transmission of Data is achieved through the inter communication among the nodes participated in the network. For most participative nodes, there is a possibility of energy depletion and thus the network dies despite the other nodes having optimal energy for being operative. Bring decentralized, another classical challenge for WSNs is the threat of intrusion detection which may arise DoS attacks that depleted the energy as well. Major works in the literature focuses either attempts to address the Intrusion detection to fix DoS attacks or keep the optimal energy level by introducing energy preserving strategy and dynamic clustering strategy so that the network lifetime could be extended. This work deals with the hybrid model in which the nodes are clustered together to form the Connected Dominating Set so that the data transmission could be augmented. The objective of the system is to include only nodes with adequate energy that can ensure the validity of the network by marking them as CDS node. The CDS probability of a node depends on foresight of the energy of the participant nodes till the transmission. Packet distribution is done based on the CDS of the node and thus the inappropriate network breakdown that keeps same node waking so often could be avoided. Thereby, retransmission has been avoided due to packet drops, which also conserved the energy of the network. From the simulation results, it is understood that the technique decreases the loss of packets and deferment. The simulation results demonstrated that the proposed model has improved performance metrics such as goodput, throughput, packet dropping ratio. Also, it is seen that the network lifetime has been significantly increased to 50% meantime packet dropping ratio has been reduced to 50% with the energy consumption little lower than 3% when compared with the preliminary enhanced energy-dependent constraint DoS (denial-of-service) detection model and thus the network seems fault-proof and extended reliable.

Keywords Machine learning · Security · Energy efficient · detection · Hybrid

1 Introduction

A Wireless Sensor Network (WSN) encompasses numerous sensor nodes and the nodes connect with each other with the help of radio signals. Of which, the self-configured and infrastructure less network could be deployed for monitoring the environment by integrating the network with sensors such as pressure, temperature and sound. In this conventional architecture, the role of base station is to acts as an interface among the users and the network do as to receive information. It is known that every node in the network must possess sufficient resources to commit the transaction. Else, the network has been considered as inactive and dead. It is also to be noted that highly active or frequently used nodes in the network are found to be intrinsically resource-drained

✉ N. M. Saravana Kumar
saravanakumaar2008@gmail.com

E. Suryaprabha
suryapraba10@gmail.com

K. Hariprasath
khariprasathit@gmail.com

[1] Department of Computer Science and Engineering, M. Kumarasamy College of Engineering, Karur, India

[2] Anna University, Chennai, India

[3] Department of Information Technology, Vivekanandha College of Engineering for Women, Namakkal, India

Published online: 17 February 2021

as the nodes is generally characterized to possess less storage capacity, limited bandwidth and processing speed so as to conserve energy consumption. By adapting to multi-hop, potentially a large area could be covered efficiently. Sensors can be deployed in the network either as event driven or incessant depends on the application. The location and the position information could be achieved through the Global Positioning System (GPS) and the local positioning algorithms. The ability of remote sensing makes it adaptable in various applications like smart city, intrusion detection, healthcare monitoring and emergency response etc. But it is observed from various studies that the network is liable to various attacks due to the features in the network (Liu et al. 2018a; Li et al. 2017).

There is always a greater threat of breaching the network by anonymous devices either to steal the data or simply to drain the energy of the nodes by initiating fake transmissions. Although there were many works in the past has been focused to fix the conventional issues such as Denial-of-Service and energy efficient data transmission, in most of the cases the existing models compromising one for the other. Thus, one of the prime contributions of the work is to achieve a balance among the efficient fault-tolerance of the nodes which would result in the lower latency and reduced packet drop whereas maintaining less energy consumption by adapting randomization of clusters and implementing reinforcement learning to fix anomalous behaviour of faulty nodes. Usage of energy could be minimized and the epoch of the network could be enhanced by making the high-energy nodes as heads or relay nodes in a cluster without pertaining the low-power nodes. The idea of Selection of CH/Relay nodes greatly depends on the various attributes such as energy and hop-distance at the moment of the time so as to handle and withstand till the successful transaction. The CH must be in such a way that it must be responsible for all actions that takes place in the cluster. While the proposed model restricts using energy-constrained node of the particular cluster either as CH or relay node, it tries to hop it with the neighbour node with appropriate CDS probability. On the other hand, every time a data transmission has been done by a node, it verifies for its sequence id and other reinforcement leaning stuffs. This capability of the network makes sure the nodes won't simply accept anonymous data transmission that may drains the power and thus greatly addresses the DoS attack as well.

The major contributions of the work that enhanced from the various similar works in the past are as follows:

1. In this work, the establishment of the nodes is completely randomized.
2. The cluster Head has been selected with a novel CDS probability that accounts for energy and other aspects as well.
3. In the discussion part, the work has been compared with two preliminary models without ML to exhibit the performance of the model and is also compared with state-of-the-art models as well to exhibit the superiority among the literature.

The rest of the paper is organized as follows: Sect. 1.1 describes about how those problems were addressed in the literature and is summarized in Table 1. Section 2 briefs

Table 1 Summary of some State-of-Art works

Protocols	Features	Challenges
LEACH (Moorthi and Thiagarajan 2020)	It measures the level of life time of the sensor-nodes and Minimize intra-cluster distance	Routing of packets is critical
DBSCAN (Jafari et al. 2018)	It categorized cluster based on belong-to, not belong-to and ambiguity and Reduce energy consumption	Minimal constraints were considered
FCM (Wang et al. 2018)	Maximizes energy consumption	Packet loss is undesirable
K-means algorithm (Zhu et al. 2019)	High throughput and Less energy consumption	Latency, consumes time
RE-attempt (Ahmad et al. 2014)	Increased network lifetime and throughput and Simplified energy consumption	Will focus on cross-layer design protocols& MAC and network layer have to be focused
Mobile sink-ring routing protocol (Tunca et al. 2015)	The overhead has been decreased and the epoch of the network has been increased by the mobile sink-ring routing protocol	The information which is used for data transmission is in the form of ring which seems to be complex as the nodes are distributed indiscriminately in the space
Load balancing protocol(Ennaciri et al. 2019)	Improved network stability, throughput, and packet drop rate	Energy harvesting scheme needs to be considered& Network lifetime further needs improvement
GECR(Tianshu et al. 2018)	Better network life cycle and Optimal energy utilization	Optimal selection is uncertain

about the problem and proposed model and the system flow. Section 3 briefs on the formation of novel coverset. Section 4 discusses about the simulation and experimental results. Section 5 concludes the result and provides the future direction of the work.

1.1 Related works

Various researchers, academicians have worked towards the energy consumption of the network, security and routing protocols. An active method which focus on the normalization of the utilization of the energy in WSN has been suggested by Li and Guan (2013). It is based on the centrality method and proved to be better than the shortest path routing. But optimization is based on a single parameter which is found to be not adequate for an optimization technique. An energy efficient CH selection (NECHS) method has been suggested by Hu et al. (2009). The principle behind this method is the fuzzy logic since it plays the role in the selection of the CH which considers the neighbouring nodes and the energy that remains still in the network. However, the CH is found to be overburden with certain activities. Dynamic clustering methodology which depends on the Signal-to-noise ratio (SNR) has been devised by Ganesh and Amutha (2013). Sink based routing is utilized for the investigation of patterns and thus security could be provided. Yogeesh et al. (2016) have done a detailed survey of various energy efficient and secured routing protocols. The overhead has been decreased and the epoch of the network has been increased by the mobile sink-ring routing protocol suggested by Tunca et al. (2015). The limitation in this method is that the information which is used for data transmission is in the form of ring which seems to be complex as the nodes are distributed indiscriminately in the space. Energy consumption is handled with the suggested protocol done by Tian et al. (2017) namely network coding and power control-based routing (NCPCR) so that the packets are encoded and decoded. Moreover, the coding gain of the network is achieved so that the energy consumption is minimized. Zaman et al. (2016) focused on the decreasing of the energy utilization with the sensors nodes that are positioned in the cross-layer format which results in minimizing the ideal time of the sensor nodes. The Position responsive routing protocol (PRRP) results in the augmentation of the WSN Performance. In addition, the distance among the source and the sink nodes is averaged. Dehghani et al. (2015) has done a survey of energy efficient routing algorithms and compared its benefits and limitations. Considering all these techniques, Alghamdi (2018) proposed a Dij–Huff Method (DHM) which is the grouping of Dijkstra's algorithm and Huffman coding. The objective of the Dijkstra's algorithm is to determine the nodes that contains the maximum energy and optimal distance path. Each hop is secured with the method known as Binary Hop Count (BHC). The working method of DHM algorithm is described as given below:

1. Nodes that possess the extreme energy and the optimal path among the nodes.
2. BHC is used to secure the hops and routing table is maintained properly. End to end authentication is provided by the Huffman coding technique.

To facilitate the high density in communication, there is a need of new methods to satisfy the severe energy and spectrum requirements.

But the smart applications expect the resources and energy to be used extensively so that the demands and the expectations of the end-users' have to be satisfied. Hence, the deployment of Artificial Intelligence (AI) techniques must be deployed at the network and node level in order to augment the capability, usage and its endurance. Thus, it leads to the empowerment of the intelligent actions and it must be suitable in deployment of various contexts (Wang Li and Leung 2015). Cognizance should be applied so that the networks must be facilitated with the smart communication, optimal management of resources, dynamic configuration of devices and reasonable provisioning of resources. Intellectual approach has to be enforced on the nodes through the implementation of distributed and autonomic methods as discussed in Huebscher and McCann (2008), Galzarano et al. (2013). Certainly, the elements of the networks are found to be raised with the quality of smartness and novel abilities of perception, computation and learning by the deployment of the AI and data mining techniques. From various inferences, it has been understood that works have been done on the optimization of the task scheduling of each and every node, path routing and computation (Sharma et al. 2012; Pottie and Kaiser 2000). The notion behind the energy spent by the node is due to the radio signal transmission. Hence, various works have been carried out in

1. optimization of the data traffic in the network thereby reducing the message load and subsequently leads to the decrease in the broadcast and the receiving time of the individual nodes.
2. the process of communication that takes place among the components of nodes, malleable organization of the node's status (either in sleep or in active periods) by disowning the fixed configuration, snooping of idle period and transmission power etc..

In Mahmood et al. (2013), the objective is to elicit the models and as well as patterns from the continuous and fast sensor data streams. Consequently, the transformation process has to be instigated on the raw data which results to less data traffic. This has been implemented with a modified method

by deploying the intellectual nodes in an autonomous manner and thereby the organization of the whole network is done with the help of the genetic algorithms (Hussain et al. 2007). In addition, the identification of node failure is also done through the application of neural networks (Joshi et al. 2013) or the short message exchange could be done in an effective way by minimizing the cost and make error-free communications from the source to the sink node (Chu et al. 2012; Savaglio et al. 2019). Energy efficiency and the autonomous behaviour is attained through the implementation of machine learning approaches (Gupta and Kumar 2000). Several other works have been done in saving the energy by choosing the radio signals to turn on/off and transmission could be done in specific slots where there is a less possibility of collision. Moreover, cognitive algorithms have been devised which are used to regulate the transmission power of the node, sharing of the clever antenna switching based on the service needs and environmental conditions (Fu et al. 2011).

Similarly, several researchers have focused in the data transmission to be done in periods so that there is a possibility of less collision and the energy could be maintained by turning on/off (Luo et al. 2009). Fasolo et al. (2007) implemented a potential method in Artificial Intelligence named as Reinforcement Learning (RL) so that an energy-preserving MAC protocol so that the epoch of the network could be extended. QL-MAC protocol results from the Q-Learning that cuddles the MAC metrics with the help of a trial and error process so that the low energy state has to be met. There are several benefits such as

1. pre-determination of the system model is not necessary for resolving the minimization problem,
2. Owing to the self-adaptive nature of the protocol, topological or other exterior changes has been done.

The protocol has the ability of amending the duty cycle of the node autonomously and the energy depletion is decreased without damaging the other parameters of the network through the fine tuning of the radio signals. The alteration of radio signals depends on the likelihood of the traffic and the transmission state of the neighbouring nodes. To prolong the network epoch, data collection has to be designed properly. Each sensor node must be supplied with the restricted power supply whereas in various applications, recharging seems to be complex. Consequently, the WSN has the feature of restriction in traffic load. Next, due to the multi-hop transmissions, data forwarding capability is more when the count of nodes is increased (Luo et al. 2009). Load balancing emerges due to the convergence feature of traffic pattern (Liu et al. 2018b). Due to this characteristic, the nodes that are near to the destination node will be short of energy and it is known as the hot spot problem (Tang et al. 2018) which results in the decreasing of epoch of the network. Moreover, more attention is required to solve the ensuing restraints such as energy saving, unreliability and security. Reliable transmission could be done at the cost of reprehensible energy since it stimulates an increase in number of retransmissions. Conversely, sensor nodes aids in simple computing task, so it might be a simple task for the implementation of pre-processing or compression of data collection task. Global traffic could be reduced by adopting the data compression method (Huang 2018). The work done in Qiu et al. (2018) showed the attainment of enticing load balancing through the deployment of the compressive data gathering (CDG) scheme that results in the decrease in the communication costs globally. Apart from the other constraints, the network is inclined to attacks due to the features of WSN. The concealed nodes might create the damage in the network through the interception in the network. Usually attacks could be categorized into external and internal attacks. Internal attacks are more harmful when compared with the external attacks (Suryaprabha and Saravana Kumar 2020; Saracevic et al. 2018, 2019). Authentication might be able to repel the external attack in an efficient manner and very less influence on internal attacks (Del-Valle-Soto et al. 2019). Node's misbehaviour or nodes that seems to be selfish create the internal attacks. Selfish nodes denote that it declines to the requests from various services for saving the energy. It is identified that the selfish nodes do not promote the attack but rather it might lead to adversity in Internet. Hence a very efficient and effective mechanism is required to resolve these issues. Taking all these in to consideration, the present work has proposed a hybrid model through which the data transmission is improved by implementing Reinforcement Learning idea to form Coverset along with existing CDS probability of the nodes and further, the detection process is still more fine-tuned.

1.2 Summary on state-of-the art models

This section deals with the summary on features and challenges of the existing state-of-the-art models that attempts to provide an energy-efficient protocol for WSNs

2 Proposed methodology

The present work deals with the hybrid model which comprises of various features such as Reinforcement Learning (RL), Logistic Regression, Eigen vector structure and the Bayesian model.

In this work, attacker detection process is done by the determination of the pattern and the dynamic structure of the network is controlled by the deployment of RL system. The proposed hybrid model comprises of several units such as

- *Sensor and Base Station (BS)* Sensors are deployed in the network so that the data signals could be detected and therefore the observed information which has been stored in the sensors would be transmitted to the data collection unit.
- *Intrusion Detection Unit (IDU)* The intention of the unit is to distinguish the unusual and malicious nodes through the verification process of the actions of the devices through the learning system that has been implemented.
- *Learning Unit* RL is applied on the behaviour classification.
- *Connected Dominating Set (CDS) Formation Unit* Information about the connection probability and forwarding prob-ability is collected. Later, the implementation of the logistic regression combining with the Eigen vector in the Bayesian network structure is done. The Bayesian probability determines the CDS nodes to be in the structure.

Nodes are positioned in the area in a random manner. Sensor devices are deployed for sensing the various devices such as temperature, pressure and other environmental changes. Nodes could be categorized into two types namely sensor nodes and the base station. In a network, base station is used as a data collector for collecting the data from various sensor nodes in the network. The nodes which are proximity to the base station could transfer the data to it directly without any intermediate hops. Several other nodes that are located out of the range of base station, then nodes behave as relay nodes so that they are connected to the base station. Sensor nodes thus deployed has restrictions in using the resources such as energy and bandwidth. Resource utilization gets reduced during the transmission and reception of data. Communication has been maintained among the sensor devices and the base station with the BS-Timer with the time interval. When the time interval gets expired, the base station sends the message to all sensor nodes in the network. The message comprises of the identifier of the base station and sequence number of the message. This message is transmitted to the one-hop neighbour in the wireless network. There are two verification's that are done in the network.

1. The sequence number is verified for the duplication of the packet before the handling of the broadcast message done by the base station. If the sequence number is existing in the table, then the sensor removes the message.
2. The incoming packet is verified for the routing loop by inspecting the nodes that are visited in the list.

These two conditions are checked and then the sequence number table is updated with the sender identifier and the sequence number. Here, the nodes are considered as the sender's identity and the sequence number is used as the broadcast identity of the sender. The visited flag is updated by including the entry into the message. Then, the rebroadcasting of the modified message would be transmitted so that all the nodes would receive the message in the network. The phenomena in the environment could be monitored with the help of sensors. The suggested hybrid model which comprised of several features is shown in the Fig. 1. Battery power is used by the nodes so that it is operated without any interventions in order to determine the environment changes. As soon as the phenomena is determined, the device provides the raw data which is in the analog form. When the raw data is ready, then the data exchanging process is carried out by the transceiver circuit.

3 Formation of coverset

Sensor nodes in the WSN are connected together to form a cover set. The target area has to be covered with various nodes deployed in the network. The sensor nodes that are connected in the network could be denoted as S = S1, S2, S3,.... If the nodes are connected with the base station without any intermediate hops, then there arise no issues in the energy depletion. When there is a possibility of multi-hops, then the forward connection of the nodes has to be decided based on the computation of the Connected Dominating Set (CDS) connectivity model. The nodes that has to participate in the CDS has to be elected based on the calculation of the CDS probability. The initial CDS probability is computed from the following parameters and it is given in Eq. 1

- Neighbour connectivity (NC)
- Unit energy requirement for completing the single transmission E_0 in terms of EMWA
- Bandwidth value in terms of EMWA(β)

$$\delta_{cds} = N_c + E_0 + \beta \tag{1}$$

The probability of the forward connectivity is examined based on the forwarding distance between the sensor nodes, energy required for maintaining the multihop connection and the bandwidth. It is given in the Eq. 2.

$$F_c = D(S1, P) + E_{m-hop} + \beta_{m-hop} \tag{2}$$

Using the naive Bayes theorem, the Bayes probability has to be computed. Applying Bayes 'theorem the probability of an event is determined based on the probability of an event which has been occurred is given. It is represented as per the Eq. 3. Then the mean value, difference between the average and the individual value, variance and standard deviation is computed for both δ_{cds} and F_c

$$P(A|B) = \frac{P(A)P(B|A)}{P(B)} \tag{3}$$

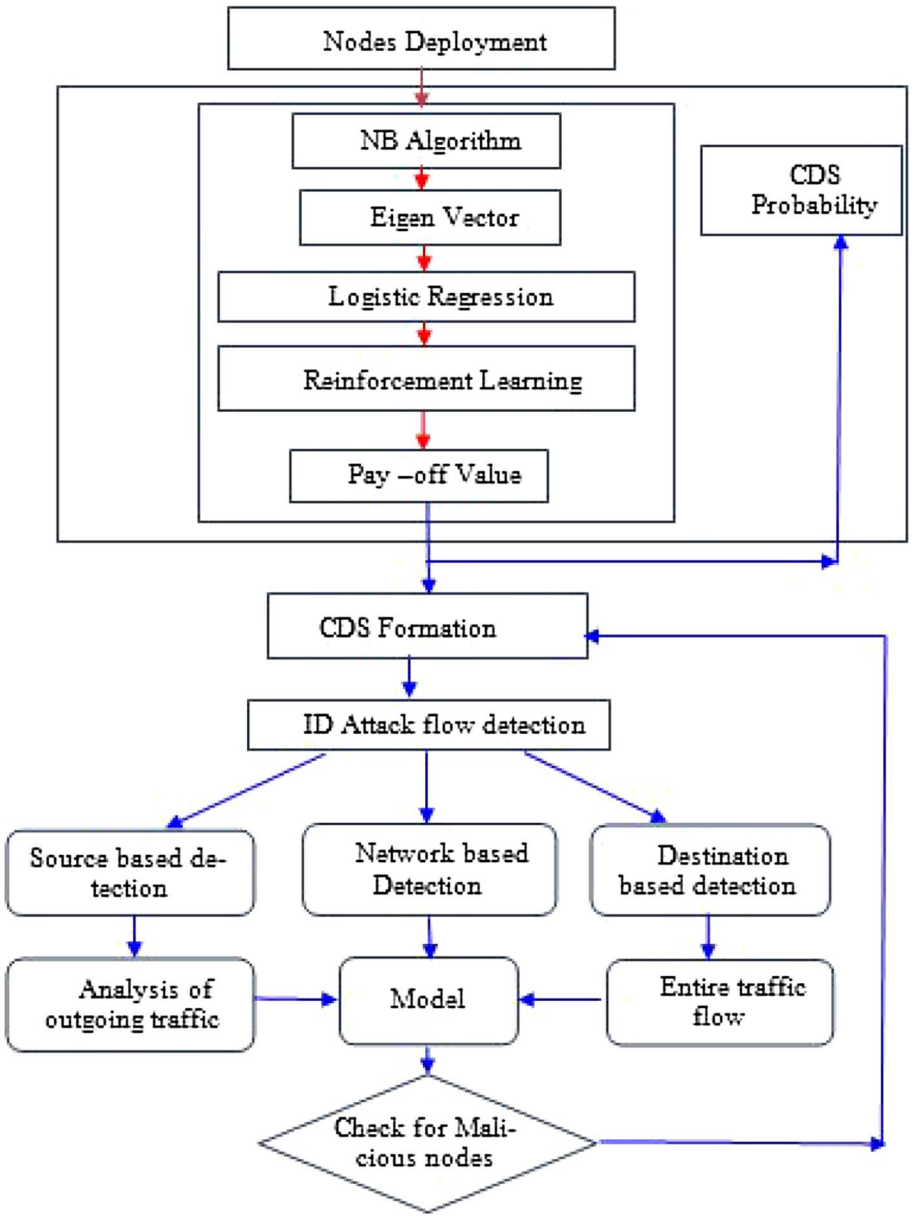


Fig. 1 Architecture of hybrid model

The covariance is predicted by combining the two values and the initial probability value is combined through the weight-based distribution. The upper bound distribution is used for the computation of the two probabilities separately. Multiple Measurement Vector is created based on the four values which could be termed as the single value matrix. Here, the computation depends on the multiple measurement constraint. Rank for the Eigen vector is computed and it is used for the covariance matrix decomposition into non-increasing principal Eigen values. The matrix representation is denoted as

$$\begin{matrix} a & b \\ c & d \end{matrix}$$

The Eigen equation is

$$(a-\lambda)*(d-\lambda)-bc=0 \tag{4}$$

Equation 4 could be rewritten as

$$\lambda^2+\lambda(-a-d)+(ad-bc)=0 \tag{5}$$

Solving Eq. 5 gives the roots of the equation and it is determined through the isolation of the absolute and real values of

the Eigen vector. The final decision value is estimated based on the relative priority values and it is used to choose the relay sensor node and the base station. As soon as the Eigen values are decomposed, then the associated eigenvectors are generated and given as input to the logistic regression. The objective of the logistic regression is to determine the association between the values. The input values are stabilized by dividing the values by minimum, maximum restrictions so that the probability values would be distributed from 0 to 1. The logistic value is evaluated as per the Eq. 6.

$$P = \frac{1}{1 + \hat{e}(-value)} \tag{6}$$

Regression value is computed as denoted in the Eq. 7.

$$R = \frac{p}{1 - p} \tag{7}$$

After the prediction of the logistic regression, adaptive reinforcement learning is estimated from the weight distribution. The data which is taken as the input is normalized with the negative value as the minimum bound and the positive value as the maximum bound. The length of size of the column vector of the normalized data is used to create the learning input factor. Next, the iterative back propagation is started with the constant iteration count. The transfer function accepts the data element in the form of weighted input. This is being joined with the bias functional value. Moreover, the transfer function is deployed for creating the initial weight matrix in which the normalized data is considered. Initially, the bias value is chosen randomly and in the later iterations, it is updated based on the previous learning segments. The next learning stage takes the input from the output of the previous learning stage which in turn disseminates the present output to the next iteration. Deviation in the value which has been analysed from the present weight and the inverse value is distributed by finding the difference between the data and its associated weight value. The payoff value for each weight estimation with respect to the learning stage is computed from the error value. The parameter that played the key role in the selection policy based on the current state and action is the payoff approximation. The decision value of each probability is modified so that the reward or penalty for the action that has been done earlier. Increase or decrease in the payoff function is based on the reward function and it is based on the action performed and its probability. Normalization is used for updating the probability values through the plotting of the lower and upper bound of the state actions. The best combination of the Coverset nodes are chosen based on the final output probability value. The nodes that are formed in the Coverset is used for the connecting each other in the network. In the second level, the same learning model is applied so that the malicious nodes could be distinguished from the normal nodes. Each node is monitored and the traffic rate deviation (T_d) is computed by inspecting the enduring traffic flow and the traffic variance between each flow. The identification attack flow is controlled in three different ways. They are source based, destination based and the network based.

In the source-based attack flow detection, OUTs denote the outbound traffic rate for a specific source node and the average stream of the complete source devices are compared. Source based attack flow detection

$$S_d \rightarrow \left(OUT_s, avg(OUT_s, IN_s)\right) \tag{8}$$

A comparison in average traffic rate and standard deviation is done so that the normal flow and attack flow is distinguished. In network-based attack flow detection and as well as in destination-based attack flow detection, a comparison is done on the whole flow and the particular flow. The specific flow is taken for the intermediate devices and destination devices correspondingly. Furthermore, the hybrid modelling of flow comparison is performed by the combination of the source, intermediate and destination devices. The input to the learning system is the computed traffic values and through this, the trust value is calculated as the final probability value. In this reinforcement learning system, the nodes that possess the lowest probability value is treated as the malicious nodes and hence these nodes would be removed from the network.

4 Results and discussion

The proposed methodology is implemented in NS-2 environment with 100 sensor nodes and 1 base station. The parameters that are considered are shown in the Table 1. Further the experiments have been performed by varying the nodes (n = 100, 125, 150, 175, 200, 225 and 250) which are deployed in a random manner (see Table 2).

Table 2 Parameters and its initial values

Number of nodes	Value
Number of nodes	100 (summed upto 250 nodes for experiment purpose)
Base station	1
Mac type	Sensor Mac with Base Standard IEEE802.11
Data structure	Priority Queue
Total area which is covered	80 m
Topology area	500 × 500
Antenna type	Omnidirectional
Packet size	512
Connection	UDP
Application	Sensor (Temperature)
Packet generation interval	0.1, 0.15, 0.2, 0.25, 0.3
Data rate	3 mbps
Simulation time	100–250 s
No of attacker	5 (DDOS) + 1 (Dropper)
Primary energy	100 J

Table 3 Analysis of total remaining energy in sensor nodes

Interval	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
0.1	10088.7	10090.24	10091.48
0.15	10088.97	10090.44	10091.65
0.2	10089.19	10090.63	10091.81
0.25	10089.41	10090.82	10091.98
0.3	10089.62	10091.00	10092.14

4.1 Simulation of energy and time

The total consumed energy and total left-over energy with respect to time is compared and it is observed that the energy depletion is very less when related with the existing approaches. The simulation results are associated with the existing approaches for further process. Figure 2 depicts the total remaining energy at various intervals. The proposed Machine learning approach is compared with the Optimized DoS (Denial of Service) Detection Algorithm (OEBS)and Denial of Service Attack Detection with energy Constraint in WSN(ODSA) (see Table 3).

From the Fig. 2, it is perceived that the total remaining energy of the sensor nodes are found to be comparatively high when compared with the existing approaches. The energy consumption of nodes must be balanced so that

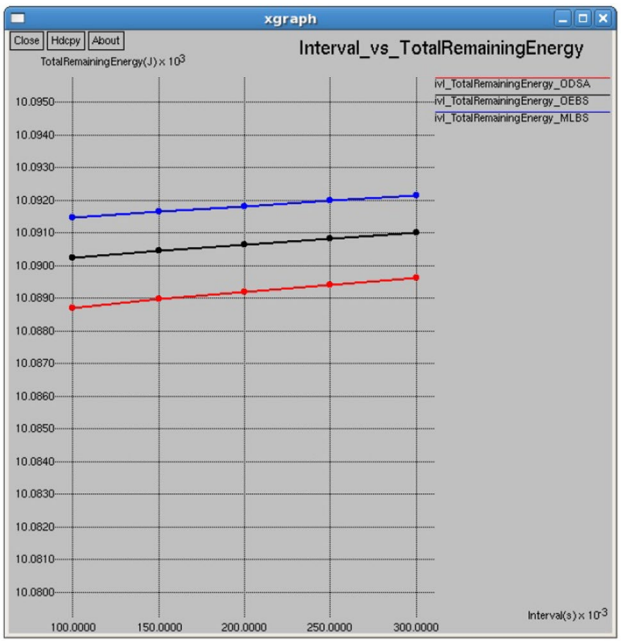


Fig. 2 Interval vs Total Remaining Energy

Table 4 Analysis of average consumed energy of sensor nodes

Interval	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
0.1	0.111424	0.096618	0.084391
0.15	0.109196	0.094686	0.082703
0.2	0.107012	0.092792	0.081049
0.25	0.104871	0.090936	0.079428
0.3	0.102774	0.089118	0.077839

the lifetime of the network has to be prolonged. With the deployment of the proposed methodology, the average consumption of energy in the sensor nodes is balanced as shown in the Fig. 3 which paved the way for the extension in the lifetime of the network as shown in the Fig. 9 (see Table 4).

Other performance metrics such as Packet Delivery Ratio (PDR), Throughput, Relative Energy, received count and packet dropped count are also measured and analysis is done.

Packet Delivery Ratio (PDR) It could be defined as the relation of the total count of the packets conveyed at the destination to the total number of packets transferred from the source.

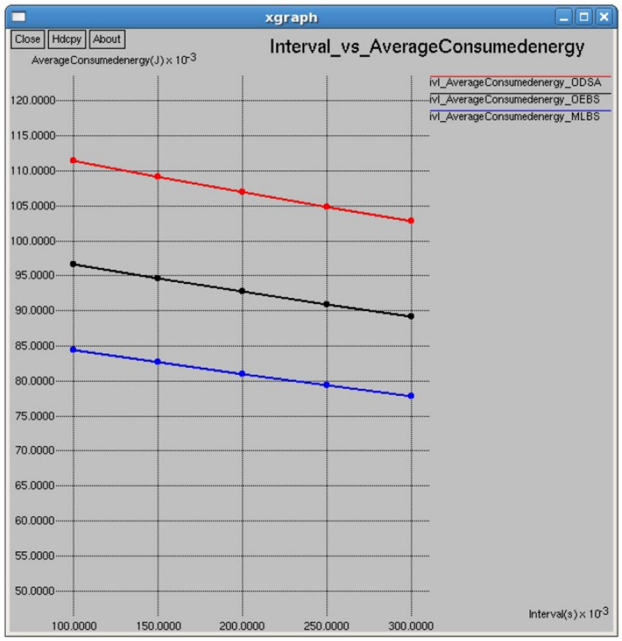


Fig. 3 Interval vs Average consumed energy of sensor nodes

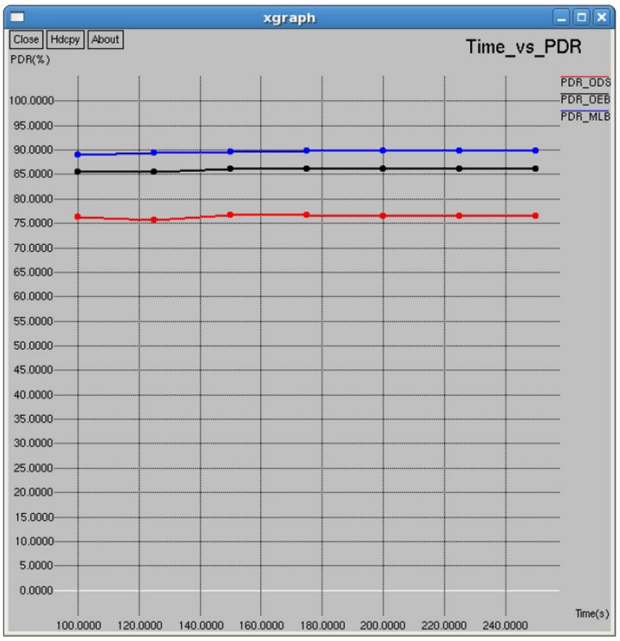


Fig. 4 Time Vs PDR

Table 5 Analysis of PDR

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	76.2195	85.4071	89.0937
125	75.6667	85.4444	89.3333
150	76.6608	86.1525	89.5147
175	76.7143	86.0714	89.7857
200	76.5455	86.0706	89.807
225	76.4211	86.0526	89.8421
250	76.4569	86.0724	89.874

Table 6 Analysis of delay

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	0.072981	0.061692	0.0535697
125	0.0715782	0.0616834	0.0528465
150	0.0710859	0.0624322	0.0518026
175	0.0704964	0.0620835	0.0512003
200	0.0710719	0.0625677	0.0507147
225	0.0710553	0.062983	0.0507992
250	0.0708911	0.0623819	0.0506969

$$PDR = \frac{P_d * 100}{\sum_{i=1}^{n} P_{S_i}} \tag{9}$$

where the P_d refers the number of packets delivered at the destination and P_{S_i} denotes the total packets transferred from the source, 'n' denotes the number of sensor nodes. The proposed ML based methodology showed a great improvement in delivering the packets successfully at the destination node when compared with the other methodologies and it is represented in the Fig. 4 (see Table 5).

Delay It could be termed as the difference in time between the data packet directed by the source node, the data packet received by the destination node and the average is computed.

$$D = \sum^{p} d_i = 1 \frac{(Time(P-d) - Time(P_s))}{P_d} \tag{10}$$

In Eq. (10), Time (P_d) denotes the time at which the packet received at the destination node and Time(P_s) denotes the time on which the packet transmitted from the source node (see Table 6).

The above Fig. 5 shows the comparison of time and delay of the proposed approach with the existing methodologies.

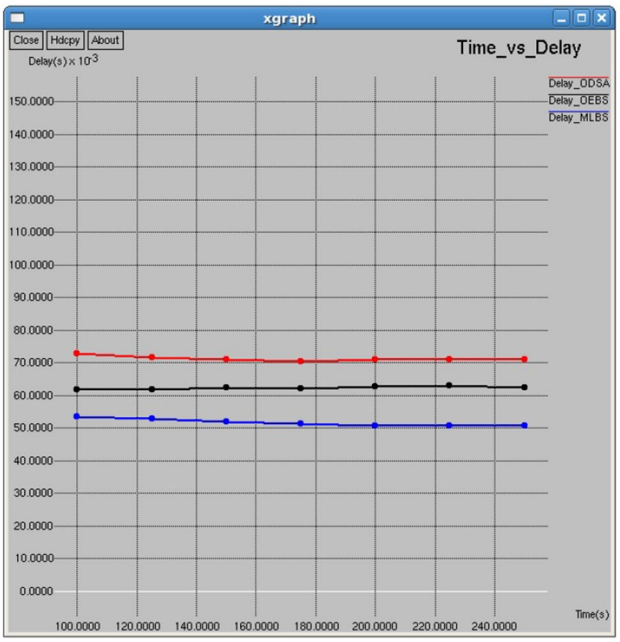


Fig. 5 Time vs Delay

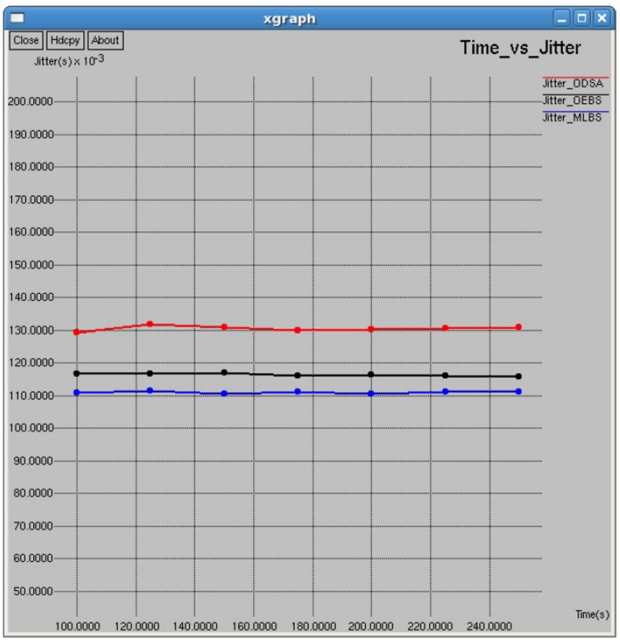


Fig. 6 Time vs Jitter

Table 7 Analysis of Jitter

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	0.12931	0.116606	0.110945
125	0.131653	0.116658	0.111352
150	0.130712	0.116858	0.11051
175	0.129995	0.116106	0.111101
200	0.130262	0.116426	0.110527
225	0.130596	0.116091	0.111136
250	0.130878	0.115916	0.111121

Table 8 Analysis of Goodput

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	56124.2	66394.4	76461.1
125	57224.1	66403.6	77507.5
150	57620.5	65607.2	79069.4
175	58102.2	65975.6	79999.6
200	57631.7	65465.1	80765.5
225	57645.2	65033.5	80631.2
250	57778.8	65660	80793.9

Delay is very less so that the packets could be delivered at the destination node when compared with the other methods.

4.2 Jitter

During the data transmission, there is a possibility of small recurrent delay of data packets that might be due to the various issues such as signal pry, congestion and network crash.

From the Fig. 6, a comparison is shown in which the proposed method shows that the performance of the jitter is less (see Table 7).

4.3 Goodput and throughput

During the data transmission, the transfer speed could be measured in terms of the packet headers, information of the protocol overhead and in addition, the information about the packet retransmission. These factors contribute towards the computation of throughput but in the case of goodput, it is measured in terms of the original data only (see Tables 8, 9).

From the Figs. 7 and 8, it is observed that the goodput and throughput is enhanced through which it is determined that the packet transmission which has been done with the

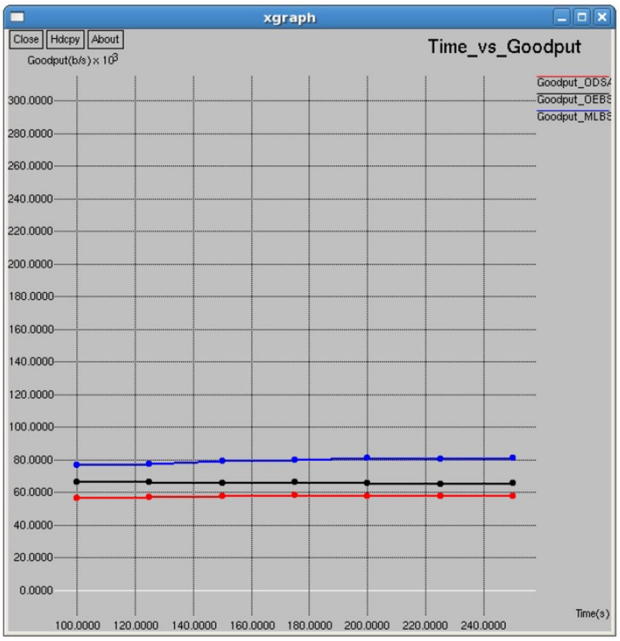


Fig. 7 Time vs Goodput

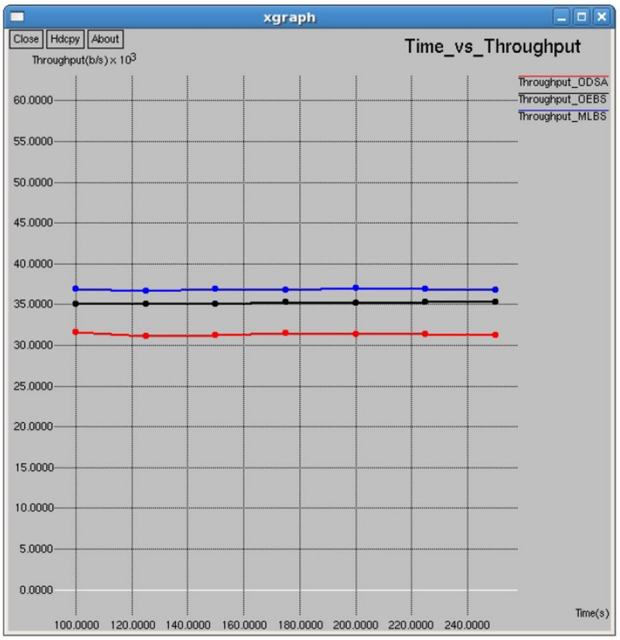


Fig. 8 Time vs Throughput

Table 9 Analysis of Throughput

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	31612.8	35097.2	36911.6
125	31046.7	35033.3	36668.7
150	31272.2	35074.8	36906.4
175	31479.9	35291.1	36824.8
200	31374.7	35190.3	37006.9
225	31331.6	35265.4	36846.1
250	31265.2	35345.8	36765.1

Table 10 Analysis of packets received

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	500	556	580
125	681	769	804
150	877	983	1033
175	1074	1205	1257
200	1263	1415	1489
225	1452	1635	1707
250	1640	1854	1926

proposed methodology showed a remarkable improvement. From the Fig. 7, it is identified that the useful data transmission is done successfully when compared with the existing methods and from the Fig. 8, the throughput is shown a great improvement. Certain metrics that could determine the impact of packet transmission are successful received count and packet dropped count. A comparison has been done and is shown in the below Figs. 9 and 10. From the results, it has been understood that there is a reduction in the packet dropped count and the number of packets received at the destination node is more when compared with the existing methods (see Tables 10, 11).

Moreover, the lifetime of the network is prolonged and it shows a tremendous in-crease when it is analysed. The period of the network has been enhanced with the deployment of Machine learning based approach and shows nearly 50% increase in the lifetime when compared with the other methods which has been depicted in the Fig. 11 (see Table 12).

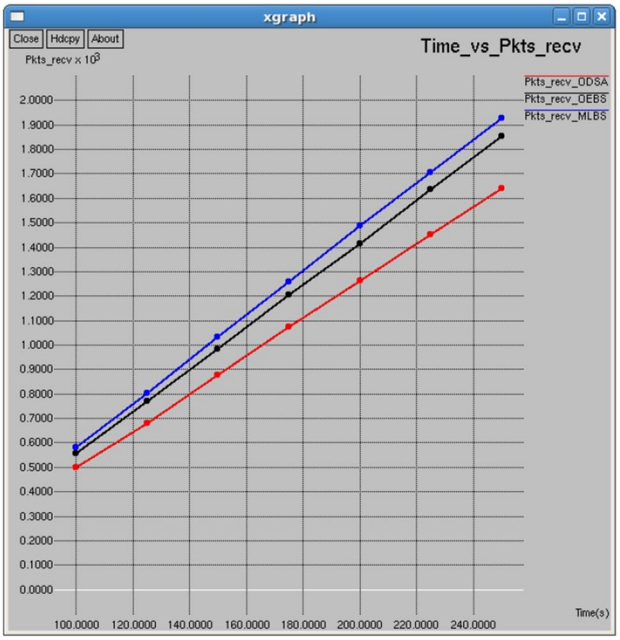


Fig. 9 Time vs. Packets received

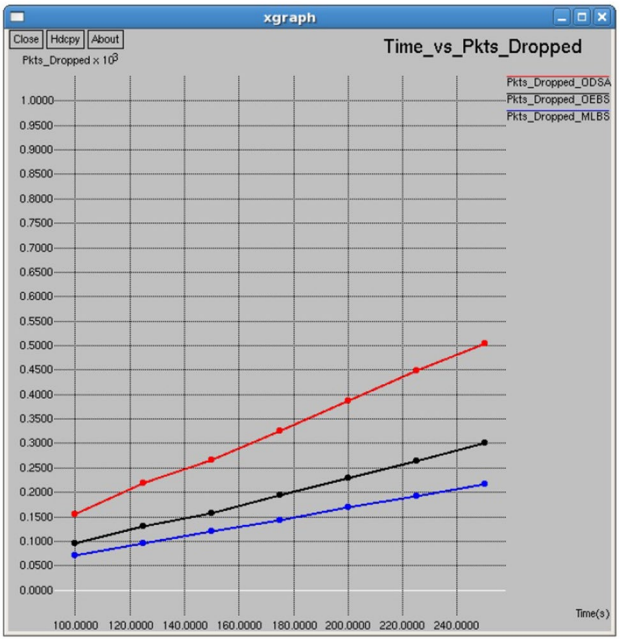


Fig. 10 Time vs Packets dropped

Table 11 Analysis of Packets dropped

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	156	95	71
125	219	131	96
150	267	158	121
175	326	195	143
200	387	229	169
225	448	265	193
250	505	300	217

Packet dropping ratio could be defined as the number of packets that get lost to the number of packets received. With the proposed methodology, the number of packets that are lost is very less when it is compared. Machine learning based methodology showed very less packet drops as shown in the Fig. 12 (see Table 13).

Table 12 Analysis of lifetime

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	100	537200	646847
125	288997	402767	490340
150	230384	322655	404146
175	189634	266576	344547
200	162349	228631	299002
225	141591	199072	265197
250	125789	176654	238645

The normalized overhead is reduced and thus the energy efficiency could be in-creased. It is depicted in the Fig. 13 (see Table 14).

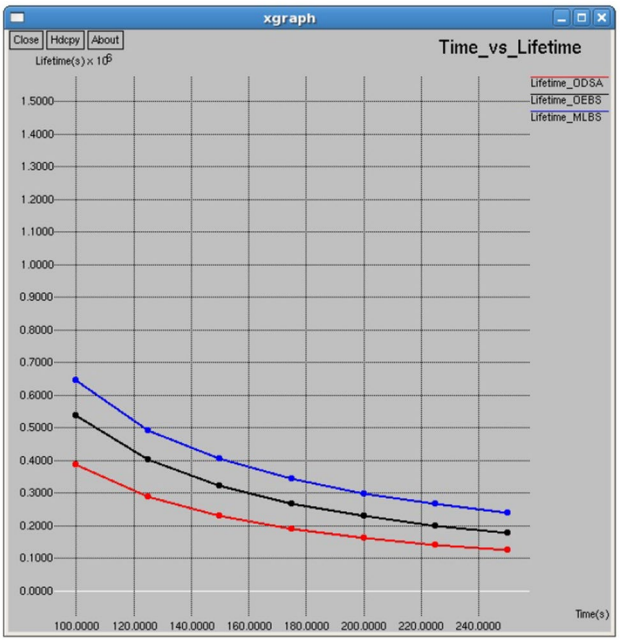


Fig. 11 Time vs Lifetime

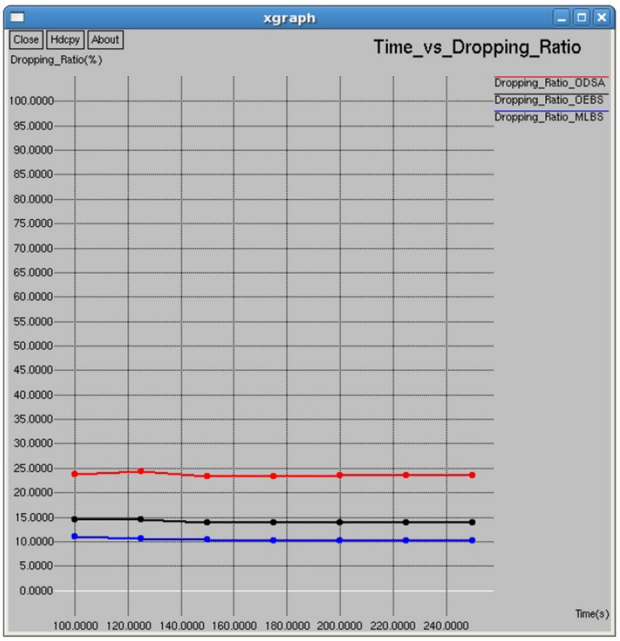


Fig. 12 Time vs Dropping ratio

Table 13 Analysis of dropping ratio

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	23.7805	14.5929	10.9063
125	24.3333	14.5556	10.6667
150	23.3392	13.8475	10.4853
175	23.2857	13.9286	10.2143
200	23.4545	13.9294	10.193
225	23.5789	13.9474	10.1579
250	23.5431	13.9276	10.126

Table 14 Analysis of NRO

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	6.768	6.57014	6.37069
125	125	5.97139	5.78109
150	5.81072	5.61343	5.40077
175	5.55214	5.36846	5.18298
200	5.39192	5.22686	5.00739
225	5.28857	5.10214	4.91564
250	5.20183	5.00324	4.83385

The average traffic rate is computed by analysing the average remaining energy and the average consumed energy. It is depicted in the Figs. 14 and 15 in which the remaining energy on an average of a sensor node is maintained properly when compared with the previous methods and the average consumed energy of sensor nodes is shown a remarkable progress (see Tables 15, 16).

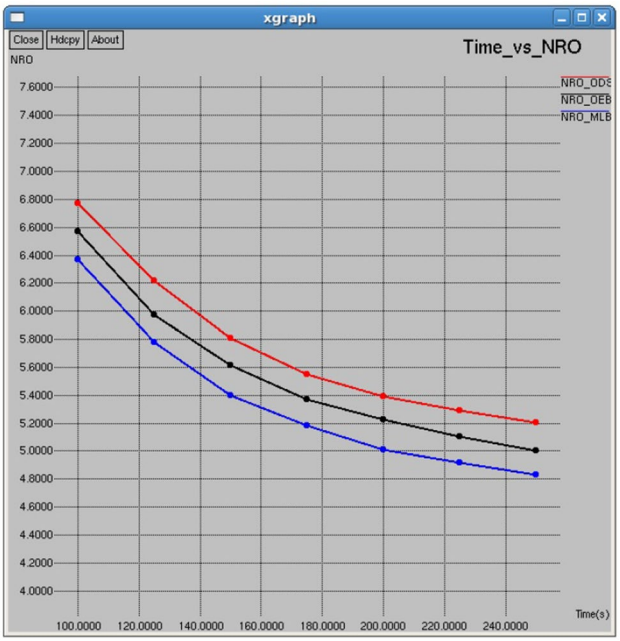


Fig. 13 Time vs. NRO

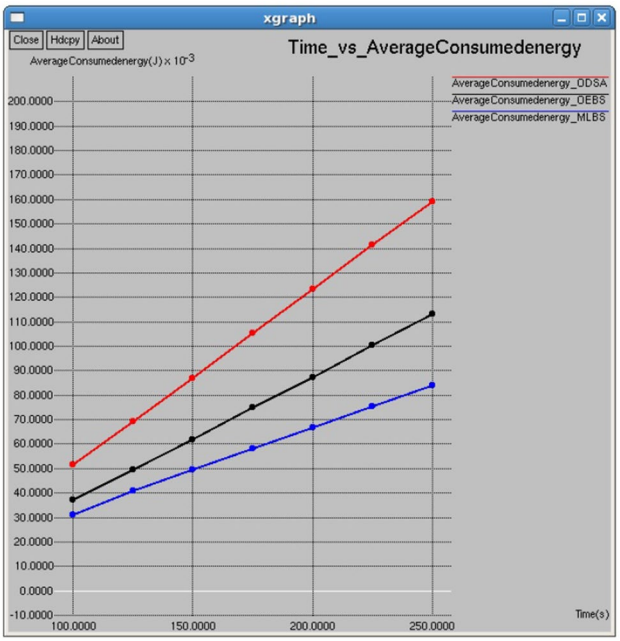


Fig. 14 Time vs Average consumed energy

Table 15 Analysis of average consumed energy

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	0.0515855	0.0372301	0.0309192
125	0.0692048	0.0496565	0.040788
150	0.0868116	0.0619858	0.0494871
175	0.105466	0.0750255	0.0580473
200	0.123192	0.0874772	0.0668891
225	0.141252	0.100466	0.0754157
250	0.158997	0.113216	0.0838065

Table 16 Analysis of average remaining energy

Nodes	ODSA (Suryaprabha and Saravana Kumar 2020)	OBES (Suryaprabha and Saravana Kumar 2020)	Proposed
100	99.9484	99.9628	99.9691
125	99.9308	99.9503	99.9592
150	99.9132	99.938	99.9505
175	99.8945	99.925	99.942
200	99.8768	99.9125	99.9331
225	99.8587	99.8995	99.9246
250	99.841	99.8868	99.9162

The following table plays a crucial part in the discussion part. It portrays the superiority of the proposed model to the recent model that possess benchmarking results and outstanding performance. By having a closer review of the table, it is very clear that proposed model has the lower energy consumption almost 60% lower than ZTR model (see Table 17).

The greatest milestone of the paper is that it possesses the best delay i.e., which signifies the less overhead with respect to time and number of nodes since Reinforcement Learning does wonder once it gets handful of information to route better.

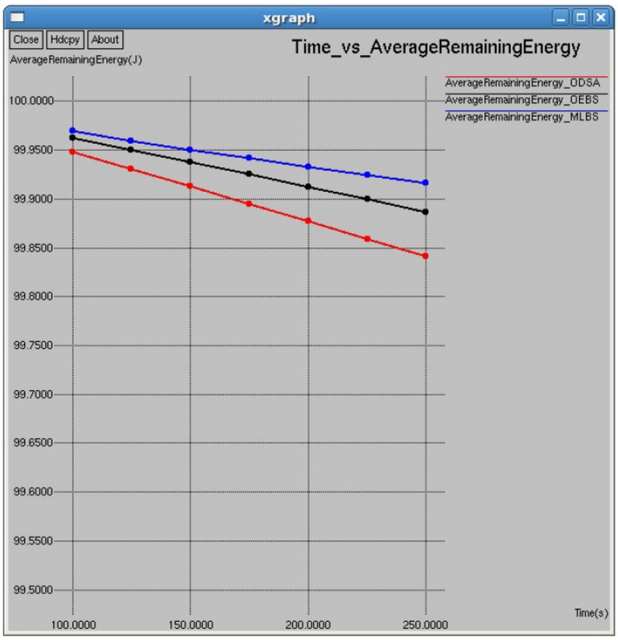


Fig. 15 Time vs Average remaining energy

Table 17 Performance analysis metrics for simulation

Metric	Existing (Del-Valle-Soto et al. 2019)			Proposed
	AODV	MPH	ZTR	MLBS
Energy	262.37	142.94	160.73	100.9
Delay	1.8955	1.1166	1.0573	0.0535697
PDR(%)	70	88	79	90

5 Conclusion

Various issues and challenges still prevail in the WSN. Data transmission takes place with more energy. The most important metric in WSN is the energy of the node in which it gets drained during the data transmission. The proposed hybrid framework which has a combination of RL and ML does the job of connecting the nodes in a remarkable way and the actions of the nodes care identified properly by the deployment of the RL methods so that the optimal cover set of nodes has been framed and thus the connectivity of the nodes is enhanced. The experimental results showed that the data transmission has been improved by analysing the various metrics such as PDR, Delay, goodput and throughput. The lifetime of the network has been prolonged and it shows nearly a 50% improvement when compared with the existing methods. The concern of the work is the PDR. Although it also getting better with number of nodes, still there is a need of improvement. By deploying the RL, the attacker detection process is done so that the malicious nodes are identified at the earlier stage and thus the network is thus formed with the authorized nodes such that the transmission could be done efficiently.

As a future work, Saracevic et al. (2018) motivates to integrate 'dyck words' during data transmission as a carrier message. Since it is light and robust, it would be interesting to implement the idea and to study how it impacts in latency. And its acceptability factor in dynamic WSNs. Similarly, the attempts made by Saracevic et al. (2019) has also been considered to include 'catalan number' as an option for robust identity numbers for authentication and integrity purposes.

References

Ahmad A, Javaid N, Qasim U, Ishfaq M, Khan ZA, Alghamdi TA (2014) RE-ATTEMPT: a new energy-efficient routing protocol for wireless body area sensor networks. Int J Distrib Sens Netw 10(4):464010

Alghamdi T (2018) Secure and energy efficient path optimization technique in wireless sensor networks using DH method. IEEE Access 4:53576–53582

Chu Y, Mitchell PD, Grace D (2012) Aloha and Q-learning based medium access control for wireless sensor networks. In: Proc. International Symposium on wireless communication systems (ISWCS), pp 511–515

Dehghani S, Pourzaferani M, Barekatain B (2015) Comparison on energy-efficient cluster-based routing algorithms in wireless sensor network. Proc Comput Sci 72:535542

Del-Valle-Soto C, Mex-Perera C, Nolazco-Flores JA, Velázquez R, Rossa-Sierra A (2019) Wireless sensor network energy model and its use in the optimization of routing protocols. Energies 13(3):1–33

Ennaciri A, Erritali M, Bengourram J (2019) Load balancing protocol (EESAA) to improve quality of service in wireless sensor network. Proc Comput Sci 151:1140–1145

Fasolo E, Rossi M, Widmer J, Zorzi M (2007) In-network aggregation techniques for wireless sensor networks: a survey. IEEE Wirel Commun 14(2):70–87

Fu L, Qin Y, Wang X, Liu X (2011) Converge-cast with mimo. In: IEEE INFO COM, pp 649-657

Galzarano S, Savaglio C, Liotta A, Fortino G (2013) Gossiping-based AODV for wireless sensor networks. In: Proceedings of IEEE International Conference on systems, man and cybernetics, pp 26-31

Ganesh S, Amutha R (2013) Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. J Commun Netw 15(4):422429

Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst 29(7):1645–1660

Gupta P, Kumar PR (2000) The capacity of wireless networks. IEEE Trans Inf Theory 46(2):388–404

Huang M (2018) A services routing based caching scheme for cloud assisted CRNs. IEEE Access 6:15787–15805

Huebscher MC, McCann JA (2008) A survey of autonomic computing' degrees, models, and applications. ACM Comput Surveys 40(3):1–28

Hu Y, Shen X, Kang Z (2009) Energy-efficient cluster head selection in clustering routing for wireless sensor networks. In: Proc.

5th Int. Conf. wireless communication network mobile comput. (WiCOM), p 14
Hussain S, Matin AW, Islam O (2007) Genetic algorithm for energy efcient clusters in wireless sensor networks. In: Proc. 4th International Conference on Information Technology (ITNG), pp 147–154
Jafari H, Nazari M, Shamshirband S (2018) Optimization of energy consumption in wireless sensor networks using density based clustering algorithm. Int J Comput Appl 43:1–10
Joshi GP, Nam SY, Kim SW (2013) Cognitive radio wireless sensor networks: applications, challenges and research trends. Sensors 13(9):11196–11228
Li X, Guan Z-H (2013) Energy-aware routing in wireless sensor networks using local betweenness centrality. Int J Distrib Sensor Netw 9(5):307038
Li J, Hu H, Ke Q, Xiong N (2017) A novel topology link-controlling approach for active defense of nodes in networks. Sensors 17(3):553
Liu A, Chen Z, Xiong NN (2018a) An adaptive virtual relaying set scheme for loss-and-delay sensitive WSNs. Inf Sci 424:118136
Liu Y, Ota K, Zhang K, Ma M, Xiong N, Liu A, Long J (2018b) QTSAC: an energy-efficient MAC protocol for delay minimization in wireless sensor networks. IEEE Access 6:8273–8291
Luo C, Wu F, Sun J, Chen CW (2009) Compressive data gathering for large-scale wireless sensor networks. In: ACM Mobi Com, pp 145–156
Mahmood A, Shi K, Khatoon S, Xiao M (2013) Data mining techniques for wireless sensor networks: a survey. Int J Distrib Sens Netw 9(7):406
Moorthi M, Thiagarajan R (2020) Energy consumption and network connectivity based on Novel-LEACH-POS protocol networks. Comput Commun 149:90–98
Pottie GJ, Kaiser WJ (2000) Wireless integrated network sensors. ACM Commun 43(5):51–58
Qiu T, Zhang Y, Qiao D, Zhang X, Wymore ML, Sangaiah AK (2018) A robust time synchronization scheme for industrial Internet of Things. IEEE Trans Ind Inf 14(8):3570–3580
Saracevic M, Adamovic S, Bisevac E (2018) Applications of Catalan numbers and Lattice Path combinatorial problem in cryptography. Acta Polytech Hung 15(7):91–110
Saracevic M, Adamovic S, Miskovic V, Macek N, Sarac M (2019) A novel approach to steganography based on the properties of Catalan numbers and Dyck words. Future Gener Comput Syst 100:186–197
Savaglio C, Pace P, Aloi G, Liotta A, Fortino G (2019) Lightweight reinforcement learning for energy efficient communications in wireless sensor networks. IEEE Access 7:29355–29364
Sharma VK, Shukla SSP, Singh V (2012) A tailored Q- learning for routing in wireless sensor networks. In: IEEE Access, pp 663–668
Suryaprabha E, Saravana Kumar NM (2020) Enhancement of security using optimized DoS (denial-of-service) detection algorithm for wireless sensor network. Soft Comput 24:10681–10691
Tang J, Liu A, Zhang J, Xiong NN, Zeng Z, Wang T (2018) A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks. Sensors 18(3):751
Tian X, Zhu Y-H, Chi K, Liu J, Zhang Daqiang (2017) Reliable and energy-efficient data forwarding in industrial wireless sensor networks. IEEE 11(3):1424–1434
Tianshu W, Gongxuan Z, Xichen Y, Ahmadreza V (2018) Genetic algorithm for energy-efficient clustering and routing in wireless sensor networks. J Syst Softw 146:196–214
Tunca C, Isik S, Donmez MY, Ersoy C (2015) Ring routing: an energy-efficient routing protocol for wireless sensor networks with a mobile sink. IEEE Trans Mob Comput 14(9):19471960
Wang Li XX, Leung VCM (2015) Artificial intelligence-based techniques for emerging heterogeneous network: State of the arts, opportunities, and challenges. IEEE Access 3:1379–1391
Wang Q, Guo S, Hu J, Yang Y (2018) Spectral partitioning and fuzzy C-means based clustering algorithm for big data wireless sensor networks. J Wirel Commun Netw 2018:54. https://doi.org/10.1186/s13638-018-1067-8
Yogeesh AC, Shantakumar BP, Premajyothi P (2016) A survey on energy efficient. Secure routing protocols for wireless sensor networks. Int J Comput Sci Eng 5(8):17702–17709
Zaman N, Jung L T, Yasin M M (2016) Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol. Sensors 2016:1–16
Zhu E, Zhang Y, Wen P, Liu F (2019) Fast and stable clustering analysis based on grid-mapping K-means algorithm and new clustering validity index. Neuro-computing 363:149–170

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.