ORIGINAL RESEARCH

Submitted: 12.10.2022; Accepted: 30.10.2022; Published online: 25.12.2022

Adaptive Reinforcement learning with Dij-Huff Method to Secure Optimal Route in Smart Healthcare System

K.Sai Madhuri[1], Jithendranath Mungara[2]

[1]Department of Information Science and Engineering, Visvesvaraya Technological University, Belagavi. Nagarjuna College of Engineering and Technology, Research Centre, Bangalore, Karnataka, India

[2]Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, Bangalore, Karnataka, India

Abstract

The Wireless Sensor Network (WSN) is a multi-hop wireless network that contains multiple sensor nodes agreed in a self-organized mode. The significant advancement in the healthcare, the security of the medical data became huge disputes for healthcare services. Intrusion Detection System increasingly demands automatic and intelligent intrusion detection approaches to handle threats caused by a growing number of attackers in the WSN environment. Reinforcement Learning is a fundamental approach to improving routing efficiency. This approach introduces Adaptive Reinforcement learning with Dij-Huff Method (ARDM) for secure optimal route in WSN. Adaptive Reinforcement Learning (ARL) is a machine learning technique that selects the best forwarder node. The node energy, node Received Signal Strength, and node delay parameters determine the forwarder nodes in the WSN. Furthermore, the Dij-Huff Procedure (DHP) is a mixture of Dijkstra's algorithm and Huffman coding. Dijkstra's algorithm is applied to discover the sensor nodes with the highest energy and the best possible distance route. Huffman coding computes the binary hop count to offer each hop security. The simulation results and their comparison with conventional protocol demonstrate that the proposed scheme has a better detection ratio, a better throughput, and increased energy efficiency.

Keywords

Adaptive Reinforcement learning, Dijkstra's algorithm, Binary hop count, Intrusion Detection System, Hop security, Wireless sensor network.

Imprint

K.Sai Madhuri, Jithendranath Mungara. Adaptive Reinforcement learning with Dij-Huff Method to Secure Optimal Route in Smart Healthcare System. Cardiometry; Special issue No. 25; December 2022; p. 1131-1139; DOI: 10.18137/cardiometry.2022.25.11311139; Available from: http://www.cardiometry.net/issues/no25-december-2022/adaptive-reinforcement-learning

Introduction:

A WSN working function is to observe, process, and forward the information in an indicated atmosphere. WSN contains a number of nodes that gather and forward the information to the Base Station (BS). WSN technology offers many advantages, for example, cost minimization, dependability, scalability, tractability, correctness, and simple distribution [1]. WSNs characteristically comprise thousands of resource-constrained sensors to observe their environments, gather information, and transmit it to the destination for further handling. Though WSN is deliberated, great encounters specified the distribution size, and the related quality disquiets, for example, resource management, reliability, and scalability [2].

RL makes up an uncomplicated non-linear facility that converts from lower layer to higher layer to reach a superior resolution. It is encouraged via transmission plan and information treatment in nerve preparations. The benefit of this learning is eliminating great-level features from the information; also, it can be qualified to achieve many aims. It is applied in many fields such as social networks, business intelligence, handwriting recognition, Bioinformatics, speech detection, and image processing. This kind of learning has many compact issues like routing, data quality evaluation, energy-saving, and attacker detection.

Energy Preserving Secure Measure against Wormhole Attack that preserves energy and it provides security by the network connectivity. This approach is worked by connectivity and information of neighborhood. This approach is used to detect the wormhole attack [3]. Presently the combination of the sensor is precise and significant by allowing the features of social networks for enhancement [4].

Recently WSN and the emergence of secure data processing techniques have enabled a wide possibilities for human-centred applications. Figure 1 illustrates Sensor node based Healthcare application. Medical sensors and devices have determined the appearance for observing patient data, and forward these information to the user. However, secure data transmission is

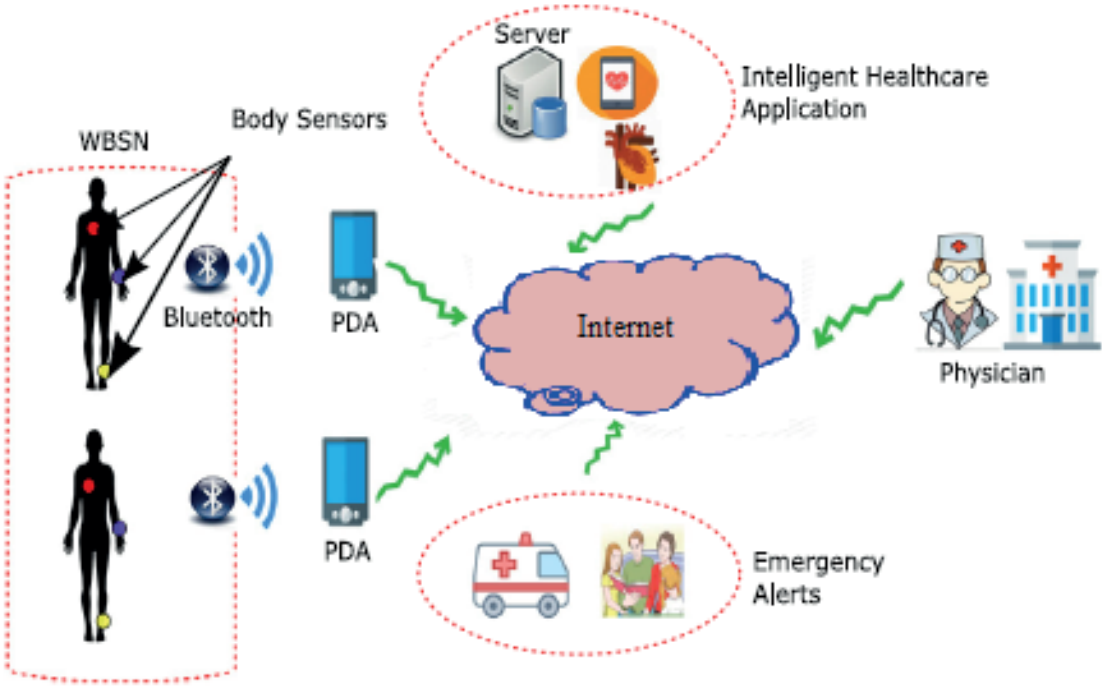

Figure 1: Sensor based Healthcare application

important factor. Thus this approach using ML algorithm for detecting intrusion nodes and it forward the reliable data from patient to the user.

Problem Statement:

Identify Selective Forwarding Attacks (ISFA) by the danger model for detecting the accuracy in WSN. The intrusion nodes launch the selective forwarding attack that drops the part packets. An artificial immune system is recognized for the attacks. The support vector machine mechanism detects the intrusion nodes based on the sensor node's energy utilization, rate of forwarding, duration, frequency of communication, and communication time. However, this approach can't provide efficient security in the WSN [5].

To solve these issues, this paper Adaptive Reinforcement learning with Dij-Huff Method for secure optimal route in WSN is proposed. Here, Adaptive Reinforcement Learning (ARL) is a machine learning technique that selects the best forwarder node. the Dij-Huff procedure is a mixture of Dijkstra's algorithm and Huffman coding. Dijkstra's algorithm is applied to discover the sensor nodes with the highest energy and the best possible distance route.

2.Related Works

An adaptive ensemble learning method can incorporate the benefits of detecting data and reach optimal outcomes by ensemble learning. The adaptive voting algorithm with Multi-tree methods enhances intrusion detection. The adaptive voting algorithm contains a decision tree, random forest, and deep neural network mechanisms. [6]. The objective of this work is to enhance the training data quality. A network intrusion detection system is important for removing network attacks. ML mechanism contains balancing, sampling, and feature engineering. Systematic ML concentrates intrusion detection [7]. ML-based Intrusion Detection System using detection threshold is selected to differentiate the benign and attacker nodes. The adaptive feature selection procedure at every reporting time enhances the function, differentiating benign and attacker nodes [8].

A malicious-node identification mechanism established on correlation theory avoids fault data injection. Initially, irregularity among the same types of sensor information is identified by time correlation. Next, detects the malicious nodes by applying the spatial correlation. Finally, the event correlation method recognized the malicious nodes. However, this approach enhances the false-positive and false-negative ratios [9]. Reinforcement learning with a deep neural network method for detecting the intrusion. The deep Q-Learning method offers an auto-learning ability to distinguish intrusions by applying an automated trial-error approach. However, this approach's accuracy is low, and it needs to improve its self-learning capabilities [10]. A passive attack represents that the

attacker nodes take the data by observing means; such an attack can be avoided through authentication and data encryption. Active attack indicates packet loss network communication and updating route information to the attacker nodes. The ML method is used to detect the malicious nodes in the WSN [11].

A blockchain established secure routing in the WSN. The blockchain method is applied to register the nodes and accumulate the communicated data packets. The Proof of Authority consent method is applied to evade the additional overhead gained [12]. The Genetic Algorithm-established Support Vector Machine and Genetic Algorithm-based Decision Tree mechanisms are introduced for detecting malicious nodes in the network. Then, the optimal routing is used to find the optimal forwarder in the network [13]. A system for detecting malicious nodes by IPv6.This method is planned for the IPv6 environment. In the application layer, the malicious node detection system is implemented. It applies cooperative algorithms and collective decision-making to detect malicious nodes [14].

A classification technique in that the decision for the class association is established on exact combinations of attribute states here, and those mixtures are stimulated by reliability. Incorporate ML into the simulation-based consistency evaluation approach, and evaluate the system consistency in an experimental manner [15]. The core reliability evaluation system is a supervised learning method named perception, a state-space classification-based approach for system state evaluation. It detects the intrusion by the node's signal strength. In this approach, energy maintenance also small handling load between the most serious problems. Particularly, classical approaches are utilized for detecting and avoiding attacks [16]. This approach enhanced the rate of node packet delivery and recognized the fake identity with ML methods, for example, Logistic Regression, Naïve Bayes, and Random Forest [17].

Any malevolent attacks lead to breaking off security by performing as a node that dishonestly declares many fake individualities concurrently [18]. ML model to distinguish the attacks based on the SVM method. Three SVM kernel operations established classifiers to differentiate the malevolent nodes from reliable ones through measuring the variance [19].Trust assessment illustrates the diversity in disparate appliances. Trust methods typically concern trust-related material to compute the trust. Although these methods can compute the trust, they moreover broadcast huge appropriate arithmetical requirements for evaluation. Sporadically, it is nonflexible for apprehension samples. The collection of trust-relevant features and the establishment of the rule significantly concern the precision of trust evaluation. It ignores intelligence and active sustain [20].

A number of trust strategies transmit linear aggregation to gather dissimilar trust-impact properties via confidence evaluation in these application regions like multi-agent systems and service environments. Concurrently employ linear aggregation to combine confidence features such as recommendations, experience, knowledge, and so on to transmit trust materialize uneven missing speculative and realistic maintain. Thus, trust evaluation accuracy could be doubtful [21].

3. Proposed Method

WSN contains number of medical sensor nodes and it capable to forward medical data in run time. Though, in WSN several security issues that demand a secure data communication and authentication in resource constrained environment. Adaptive Reinforcement learning is a ML during the interface between a decision-making agent and its situation. Here the agent performs an action through mapping the environmental input to state in discrete time steps. The situation demonstrates the new state and responds with positive or negative feedback, which is the reward that measures the efficiency of the executed action. The collection method of action is established on a factor, for example, the average reward with time. The agent next informs its related rule targeting the best future rewards.

DHP represents the combination of Dijkstra's with Huffman coding. Dijkstra's algorithm is applied to discover the medical sensor nodes with the highest energy and best minimum distance route. Huffman coding is utilized to receive end-to-end security. To offer security at every hop is known as a Binary Hop Count (BHC).

DHP is using the following procedures

- To discover the nodes with the highest energy and the best route between end sensor nodes.
- To compute the binary hop count at every hop through handles the routing table to offer the security.
- End to end authentication is specified by applying a half-man Coding

Figure 2 illustrates a sample network structure. The S represents the sender, and the R represents the receiver in this figure. The sender desires to forward the data to a receiver; we use the ARL method to select the best forwarder and BHC to isolate the intrusion sensor nodes in the WSN.

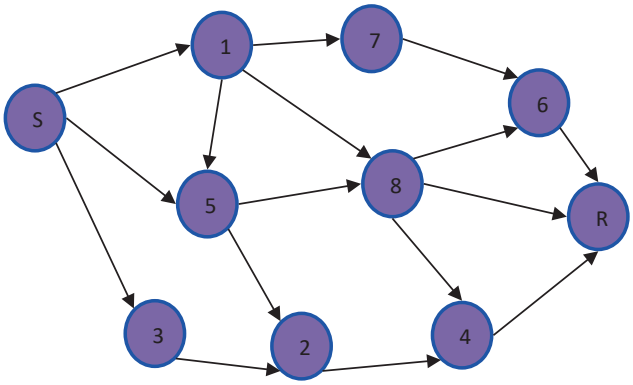

Figure 2: Sample Network Structure

In WSN, each sensor node is homogeneous since each node has similar transmission energy. The RSS value is utilized to indicate the energy level in the received signal. The RSS calculates the equation given below.

$$RSS = \frac{T_p G_t G_r H_t H_r}{d^4} \quad (1)$$

Where,

T_pà Transmission energy

G_tà Gain of Transmitter

Gr à Gain of Receiver

H_tà Transmitter antenna height

H_rà Receiver antenna height

d à Distance between sender and receiver

In WSN, sensor node energy acts as a significant function in communication. A node with lesser energy dies in a minimum time interval, and it is not able to transmit the data packets. Therefore it is a significant factor to consider this parameter to intend an efficient route. The sensor energy can be computed as

$$E_N = \frac{R_{RP} \bullet D_{i,j}}{\alpha \bullet D_{S_n,R_n}} \quad (2)$$

Here, R_{RP}- Rate of Received Packet

$D_{i,j}$- Distance between nodes i and j

α - Constant

$D_{Sn,Rn}$ – Distance between sender and receiver

The delay between the nodes i and j is computed as

$$D_{i,j} = OPT_j - GPT_i \quad (3)$$

OPT_j- Obtained R_{REQ} packet time

GPT_i- Getting R_{REP} packet time

Markov Decision Process (MDP) offers a statistical framework for making a decision environment under different actions. It facilitates the forecast of the following state s,' and the following reward r along with the present state s and action a. Figure.3 explains a block diagram of the ARDM method.

An MDP is four attributes (S, A, Ra, Pa) here:

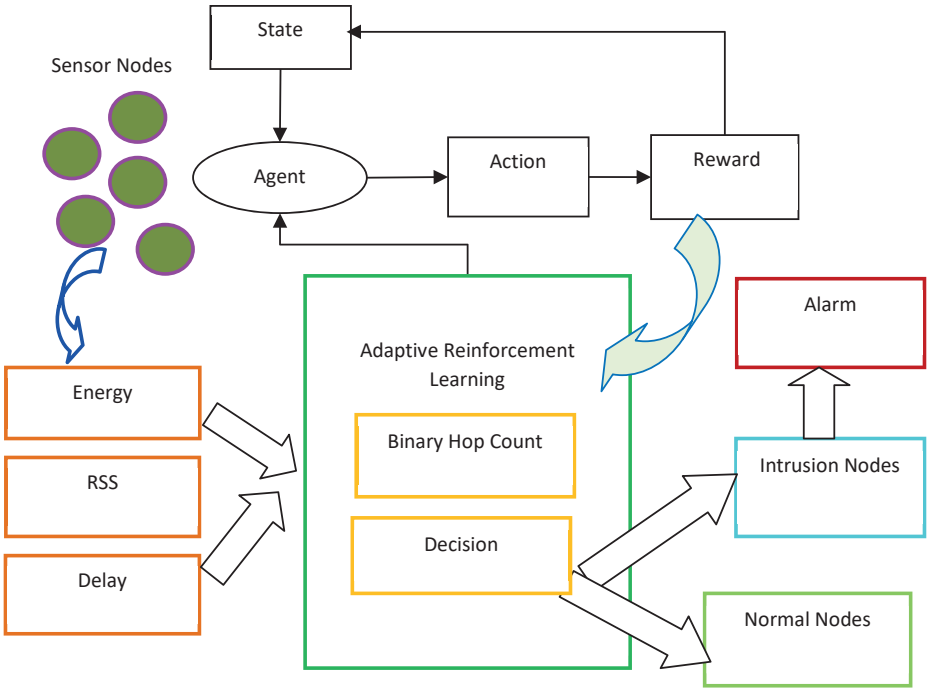

Figure.3 Block Diagram of ARDM approach

S represents a limited set of states. A is a limited set of actions, and A_s indicates, the limited set of actions available from state s.

$(P_a(s, s')=pr(s_{t+1} = s' | s_t = s; at = a)$ is the transition probability function that action a in state s and time t will lead to state s0 at time t + 1.

$R_a(s, s')$ is the instantaneous reward that is obtained after alteration from state s to state s' owing to action a.

P_a and R_a are the dynamics situation.

A limited MDP with a limited set of states and actions here, every action utilizes an identical duration, and the agent can examine the situation at all periods. ARL builds the table where the rows indicate the states and the columns indicate the actions. In each S, the agent obtains an action A, observes the reward for action R and the following state S, and modifies the predictable Q value.

$$Q'(S_t, A_t) \leftarrow (1-\lambda)Q(S_t, A_t) + \\ +\lambda(R_t + \gamma \max Q(S'_t, A'_t)) \quad (4)$$

It maintains a Q-value in a table for every state-action Q(s, a). Permit a_t and s_t submit to the action and state perform through an agent at time t and r_{t+1} indicates the RL that the situation has created for acting in-state s_t. When the agent accepts the returned reward r_{t+1}, it updates the table Q-value that communicates to s_t and a_t. Here, we determine the R_t value by node RSS, energy, delay, and Binary hop count for data transmission. The highest reward node is selected as the best rewards node. Here, the value rewards computation is given below.

$$R = \gamma^{BHC} \times (RSS + E + D) \quad (5)$$

Here, λ indicates the learning rate that presents between 0 to 1 and γ indicates a constant for the rewards relative value that presents between 0 to 1 correspondingly.

Forwarder Selection and Intrusion Isolation:

We measure the sensor node distance and energy, and RSS parameters then the node is verified BH security. If it is equivalent to the predictable security, that sensor node is normal and can receive the data from the forwarder node.

The security code of hop 1 is 01.

The security code of hop 2 is 10.

The security code of hop 3 is 11.

The security code of hop 4 is 100.

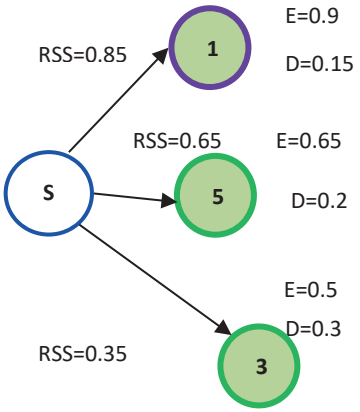

Figure 4 ARDM based optimal Forwarder Selection (First Step)

In this approach, the sender S searches the forwarder nodes among nodes 3, node 5, and node 1. S selects the forwarder node based on the node delay, energy, and RSS value. Here, the node 1, 5, and 3 nodes BHC value is 01. As a result, nodes 1,5,3 are normal nodes. From figure 4, the node 1 RSS value is 0.85 and that value is greater than the other two-node values. Similarly, the node 1 energy value is 0.9. This energy value is greater than other values. In addition, the node 1 delay is very low compared to the other node values. Hence, we select node 1 as a forwarder node.

From figure 5, node 1 selects the forwarder node based on the node energy, node delay, and node RSS values. Here, the chances of nodes 5, 7 and 8 BHC value is 10. But, the node 7 BHC value is 01. Hence, node 7 is an intrusion sensor. But, node 8 is a forwarder node based on the node energy, delay, and RSS values. Similarly, these processes proceed till the receiver receives the information.

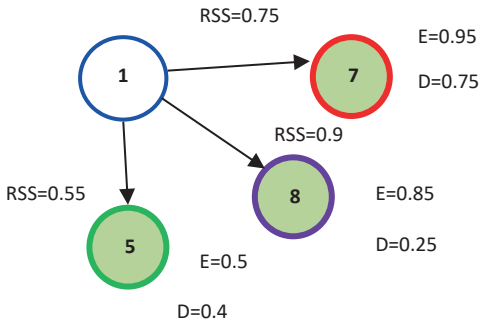

Figure 5 ARDM based optimal Forwarder Selection (Second Step)

Simulation Analysis:

In this paper, we performed experiments to estimate the function of the ISFA and ARDM approaches. In this work, we use the network simulator-2.35 tool to measure the network function of ISFA and ARDM

approaches. In this setting, sensor node's transmission range is 250 metre and utilizes 100 sensor nodes. It detects the performance of ISFA and ARDM approaches in terms of packet delivery ratio, delay, packet loss ratio, remaining energy, and intrusion detection ratio.

Throughput Ratio:

Throughput denotes the number of data packets transmitted to the receiver node per unit of time. It is measured as obtained throughput in bps unit, and it is computed through the equation as given below:

$$Throughput = \frac{\sum_0^m PacketReceived(m)*512}{1000} \quad (6)$$

Here, m indicates the sensor node count

Figure 6 displays the throughput of ISFA and ARDM approaches based on Sensor node count. From this figure, the ARDM approach offers better throughput than the ISFA approach. The binary hop count method improved the security, and the ARL method selects the best forwarder in the node. But, the ISFA approach can't choose the optimal forwarder in the network.

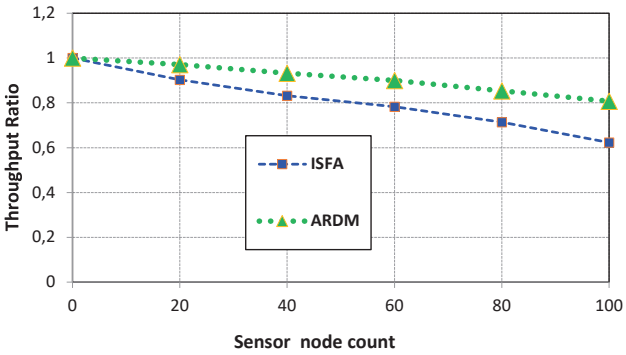

Figure. 6 Throughput of ISFA and ARDM approaches based on sensor node count

Average Delay:

The delay is the time between the receiver node receiving the packets and the sender node forwarding the packet. It is measured by the equation given below.

$$Delay = \\ = \sum_0^m \text{Time of } Packet \text{ Re}ceived - Time\ of\ Packet\ Sent \quad (7)$$

Figure 7 displays the delay of ISFA and ARDM approaches based on sensor node count. From this figure, the sensor node raises, and the node delay also increases in the network. The ARDM approach selects the forwarder based on the minimum delay nodes. Hence, it minimized the network delay. But, the ISFA approach improves the network delay.

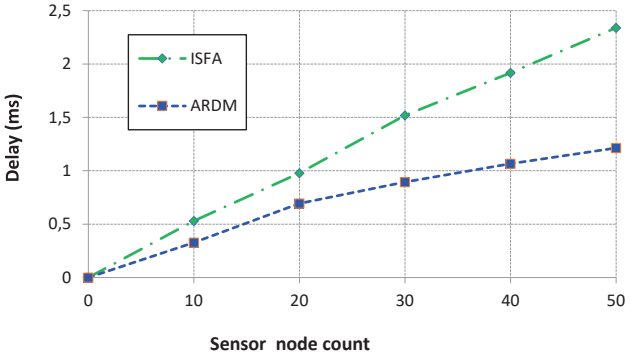

Figure. 7 Delay of ISFA and ARDM approaches based on Sensor node count

Packet Loss Ratio:

Packet Loss Ratio is represented as the whole forwarded packets not obtained at the recipient. It is computed as the equation given below.

$$Packet\ Loss\ Ratio = \\ = \sum_0^m Forwarded\ Packets - \text{Re}ceived\ Packets \quad (8)$$

Figure 8 illustrates the packet loss ratio of ISFA and ARDM approaches based on sensor node count. Usually, packet losses are owing to the minimum RSS, inadequate energy, increases in the delay, etc. In the ARDM approach, the ARL method selects the forwarder by the node RSS, the energy, and the delay. Hence, the ARDM approach minimized the packet loss ratio in the network. However, the ISFA approach raises the packet loss ratio in the network.

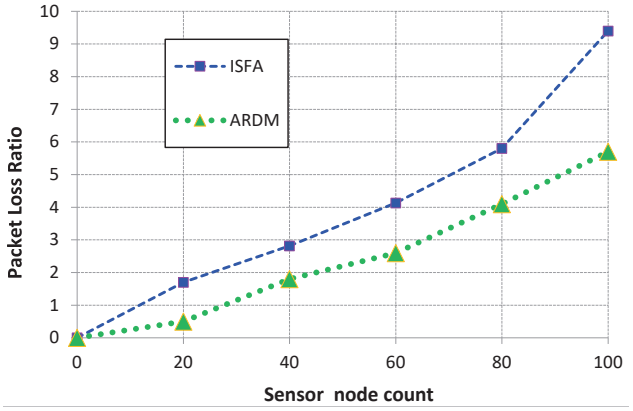

Figure. 8 Packet Loss ratio of ISFA and ARDM approaches based on sensor node count

Remaining Energy:

Figure 9 demonstrates the remaining energy of ISFA and ARDM approaches based on sensor node count. From this figure, our ARDM approach has the highest remaining energy than the ISFA approach. In the ARDM approach, the energy parameter is important for select-

ing the forwarder node. As a result, the ARDM approach minimized the unwanted energy utilization in the network. But, the ISFA approach raises energy utilization.

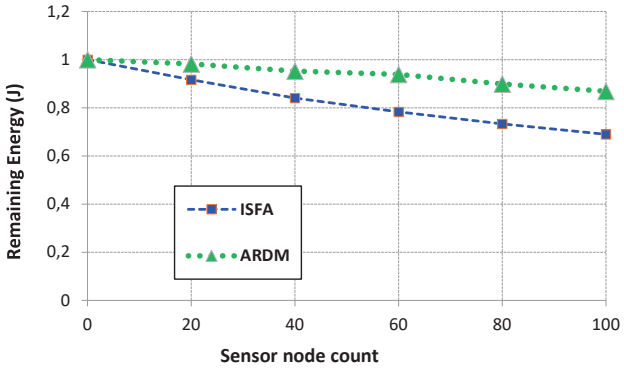

Figure. 9 Remaining Energy of ISFA and ARDM approaches based on sensor node count

Detection Ratio:

The detection Ratio is declared as the correlation between the count of properly-recognized intrusion sensors and the count of intrusion sensor. It is computed by the formula given below.

$$DR = \\ = \frac{Count\ of\ \ properly\ recogonized\ \text{int}rusion\ Sensor}{Whole\ count\ of\ \ \text{int}rusion\ sensor} \quad (9)$$

Figure 10 explains the DR of the ISFA and ARDM approaches based on sensor node count. From this figure, the DR of the ARDM approach is greater than the ISFA approach. Since ARDM approach by applying the BHC method to isolate the intrusion sensor efficiently. But, the ISFA approaches can't detect the intrusion efficiently.

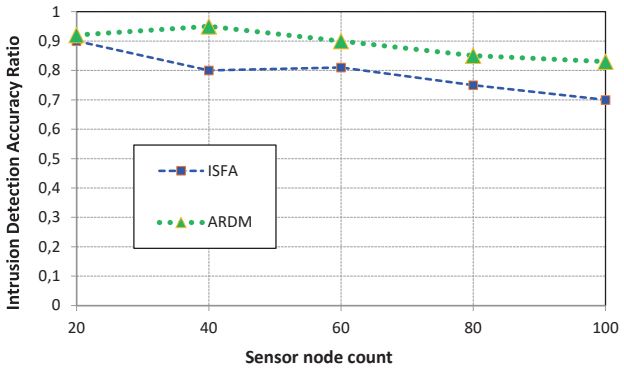

Figure. 10 Detection Ratio of ISFA and ARDM approaches based on sensor node count

False-negative ratio (FNR):

It is mentioned as the ratio between the number of intrusion nodes that are incorrectly classified as normal sensor nodes and the entire number of normal sensor nodes. It is mentioned in equation.

$$FNR = \\ = \frac{Number\ of\ \ incorrectly\ recogonized\ as\ a\ normal}{Number\ of\ \ Normal\ Nodes} \quad (10)$$

Figure 11 demonstrates the FNR of the ISFA and ARDM approaches based on sensor node count. Here, the FNR of ARDM is smaller than the ISFA; since ARDM, the intrusion nodes are isolated through an adaptive reinforcement learning.

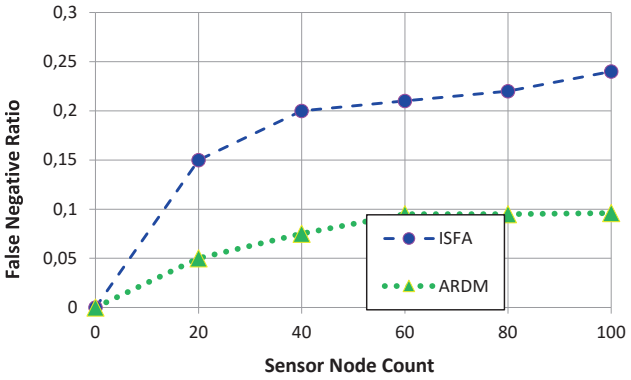

Figure 11: False Negative Ratio of ISFA and ARDM approaches based on sensor node count

False-positive ratio (FPR) versus sensor node:

It is mentioned as the association between the number of usual sensor nodes that are incorrectly categorized as an intrusion and the entire number of normal sensor nodes. It is mentioned in equation (11).

$$FPR = \\ = \frac{Number\ of\ \text{incorrectly}\ categorized\ Intrusion}{Number\ of\ \ Normal\ Nodes} \quad (11)$$

Figure 12 demonstrates the FPR of ISFA and ARDM approaches based on sensor node count. The FPR of the ARDM is smaller than ISFA because ARDM approach isolates an intrusion sensor nodes efficiently. Thus, the ARDM approach reduced the FPR.

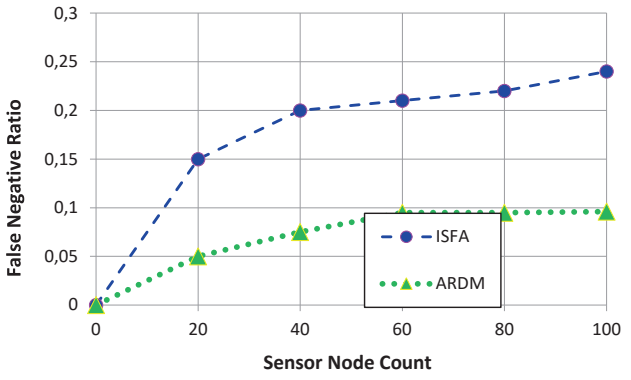

Figure 12: FPR of ISFA and ARDM approaches based on sensor node count

Conclusion:

Secure health care system main objective should maximizes the health care quality and minimize the health care cost. WSN presents numerous issues and challenges caused by intrusion sensor, inadequate energy, and the absence of security. The sensor node energy is the significant parameter; this approach avoids the break down. This approach exists an Adaptive Reinforcement learning with Dij-Huff Method for Secure Optimal Route in the WSN. The diji-Huff method is able to forward the information to the nodes with greater energy and offer secure transmission. Adaptive reinforcement learning initiated from the present state, the best rule can be a launch to raise the rewards' predictable value. ARL method computes the rewards' predictable value to select the forwarder by the node RSS, the energy, and the delay. The simulation outcomes illustrate that the ISFA approach improved intrusion sensor detection and minimized packet delay. In addition, it improves the network throughput and diminishes the packet losses in the WSN.

References:

1. Farooq, Y., Beenish, H., & Fahad, M. (2019, November). Intrusion detection system in wireless sensor networks-a comprehensive survey. In 2019 Second International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT) (pp. 1-6). IEEE.
2. Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., & Nazir, S. (2022). An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs. Sensors, 22(4), 1407.
3. de Araujo-Filho, P. F., Kaddoum, G., Campelo, D. R., Santos, A. G., Macêdo, D., & Zanchettin, C. (2020). Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment. IEEE Internet of Things Journal, 8(8), 6247-6256.
4. Yahyaoui, A., Abdellatif, T., Yangui, S., & Attia, R. (2021). READ-IoT: Reliable event and anomaly detection framework for the Internet of Things. IEEE Access, 9, 24168-24186.
5. Huang, X., & Wu, Y. (2022). Identify Selective Forwarding Attacks Using Danger Model: Promote the Detection Accuracy in Wireless Sensor Networks. IEEE Sensors Journal, 22(10), 9997-10008.
6. Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2019). An adaptive ensemble machine learning model for intrusion detection. IEEE Access, 7, 82512-82521.
7. Chindove, H., & Brown, D. (2021, December). Adaptive Machine Learning Based Network Intrusion Detection. In Proceedings of the International Conference on Artificial Intelligence and its Applications (pp. 1-6).
8. Zou, K., Ouyang, Y., Niu, C., & Zou, Y. (2012, September). Simulation of Malicious Nodes Detection Based on Machine Learing for WSN. In International Conference on Information Computing and Applications (pp. 492-499). Springer, Berlin, Heidelberg.
9. Lai, Y., Tong, L., Liu, J., Wang, Y., Tang, T., Zhao, Z., & Qin, H. (2022). Identifying malicious nodes in wireless sensor networks based on correlation detection. Computers & Security, 113, 102540.
10. Alavizadeh, H., Alavizadeh, H., & Jang-Jaccard, J. (2022). Deep Q-Learning based Reinforcement Learning Approach for Network Intrusion Detection. Computers, 11(3),41.
11. Umar, M., Wu, Z., & Liao, X. (2020). Mutual authentication in body area networks using signal propagation characteristics. IEEE Access, 8, 66411-66422.
12. Sajid, M. B. E., Ullah, S., Javaid, N., Ullah, I., Qamar, A. M., & Zaman, F. (2022). Exploiting Machine Learning to Detect Malicious Nodes in Intelligent Sensor-Based Systems Using Blockchain. Wireless Communications and Mobile Computing, 2022.
13. Grgic, K., Zagar, D., & Krizanovic Cik, V. (2016). System for malicious node detection in IPv6-based wireless sensor networks. Journal of Sensors, 2016.
14. Zhang, J., Qiu, X., Li, X., Huang, Z., Wu, M., & Dong, Y. (2021). Support Vector Machine Weather Prediction Technology Based on the Improved Quantum Optimization Algorithm. Computational Intelligence and Neuroscience, 2021.
15. Du, Y., Xia, J., Ma, J., & Zhang, W. (2021). An Optimal Decision Method for Intrusion Detection System in Wireless Sensor Networks With Enhanced Cooperation Mechanism. IEEE Access, 9, 69498-69512.
16. Kavitha, N., & Selvi, V. Supervised Machine Learning Classifier For The Detection Of Malicious Nodes In WSN, Journal of Analysis and Computation, pp.1-5, 2018.
17. Amouri, A., Alaparthy, V. T., & Morgera, S. D. (2020). A machine learning based intrusion detection system for mobile Internet of Things. Sensors, 20(2), 461.
18. Bartoletti, M., Lande, S., & Podda, A. S. (2017, April). A proof-of-stake protocol for consensus on bitcoin subchains. In International Conference on Finan-

cial Cryptography and Data Security (pp. 568-584). Springer, Cham.
19. Mohd, N., Singh, A., & Bhadauria, H. S. (2020). A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. Wireless Personal Communications, 111(3), 1999-2022.
20. Peng, D., Chen, W., & Peng, Q. (2013). TrustVis: visualizing trust toward attack identification in distributed computing environments. Security and Communication Networks, 6(12), 1445-1459.
21. Li, X., Zhou, F., & Du, J. (2013). LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. IEEE transactions on information forensics and security, 8(6), 924-935.