Reinforcement Learning for Intrusion Detection and Improving Optimal Route by Cuckoo Search in WSN

K.Sai Madhuri

Research Scholar, Department of Information Science and Engineering, Visvesvaraya Technological University,
Belagavi. Nagarjuna College of Engineering and Technology,
Research Centre, Bangalore, Karnataka, India
saimadhuri069@gmail.com

Dr. Jitendranath Mungara

Principal, Department of Computer Science and Engineering,
Nagarjuna College of Engineering and Technology, Bangalore, Karnataka, India

Abstract

Wireless Sensor Network (WSN) is a generally hopeful technology for several real-time applications due to its cost-effective, size, and distribution nature. WSN is a collection of sensor nodes spread in a great region such that the required information can be collected. However, sensor nodes are susceptible to attacks, for example, intrusion, hackers, defective hardware starting the physical incident, etc. Therefore, it is compulsory to defend a sensor node from an intrusion. If it brings attacked next, the information transmitted through the sensor may be wrong and lead to incorrect data analysis, leading to unnecessary outcomes. To solve these issues, Reinforcement Learning for Intrusion Detection (RLID) and Improving Optimal Route by Cuckoo Search is proposed. The Reinforcement Learning uses the repeating node classification for detecting the intrusion during the route discovery. Reinforcement learning evaluates the sensor node behaviour by the quality of the link, and it is computed by sensor node packet forward rate and node residual energy. Here, the repeating node classification method classified the intrusion sensor based on node-link quality. As a result, it can improve intrusion detection performance efficiently. Besides, the Cuckoo Search Technique (CST) is used to find the optimal forwarder for transmitting the data from sender to destination. The main objective of this work is to offer optimal routing and communicate the data via normal sensor nodes in WSN. The simulation platform and the obtained results are compared with the baseline protocol to prove the efficiency of our proposed approach.

***Keywords*: Wireless sensor network, Repeating node classification, Reinforcement Learning, Cuckoo search technique, Intrusion Detection.**

1. Introduction

WSNs attained fame as they can adjust to the updates in a physical setting, for example, pressure, temperature, sound, and pollution. The advantage of such structures is that they are flexible, suitable for isolated places such as mountain areas, seas, forests, and rural areas. WSNs have been extensively useful in various areas, for example, surroundings supervising, political, intelligent transportation military, industrial fields and agricultural also medical (sen et al. 2018). In WSN, intrusion denotes the trouble of observing and separating flows and performance from the usual behavior that can unfavourably crash the information security (Sun et al. 2015). Owing to the enormous development of Internet applications, the necessity for data security has enlarged multiple. Because a major defence of network structure, a Detection of Intrusion is accepted to adjust to energetically altering risk scenery.

Cryptographic key management is a complex system, and it is an expensive process. Pre-configuring plus cryptographic keying material is a precondition for transition link securing if indirect key validation is not accessible. This approach provides security to every intermediate node through authentication using Dij-Huff Approach (DHA). In this approach, the Huffman coding offers security, and all intermediate nodes provide security using the Binary Hop Count method. However, the Binary Hop Count method does not work better during a malevolent attack (Alghamdi et al. 2018). Trust management is measuring trust with properties which manipulate trust. Bayesian-based Trust Management Approach (BTMA) is used for detecting the intrusion. However, trust management creates several problems, for example, limitation of necessary valuation data, require of big data procedure, the demand of easy trust correlation appearance as well as the expectation of automation (Meng et al. 2017).

Machine Learning (ML) techniques can be functional to respond accordingly ML is a method in which repeatedly learns from the experience also plays lacking unambiguously programmed. ML computing procedure is well-organized, dependable as well as cost-effective (Patel and Jhaveri, 2015). ML makes an example through examining still extent composite data repeatedly, speedily also correctly. ML is mostly categorized into supervised, unsupervised learning, semi-supervised as well as reinforcement (Manikandan and Kumar, 2020).
Several supervised and unsupervised techniques have been invented through investigators from the regulation of ML. As a safeguard alongside these attacks, Detection of Intrusion is a vital concept in the WSN. Reinforcement learning (RL) is a type of ML, and it is essentially the idea of artificial intelligence. This type of learning is utilized for gathering information and predicts the data.

Generally, cuckoos are a family birds by distinctive method equated to other bird's type. A number of cuckoo bird's type rest eggs in shared nests; though, they may eliminate others' eggs to enlarge the formulating possibility of their own eggs. Other type utilize children parasitism process of laying their eggs in the other birds' nests or nest of host. The parasitic cuckoos are high-quality in sporting nests here eggs have just been place and their timing of placing eggs is extremely precise (Das et al. 2017). They place one egg in the host nest that will usually producing faster than the other eggs. While this occur, the unknown cuckoo would eliminate the non-hatched eggs from the nest through pushing the eggs out of the nest. This activities is intended at minimizing the possibility of the valid eggs from hatching. In addition, the unknown cuckoo baby bird can expand access to additional food through miming the name of the host baby bird. At a time, the host cuckoo identifies that one of the eggs is unknown. This situation, the cuckoo either obtains clear of the egg otherwise discard the nest also moves to make a fresh nest anywhere (Masoodi et al. 2018).

Work Contribution:

The contribution of this approach concentrate on three most important parts;

During the route discovery, the Reinforcement Learning uses the repeating node classification for detecting the intrusion sensors in the WSN.

Reinforcement learning evaluates the sensor node behaviour by the quality of the link. The sensor link quality is computed by sensor node packet forward rate and node residual energy.

The Cuckoo Search Technique (CST) is used to find the optimal forwarder for transmitting the data from source to destination.

The structure of this article consider the following divisions; section-II discusses the related works for ML, section-III proposed the RLIT methods, section-IV analyzes the simulation results and section-V presents the conclusion.

2. Related Works

The reinforcement learning technique is used to enhance the total capacity connections while assurances the severe communications delay as well as reliability. This approach using multi-agent deep Q-learning is the optimal rule that satisfies the multiple QoS desires (zhao et al. 2020). An anomaly-based Intrusion Detection approach is determined the intrusions through unsupervised and semi-unsupervised deep learning methods. Additionally, an Auto-encoder procedure is applied to recognize the unidentified attacks. This approach detects the usual data and anomaly data by support vector machine (Zavrak and İskefiyeli, 2020). Enhanced Network Anomaly Detection approach is used to examine the fitness function for detecting intrusion. In this approach, the application established a traffic description which intended to evaluate the intrusion. A class label is offered with every record that recognized the traffic of the network and, as usual, or intrusion. However, this approach can't examine deep learning to discover capable information depiction for detection issues (Naseer et al. 2020).
Key pre-distribution approaches contain secure connectivity through demonstrating pair-wise keys among nodes. In this approach, a linear programming to discover the imperfect secure link issues regarding its crash on lifetime, length of the path, size of the queue, and energy. Though, this approach increases the packet losses (Yildiz et al. 2016).
SVM-based ML technique is used to identifying the intrusion. In this approach, a linear programming-based hyper-ellipsoidal formulation provides flexibility. A one-class quarter-sphere SVM that detain the usual data vectors for every sensor node. Then review detail is distributed between the nodes that are utilized to recognize intrusion (Rajasegarar et al. 2010). Tripartite active learning technique is applied to remove arithmetical outliers since it is a lesser memory need and computational complexity. This approach efficiently detects the intrusion in the WSN. However, this approach increases the variance for intrusion detection (Zhu and Yang, 2019). The RL concept permits agents to resolve jobs via learning of trial-and-error. In long-term learning, RL agents must be capable of concern knowledge earned in the history to recent jobs they may meet in the future. The capability to forecast action effects may help this knowledge transfer (Chalmers et al. 2019).

A self-taught anomaly detection approach is a fusion of unsupervised also supervised ML. Initially, it applies unsupervised data to examine the models of observing the data. It allows a self-learning ability that rejects the necessity of earlier awareness of abnormal behaviors. Also, it can potentially notice unexpected intrusion. In addition, a self-taught method that transmits the patterns learned by classification module (Chen et al. 2019). Reinforcement learning is enhancing intrusion detection by sensor node behavior (Nagaraja et al. 2020). Feature transformation applies the Gaussian distance function to attain dimensionality decline to signify the unique input dataset (Mukherjee et al. 2011). An efficient anonymous authentication approach is used to enhance security and privacy. This approach forward secrecy, user anonymity as well as resistance to attack. This approach is used to detect the flooding, replay and poison attacks (Indira and Sakthi, 2021).

IDS using swarm optimization enhanced Artificial Neural Network is used for enhanced the network function. First dimensionality reduction is applied using Principal Component Analysis. This information is served to the Swarm Optimized for classification. This approach using grey wolf optimization technique to optimize the weights over several iterations. The accuracy of the system is represented as the cost operation. However, this approach increases the network delay (Vardhini and Mahalakshmi, 2020). Trusted Computing Group Specification Architecture approach is used to light weighted key encryption based certificate establishment as well as its authentication procedure through the different operational units (Ravindra and Shankaraiah, 2020).

3. Reinforcement Learning Technique based Intrusion Detection and Improving Optimal Route by Cuckoo Search Technique in WSN

In this approach, the WSN contains the number of sensor nodes that sense the surrounding information and transmit the recognized data to the base station. However, the intrusion sensor nodes presented inside the network and compromised the normal sensor nodes, then totally destruct the whole network. Thus, intrusion sensor node detection is an important factor. Here, Reinforcement Learning using the Repeating Node classification technique for detecting the intrusion in WSN is proposed.

Intrusion Sensor Detection:

Figure 1 shows the structure of the RLID approach. WSN contains different categories of nodes include infected nodes, known intrusion, and normal nodes. The node neighborhood matrix is used to calculate the node-link quality. The Link quality represents the connectivity strength among two nodes. The node-link quality calculation is given below.

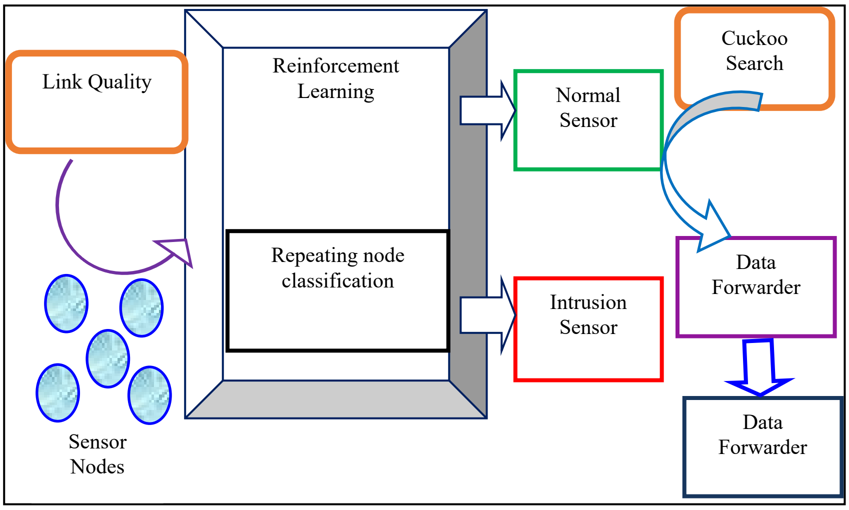

Fig. 1. Structure of RLID

$$link\ quality = Packet\ Forward\ Ratio * \mathrm{Re}sidual\ Energy \tag{1}$$

The link quality is stored in matrix M, and the following steps are executed in the repeating node classification method. In this scheme, the node Packet Forward Ratio and Residual Energy value represent among 0 to 1.

For example, the Neighborhood Matrix calculation among the node u and v is denoted by $L_{uv.}$ Let assume state variable for every node referred STV. Where STV=1 represents the known intrusion node, and STV=0 represents the rest of the intrusion node.

At time t, the node u is categorized as an intrusion if it is connected to threshold number of known intrusion,

$$STV_u = \Omega\left[\sum_j L_{uv} STV_v - TH\right] \quad \text{here} \quad \Omega[x]=1, x \geq 0, \quad \Omega[x]=0,\ x<0 \tag{2}$$

The value of threshold TH is computed below

$$\text{TH}=\frac{\text{Addition of whole entries in the matrix L}}{\text{Amount of Connections present among the nodes}} \tag{3}$$

Iteration t=1 to T_{Max}

$$STV_u(\text{t}+1) = \Omega\left[\sum_v L_{uv} STV_v(\text{t}) - TH\right] \tag{4}$$

Here, the node with iteration STV (T_{Max})=1 is classified as an intrusion in the network.

Nodes	1	2	3	4
1	0	0.85	0.76	0
2	0	0	0	0
3	0	0.71	0	0.87
4	0	0	0	0

Table 1. Neighbourhood matrix computation for quality of the link

For example, the 1st node packet forward ratio is 0.9, and the residual energy value is 0.95. The iteration calculation among nodes 1 to 2 is given below.

$$STV_u = \Omega[0.9 * 0.95(0) - 1]$$

$$STV_u = \Omega[0 - 1]$$

$$STV_u = \Omega[-1]$$

Here, $\Omega[-1] < 0$

Hence the node 2 is a normal node.

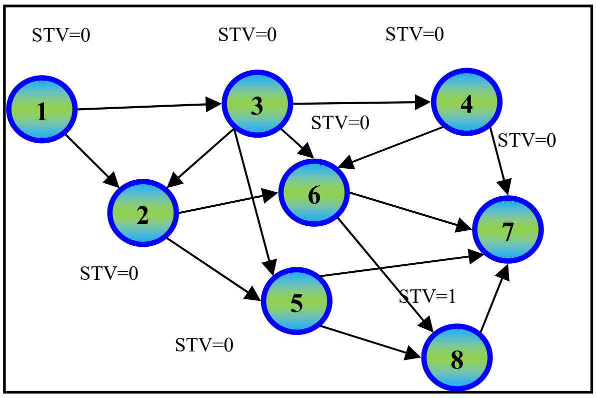

Fig. 2. Sample Diagram of RLID

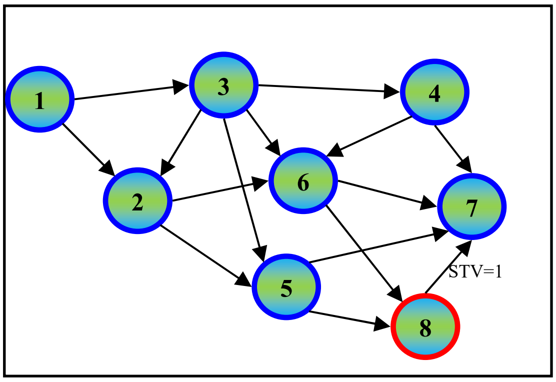

Fig. 3. RLID technique based Intrusion Detection (First Iteration)

Table 1 demonstrates the neighborhood matrix among nodes from 1 to 4. Figure 2 indicates the example diagram of RLID.

Here, k number of iterations is carried out to detect the intrusion nodes in the communication network. Node repeating classification-based intrusion detection scheme is shown in Figure 3. This method is considered the first iteration. In this scenario, node 8 is a Known intrusion node based on threshold. That is, the node 8 STV is 1. The other node's STV value is 0.

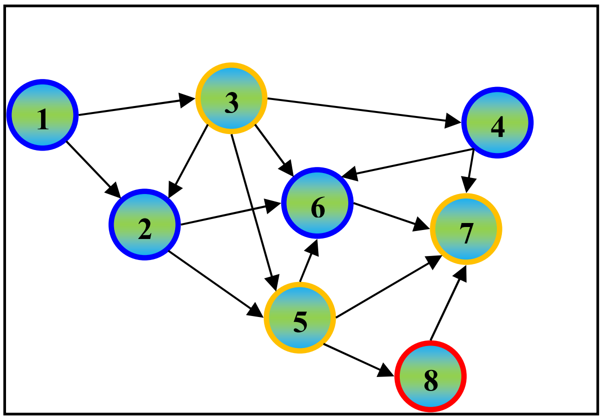

Fig. 4. RLID technique based Intrusion Detection (After First Iteration)

After the first iteration, nodes 3, 5, 7 are connected to intrusion node 8 is shown in figure 4. Also, the node 5 and 7 directly connected to intrusion node. In the second iteration, the STV of node 3 is 1. Thus the node is denoted by intrusion node in the network, is explained in figure 5. Here, node 7 is disconnected from 8.
Similarly, node 5 is detected as the intrusion based on the third iteration. Thus the nodes 1, 2, 4 disconnect the communication from nodes 3 and 5.

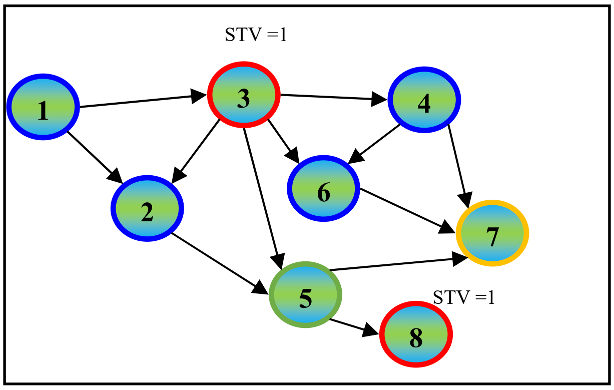

Fig. 5. RLID technique based Intrusion Detection (Second Iteration)

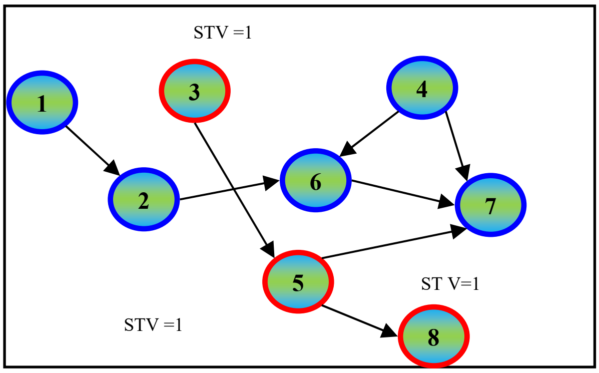

Fig. 6. RLID technique based Intrusion Detection (Second Iteration)

Finally, in figure 6, the nodes 3, 5, and 8 nodes are identified as intrusion nodes based on the repeating node classification method is done until Tmax. Here, intrusion node detection between nodes 1 to 8. Node 3, 5, and 7 isolated the Neighbourhood matrix is specified as input. The Neighbourhood matrix contains the quality of the link. It is determined as the lifetime of links present among two nodes. The node is considered as intrusion if the node has the connection with the threshold number of intrusion. Through applying IDS in the repeating node intrusion node.

Optimal Route Formation:

Cuckoo search Technique (CST) is a nature-inspired algorithm formulated by imitation of cuckoo birds. While functioning with CS, it is significant to correlate potential solutions with cuckoo eggs. Cuckoos generally lay their enriched eggs in other cuckoos' nests with the expectation of their off-springs being increased through proxy parents. There are times while the cuckoos determine which the eggs in their nests do not belong to them, in those situation the foreign eggs are either thrown out of the nests otherwise the complete nests are discarded. The CS optimization technique is fundamentally established on the following three rules:

- Every cuckoo chooses a nest arbitrarily and rests one egg in it.
- The optimal nests with great quality of eggs will be accepted over to the next generation.
- For a predetermined number of nests, a host cuckoo can determine a unknown egg with a possibility p ϵ [0,1]. This situation, the host cuckoo can either remove the egg otherwise discard the nest and construct a new one somewhere else.

The final rule can be approximated through replacing a portion p of the n host nests through a new nests. The fitness of a solution can merely be relative to the goal function value. The objective is to utilize the new and potentially optimal solution to substitute a worst solution in the nest.

Optimal Route Formation Algorithm

```
Task of Objective f (y), $y= (y_1, y_2 \ldots\ldots y_d)^t$
Make n host nests initial population $y_i$ ($i = 1, 2...n$)
While (t < Max Generation)
Obtain a cuckoo i arbitrarily;
Measure its fitness;
Select a nest among n j arbitrarily;
Measure its fitness;
If ($Fit < Fit_j$)
Restore j through the recent solution;
End
A portion of P of poorer nests are discarded and
Recent ones are form at new positions;
Maintain the optimal solutions;
Category the solutions and discover the present optimal;
End while
```

In this approach, the CST method is compute the fitness function by node delay value, distance value and consumed energy value. The optimal fitness function is selected through the node with minimum delay value, minimum distance value and minimum energy utilization. Thus, the lowest fitness value node is selected as a data forwarder node. Energy, delay and distance computation is given below.

Energy is the preliminary necessity for WSNs in supporting several actions, with signal recognition, dispensation, communication, and idle listening. WSN lifetime mainly establishes on the node remaining energy. In WSN, function node energy reducing, so the chosen of the best routing technique influence for energy necessity. Sensor node consumed energy calculation is given below.

$$Consumed\ Energy = Initial\ Energy - \Pr esent\ Energy \tag{5}$$

Sensor nodes with greater energy ratio have a greater possibility of being incorporated in the most favorite route. The delay computation between node i and node j is given below.

$$Delay = \mathrm{Time\ of}\ Packet\ \mathrm{Re}ceived - Time\ of\ \ Packet\ Sent \tag{6}$$

The distance computation between nodes i and j is given below.

$$Dis\tan ce = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \tag{7}$$

Fitness function based on CST is given below.

$$Fit = \frac{CE + Delay + Dis\tan ce}{3} \tag{8}$$

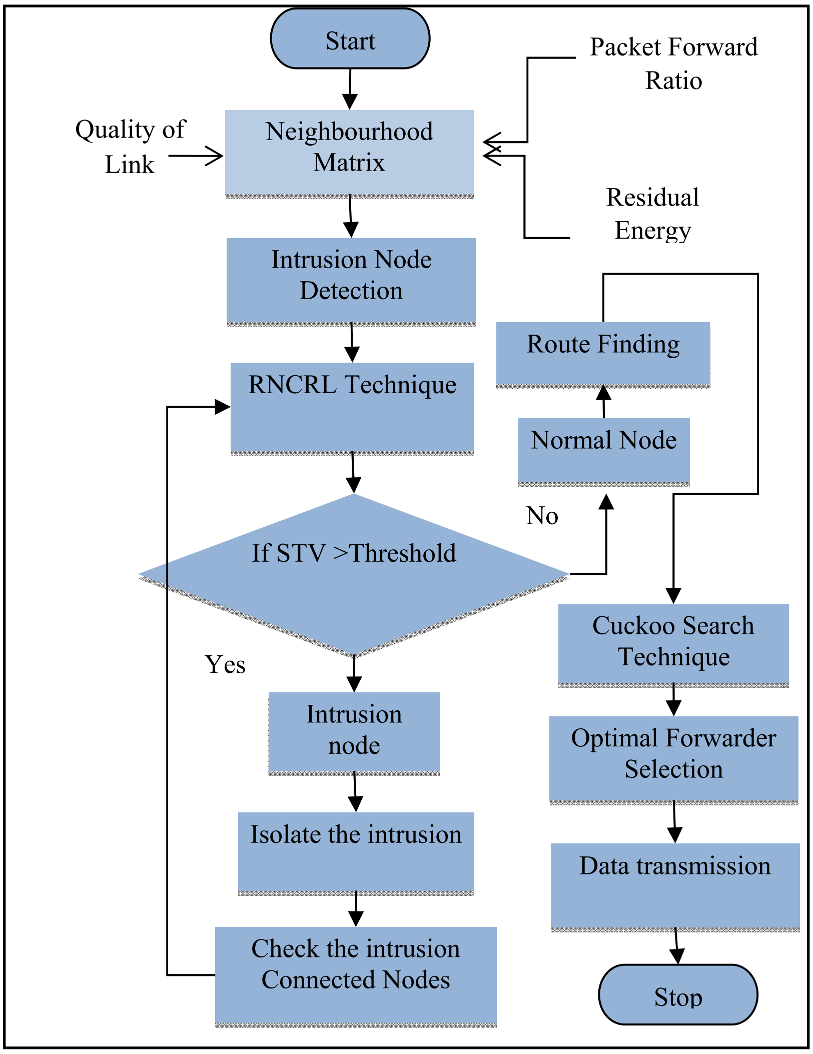

Fig. 7. Flow Diagram of RLID

Figure 7 demonstrates the flowchart of the RLID approach. As shown in Figure 7, in the RLID, the classification method, the nodes are classified as the intrusion node and non-intrusion node. The STV will adjust actively along with the node-link quality. The STV is allocated as 1 for the recognized intrusion, and 0 denotes the rest of the nodes. The STV is updated through the connection presents with the intrusion node. Sensor Node with STV= 0 is a normal sensor, and the node with STV=1 is an intrusion sensor. The RLID is utilized for filtering out the normal sensor nodes that turn into the intrusion sensor node in the WSN. In addition, the CST is used for select the optimal forwarder by the node consumed energy, node delay and node distance. The lowest fitness function value node is selected as a data forwarder. Finally, the sender transmit the data through reliable forwarder in the WSN.

4. Experimental Results

We simulate a WSN system where 100 sensor nodes are distributed arbitrarily in a 400x500 m region. Network simulator-2.35 is a suitable and efficient tool for evaluating intrusion detection. RLID approach analyzes the security against the BTMA. The quality of service parameters like detection ratio, false-positive ratio, and false-negative ratio, delay, and throughput is analyzed in the network performance.

4.1. *Delay Analysis*

The delay is usually defined for the time in use to treat the packets transmitting them from the sender sensor node to the receiver sensor node. It is computed via the formula 6.

In WSN, the delay of a sensor node is shown in figure 8 for BTMA and RLID approaches. Additional delay is created by the intrusion sensor node. The RLID approach detecting the intrusion and isolates them; thus, the delay is minimized. But, the BTMA approach using trust management probability that is not identified intrusion nodes accurately; as a result, it makes additional delay in the network.

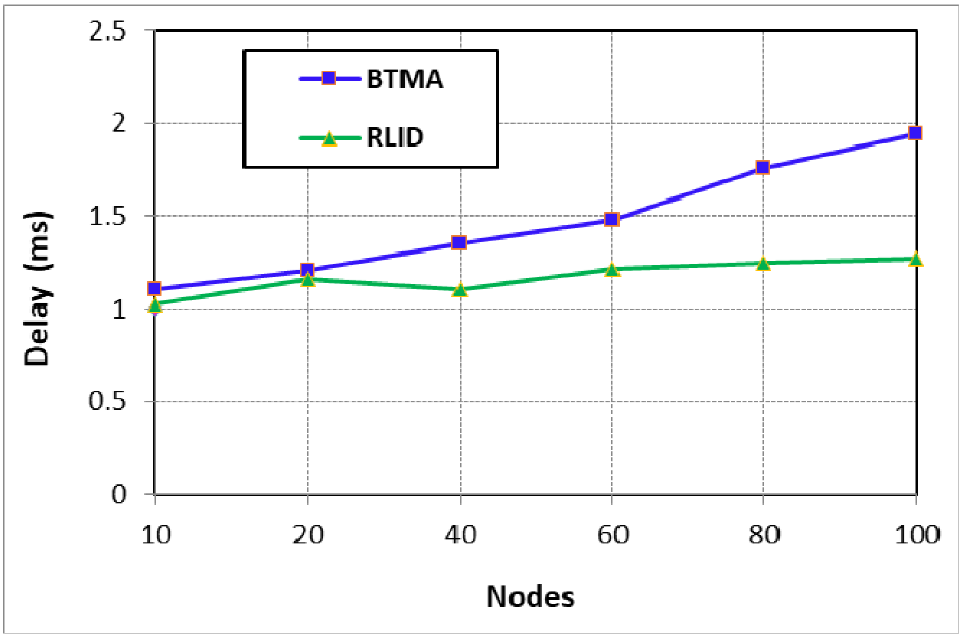

Fig.8. Delay of BTMA and RLID

4.2. *Throughput Analysis*

Figure 9 proves the throughput among BTMA and RLID. It mentioned that the amount of packets received efficiently to every 1000 packets for 10 to 100 sensor nodes. In BTMA, the sensor node count raises the throughput ratio is decreased but RLID approach the nodes count increases the ratio of throughput also approximately same level. Since the RLID approach detects the intrusion perfectly thus minimizes the packet loss. In addition, CST also forward the data through the optimal forwarder in the WSN.

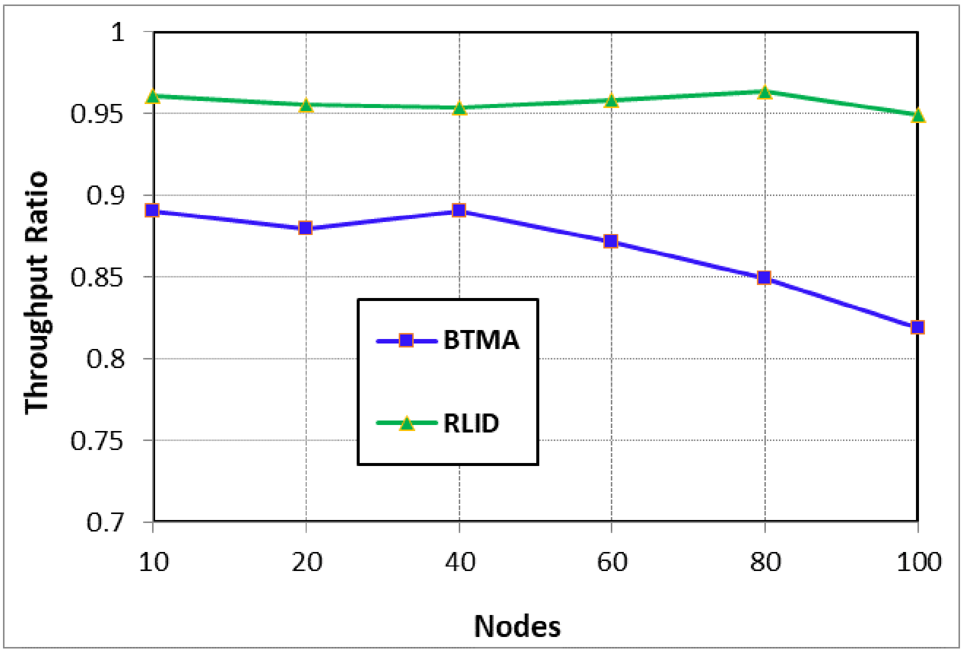

Fig. 9. Throughput of BTMA and RLID

4.3. *Detection Ratio (DR) Analysis*

It is mentioned as the relationship among the amount of properly-recognized intrusion and the amount of intrusion. It is computed by the formula given below.

$$DR = \frac{Amount\ of\ \ properly\ identified\ \mathrm{int}\,rusion}{Whole\ Amount\ of\ \ \mathrm{int}\,rusion} \tag{9}$$

The figure explains the DR of the BTMA and RLID. From this Figure, the DR of the RLID is superior to the RLID based on the number of sensor nodes. This is because the RNTM checks the intrusion efficiently. But, the BTMA approach increases the sensor node; the detection ratio performance is decreased in the WSN.

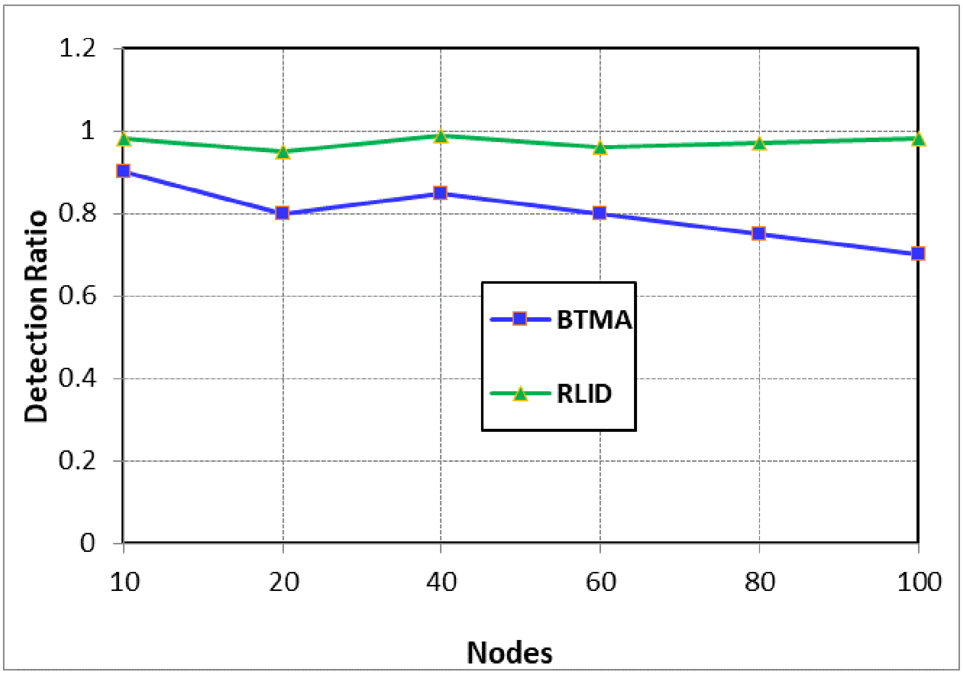

Fig.10. Detection Ratio of BTMA and RLID

4.4. *False-Positive Ratio Analysis*

It is defined as the relationship among the amount of usual sensor nodes which are improperly classified as intrusion and the whole amount of usual sensor nodes. It is specified as the formula is given below.

$$FPR = \frac{Amount\ of\ \mathrm{Im}\ properly\ identified\ Intrusion}{Amount\ of\ Usual\ Nodes} \tag{10}$$

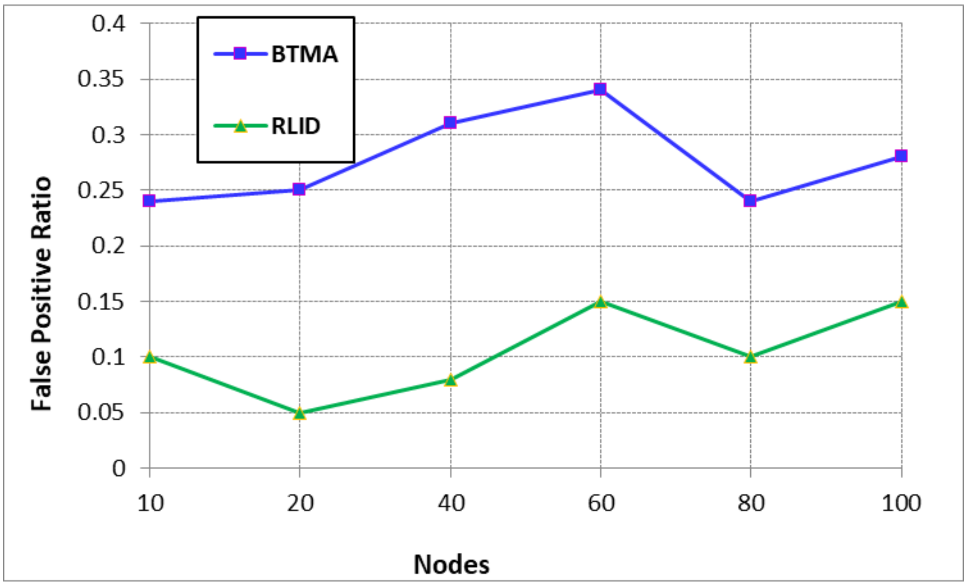

Fig. 11. False Positive Ratio of BTMA and RLID

Figure 11 explains the FPR of BTMA and RLID. The FPR of the RLID is lesser than BTMA since RNTM checks the intrusion sensor repeated iteration. But, BTMA detects the intrusion by the probability of node behavior. It is chosen to utilize an approach with the lesser FPR to make certain better security.

4.5. *False-Negative Ratio Analysis*

It is defined as the ratio among the amount of intrusion nodes which are improperly categorized as usual sensor nodes and the whole amount of usual node. It is defined as the formula given below.

$$FNR = \frac{Amount\ of\ \ improperly\ identified\ as\ a\ usual}{Whole\ Amount\ of\ \ Normal\ Nodes} \qquad (11)$$

Figure 12 explains the FNR of the BTMA and RLID approaches. From this Figure, the FNR of RLID is lesser than the BTMA approach because the sensor nodes are checked by a number of iterations. In addition, this approach select the data forwarder by CST fitness function. Thus, this approach minimized the false negative rate.

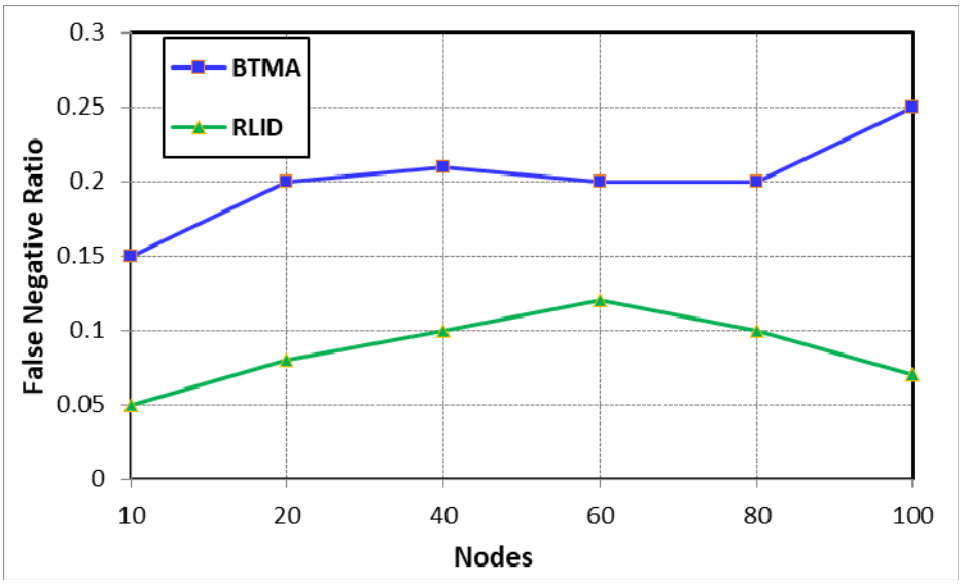

Fig. 12. False Negative Ratio of BTMA and RLID

5. Conclusion

In this paper, we examined the Reinforcement Learning Technique based Intrusion Detection and Improving Optimal Route by Cuckoo Search in a WSN. Reinforcement learning allows sensor node behavior by the quality of the link, and it is computed by packet forward rate and node residual energy. During route discovery, the Repeating node classification method is used for detecting the intrusion sensor perfectly. Here, the repeating node classification method classified the intrusion sensor based on node-link quality. Besides, the CST is used to discover the optimal route from source to destination. CST fitness function is computed by node consumed energy, node delay and node distance. The simulation results explain to make possible the RLID has enhanced the intrusion sensor detection and raises the throughput in the WSN. In addition, this approach minimized the false-positive ratio and false-negative ratio in the network. In the future, we have investigates the issue of CST early convergence.

References

[1] Sen, S.; Koo, J.; Bagchi, S. (2018). TRIFECTA: security, energy efficiency, and communication capacity comparison for wireless IoT devices. IEEE Internet Computing, **22**(1), pp. 74-81.

[2] Sun, W.; Song, X.; Wang, F. (2015). Energy-balanced clustering routing protocol based on task separation in wireless sensor networks. In 2015 8th International Conference on Biomedical Engineering and Informatics (BMEI) pp. 778-782. IEEE.

[3] Albert Alghamdi, T. A. (2018). Secure and energy-efficient path optimization technique in wireless sensor networks using DH method. IEEE Access, 6, 53576-53582.

[4] Meng, W.; Li, W.; Su, C.; Zhou, J.; Lu, R. (2017). Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data. IEEE Access, **6**, pp.7234-7243.

[5] Patel, N. J.; Jhaveri, R. H. (2015). Detecting packet dropping nodes using machine learning techniques in Mobile ad-hoc network: A survey. In 2015 International Conference on Signal Processing and Communication Engineering Systems, pp. 468-472. IEEE.

[6] Zhao, D.; Qin, H.; Song, B.; Zhang, Y.; Du, X.; Guizani, M. (2020). A Reinforcement Learning Method for Joint Mode Selection and Power Adaptation in the V2V Communication Network in 5G. IEEE Transactions on Cognitive Communications and Networking, **6**(2), pp. 452-463.

[7] Zavrak, S.; İskefiyeli, M. (2020). Anomaly-based intrusion detection from network flow features using variational autoencoder. IEEE Access, **8**, pp. 108346-108358.

[8] Naseer, S.; Saleem, Y.; Khalid, S.; Bashir, M. K.; Han, J.; Iqbal, M. M.; Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. IEEE access, **6**, pp. 48231-48246.

[9] Yildiz, H. U.; Ciftler, B. S.; Tavli, B.; Bicakci, K.; Incebacak, D. (2016). The impact of incomplete secure connectivity on the lifetime of wireless sensor networks. IEEE Systems Journal, **12**(1), pp. 1042-1046.

[10] Rajasegarar, S.; Leckie, C.; Bezdek, J. C.; Palaniswami, M. (2010). Centeredhyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks. IEEE Transactions on Information Forensics and Security, **5**(3), pp. 518-533.

[11] Zhu, Y.; Yang, K. (2019). Tripartite active learning for interactive anomaly discovery. IEEE Access, **7**, pp. 63195-63203.

[12] Chalmers, E.; Contreras, E. B.; Robertson, B.; Luczak, A.; Gruber, A. (2017). Learning to predict consequences as a method of knowledge transfer in reinforcement learning. IEEE transactions on neural networks and learning systems, **29**(6), pp. 2259-2270.

[13] Chen, X.; Li, B.; Proietti, R.; Zhu, Z.; Yoo, S. B. (2019). Self-taught anomaly detection with hybrid unsupervised/supervised machine learning in optical networks. Journal of Lightwave Technology, **37**(7), pp. 1742-1749.

[14] Nagaraja, A.; Boregowda, U.; Khatatneh, K.; Vangipuram, R.; Nuvvusetty, R.; Kiran, V. S. (2020). Similarity-Based Feature Transformation for Network Anomaly Detection. IEEE Access, **8**, pp. 39184-39196.

[15] Mukherjee, P.; Sen, S. (2011). Comparing reputation schemes for detecting malicious nodes in sensor networks. The Computer Journal, **54**(3), pp. 482-489.

[16] Manikandan, S and Kumar, S.B. (2021) Energy Efficient Clustering Algorithm For Mobile Cluster Heads To Enhance The Lifespan Of Wireless Sensor Network, Indian Journal of Computer Science and Engineering, **12**(3), pp. 605-617.

[17] Indira, K and Sakthi, U. (2021) An Efficient Anonymous Authentication Scheme to Improve Security And Privacy In SDN Based Wireless Sensor Networks, Indian Journal of Computer Science and Engineering, **11**(1),pp.27-35.

[18] Vardhini, K.K and Mahalakshmi, T.S. (2020). Implementation of Swarm Optimized Artificial Neural Network for Network Intruder Detection and Attack Classification, Indian Journal of Computer Science and Engineering, **11**(2).

[19] Ravindra, S and Shankaraiah, (2020). MAPSDN-EESC: A Modeling Of Authentication Process For The Software Defined Network Using Encrypted Entity Scheme Cryptography, **11**(4).

[20] Das, S.; Barani, S.; Wags S.; Sonavane S.S. (2017) Optimal Clustering And Routing For Wireless Sensor Network Based On Cuckoo Search. International Journal of Advanced Smart Sensor Network Systems, **7**(2/3), pp. 1-13.

[21] Masoodi, I.S.; Dar, M.A..; Banday, M.T. (2018) Energy Efficient Routing in WSNs Based on Dynamic Cuckoo Search Algorithm, IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology, pp. 2514-2517.

Authors Profile

K. Sai Madhuri is currently Pursuing Ph.D. in the Department of Computer Science at VTU, Belagavi under the Research Centre of NCET, Bangalore. She received her M.Tech degree in Computer Science from JNTUH, Hyderabad in 2010. Since 2010, she is working as an Assistant professor in many of reputed colleges. Her Research interest include in IDS in Network using latest Machine and Deep Learning techniques, Artificial Intelligence, Data science etc. Reviewed and Handled many Research papers on latest techniques and guided many students in the same technology.

Dr. Jitendranath Mungara, Principal & Prof. is a dynamic, team spirited, and performance driven engineering professional and Educational Leader in the fields of Academic Administration, Research, Quality Assurance, Educational Consultancy and also Extension Activities. He completed many Technical and management Proficiency Certificate courses in USA. He is good in SQA & TQM Audits. He taught many MOOC Courses to the faculty and students under the train the trainer’s concept. He is author of over 150+ scholarly research/ review papers, including 100+ reputed and peer reviewed international journal (Scopus/SCI/UGC/IEEE/ Springer/WOS) papers with 310+ Citation index, 10+ h-index and 10+ i10 index. He has won several research paper awards in different National and International conferences and symposiums. He is double Ph.D. holder from different universities and has filed 6 patents and published 3 Patents. He is Member in many leading professional Societies and Forums. He is reviewer and editorial board member/ Advisory board for many reputed/ UGC approved International/ National Journals and has published 3 Technical books in the field of Computer Engineering. He delivered many Keynote Speeches and Chaired Technical sessions in many International, National Conferences and Symposiums.