Complex Leap Collection-based CNN Method Using Jamming Detection in Wireless IoT Networks

Y.M.Blessy[1], V.S.Prabhu[2], M.perarasi[3], J.Jasmine Hephzipah[4], B.Sarala[5], M.S.Kavitha[6], T.D.Subha[7]

[1]Department of Electronics & Communication Engineering, R.M.K. Engineering College, RSM Nagar, Kavaraipettai-601206,Email:ymb.ece@rmkec.ac.in
[2]Department of Electronics & Communication Engineering, R.M.D. Engineering College, RSM Nagar, Kavaraipettai-601206,Email:vsp.ece@rmd.ac.in
[3]Department of Electronics & Communication Engineering, R.M.K. Engineering College, RSM Nagar, Kavaraipettai-601206 , Email:mpi.eee@rmkec.ac.in
[4]Department of Electronics & Communication Engineering, R.M.K.Engineering College, RSM Nagar, Kavaraipettai-601206,Email:jazzjoell@gmail.com
[5]Department of Electronics & Communication Engineering, R.M.K. Engineering College, RSM Nagar, Kavaraipettai-601206,Email:bsa.ece@rmkec.ac.in
[6]Department of Electronics & Communication Engineering, R.M.K. Engineering College, RSM Nagar, Kavaraipettai-601206, Email:msk.eee@rmkec.ac.in
[7]Department of Electronics & Communication Engineering, R.M.K. Engineering College, RSM Nagar, Kavaraipettai-601206, Email:tdsubha2010@gmail.com

Corresponding Author: Y.M.Blessy
Email: ymb.ece@rmkec.ac.in

Abstract

Jamming attack is one of the most threat-based issues in wireless sensor networks in the Internet of Things (IoT). Most of the jamming detection mechanisms are used for low-range detection. Jamming attacks are primarily performed in a time interval and signal strength based on IoT WSN. The problem with existing jamming detection solutions using localized jamming detection systems is that it needs to be lead to detect the jamming attacks adequately. The cost for node communication and overhead is the problem in IoT WSN. The proposed will use the Deep learning-based Complex Leap Collection based CNN method to detect the jamming attack. The Jamming detection mechanism enhances the passive, non-node-centric, and low-overhead network. In WSN, the quantum search algorithm finds the energy level in multiple nodes. The most practical algorithm is used WSN to find time intervals and signal lengths. The N-to-N multipath routing algorithm finds various routes to send several nodes in IoT WSN.

Keywords: Deep learning-based Complex Leap Collection based CNN method, the quantum search algorithm, N-to-N multipath routing algorithm.

1. Introduction

The various wireless-based IoT application communicates with each other nodes. The user needs better energy levels and increased signal strength. WSN has n number of sensor nodes which is efficient for detecting and communicating in its way. It collects information from the nearest node and can perform automatically through wireless, less energy, single or multi-hop transmission, sending and receiving information between nodes. These nodes have more data asset ability and can use different situations, times, and locations. It accommodates natural environments such as medical practice, traffic management, and user-friendly monitoring. The WSNs have been needed in the multipath way of routing data transmission. The wireless-based IoT applications are required for multipath routing because of fast-running applications. The users quickly allow the IoT-based application to work simultaneously because most wireless applications run slowly. Then the reason for not having proper routing methods. The N-To-N multipath routing algorithm has been using the appropriate method applied there. The previous application compared to better the proposed system.

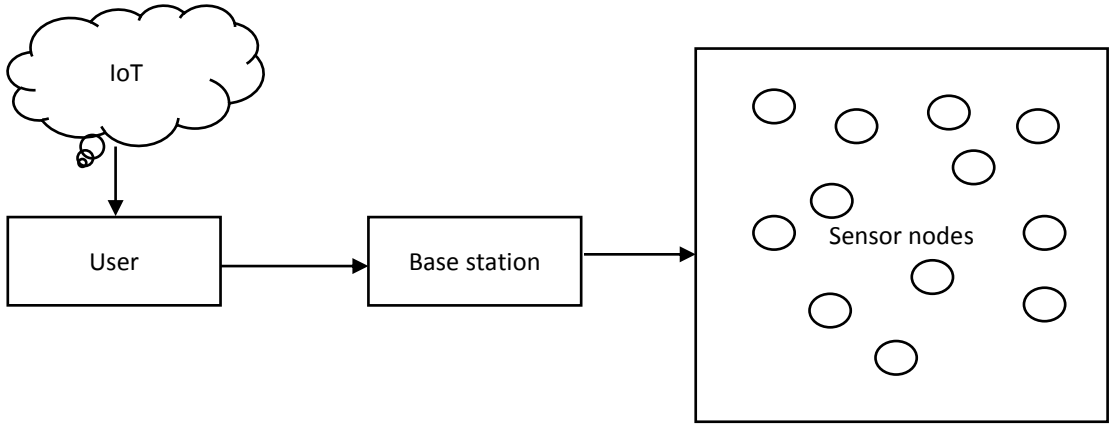

Figure.1 The General architecture of WSN with IoT

Figure. 1 define the general architecture of wireless sensor with IoT. The user transmits the data to the internet, but more users communicate simultaneously. In the send-to way of the base station (BS), BS receives user data, then after data send to multipath routing, finally receives data to the end of the user.

2. Related Works

This proposal using machine learning-based Delimitated Anti-Jamming protocol has used vehicular traffic environments. It mainly focuses the vehicular network jamming detection. The jamming detection and attack are primarily based on signal strength due to jamming attack detection for this method. The Cat-boost algorithm is used for a vehicular location to find the networks [1].

This is VANET and WSN-based networks jamming attack detection in IOT. The existing system uses a low range of speed to transmit the data of VANET communications. It is the low power supply for the networks because packet transmission slowly and then jamming attacks has been detected on the networks the best solution for Hierarchical, trust-based, multi-hop protocols [2].

The attack detection on Delay Tolerant Networks (DTNs). Here the Delay Tolerant Networks (DTNs) have been detected in the Black hole attacks. The proposed system uses Opportunistic Network Environment attacks based on Spray and Waits as the base routing protocol. It is one of the Potential Threats (PT) established security protocol bases [3].

It is a wireless sensor network that mainly detects Denial of Service attacks. These attacks disturb the network services and communications in WSN. The proposed system to present the new Artificial Bee Reverse Tracing (ABRT) approach is introduced. It works for data security bases [4].

Manet is one of the mobile-based applications that are interfaces there. More Problem for Manet is prone to interception and manipulation with node identity and routing optimization. The proposed uses the CRCMD&R (Cluster and Reputation-based cooperative malicious node Detection and Removal) scheme. It is used for the optimization of easy routing [5].

It is one of the wireless sensor networks; it is so many problems with wireless sensor networks, and most of the problem is intrusion detection system. One more problem is the user behavior analysis of wireless sensor networks. The proposed method uses a simple dynamic statistical model to be solved the existing problems [6].

In wireless sensor networks, the primary problem is the intrusion detection system (IDS). The current plan has introduced the framework-based architecture approach to address all networking issues. [7].

One of the essential routing networks is multi-hop routing wireless sensor networks. Most problems are jamming attacks on networks, packet delivery ratio, and data communications on wireless sensor networks. The proposed system of MAC and physical models are used to resolve the problems in wireless sensor networks [8].

IoT is famous for wireless sensor networks. The main problem is energy and jamming attacks; the attacker hacked the networks the total energy is entirely wasted. To resolve using maximize the attacker energy efficiency (AEE) in secure IoT. [9].

This is one of the IoT-based wireless sensor networks, the network detection on attacks and secondary overall network analysis of the user behaviors; they're a significant problem of jam attack and energy consumption. The proposed system has been offered for the green design method. With this method, the overall situation was 45% solved on the networks [10].

This method is one of the IoT-based wireless applications. Most problems are jamming attacks and network interfaces; both problems are solved using an Electronically Steerable Parasitic Antenna Radiator (ESPAR). This method has been translated for emergency support of the wireless sensor network [11].

IoT is a virtual network in WSNs, Securing ZigBee Communications against Constant Jamming Attack Using CNN. Here low bandwidth or the wireless application and jamming attack detection on wireless sensor network. The proposed system uses a new ZigBee receiver, leveraging MIMO technology-based jamming attack detection and accuracy [12].

It is an ad-hoc vehicle network with additional obstruction assaults on vehicle-to-vehicle and vehicle-to-vehicle correspondences, danger recognition, and impedance

assault discovery utilizing a regulated AI mode. This accuracy is 99.84% of remote sensor organizations. [13].

The most important problem is ratio jamming attacks; this attack appears to disrupt the packet transmission on the wireless spectrum. Here the proposed method of traditional anti-jamming methods has solved the overall problems [14].

This is IoT based on congestive networks with malicious nodes in the network. Here various interfaces with other nodes. At that time, jamming attacks are detected. The proposed system solves this using a Deep Auto Encoder Trust Model; this model finds out the jamming attacks and network interface problems [15].

IoT-based network communication systems, so many problems occur in the networks; one the problem is the denial of service attacks, jamming attacks, and spectrum-based attacks detection accuracy need. An existing system using machine learning methods could not correctly detect the correct accuracy, but the proposed approach to deep learning methods sincerely finds the accuracy [16].

IoT and VANETs-based wireless networks. The network performance is based on multi-input and multi-output communication simultaneously at that time, and the jamming attack has been detected there. The existing system does not see the attacks; the proposed methods of the MIMO OFDM system present a novel rate-reliability of a good performance of the jamming detection [17].

The devices using IoT-based applications run there, but sometimes applications run interruption of jamming attacks. They were running the application stopped suddenly. The existing system needs to be appropriately managed. The proposed method of Spectrum Assignment in Cognitive Radio Networks Using IoT Devices performs well in jamming detections [18].

The proposes of Intelligent Reflecting Surface (IRS) used for the green jammer. When a place jamming attack is detected, this system is processed for energy-based jamming detection and power signal problems. The proposed method of green jamming is generated to detect the attacks [19].

2.1 Problem Definition

The main problem of the jamming attack is the following statements explain here. Jamming attacks are primarily performed in a time interval and signal strength based on IoT WSN. The problem with existing jamming detection solutions using localized jamming detection systems is that it needs to be lead to detect the jamming attacks adequately. The cost for node communication and overhead is the problem in IoT WSN.

2.2 Objective of the Paper

The paper's main objective is jamming attack detection. Using the following statements, explain the detection attacks; the ideas are deep learning-based Complex Leap Collection-based CNN applied for detecting the jamming attack. The Jamming detection mechanism enhances passive and low-overhead networks. In WSN, the quantum search algorithm finds the energy level in multiple nodes. The most practical algorithm is used WSN to find time intervals and signal length. The N-to-N number

of the multipath routing algorithm is used for finding various routes to send the number of nodes in IoT WSN

3. Proposed Methodology

The IoT with wireless applications is most important in the real world. The IoT-based wireless application is an essential part of human life. The cost for node communication and overhead is the problem in IoT WSN. The proposed will use the Deep learning-based Complex Leap Collection based CNN method to detect the jamming attack. The Jamming detection mechanism enhances passive, non-node-centric, and low-overhead networks.

In WSN, the quantum search algorithm finds the energy level in multiple nodes. The most practical algorithm is used WSN to find time intervals and signal length. The N-to-N multipath routing algorithm finds various routes to send several nodes in IoT WSN, the critical problem of jamming attacks in IoT-based wireless applications. The previous system could find a low level of jamming detection in WSNs. Here find out the accuracy of energy consumption, maximum throughput, packet delivery ratio, jamming detection, and delay performance. Figure. 2 define the proposed architectures of WSN with IoT.

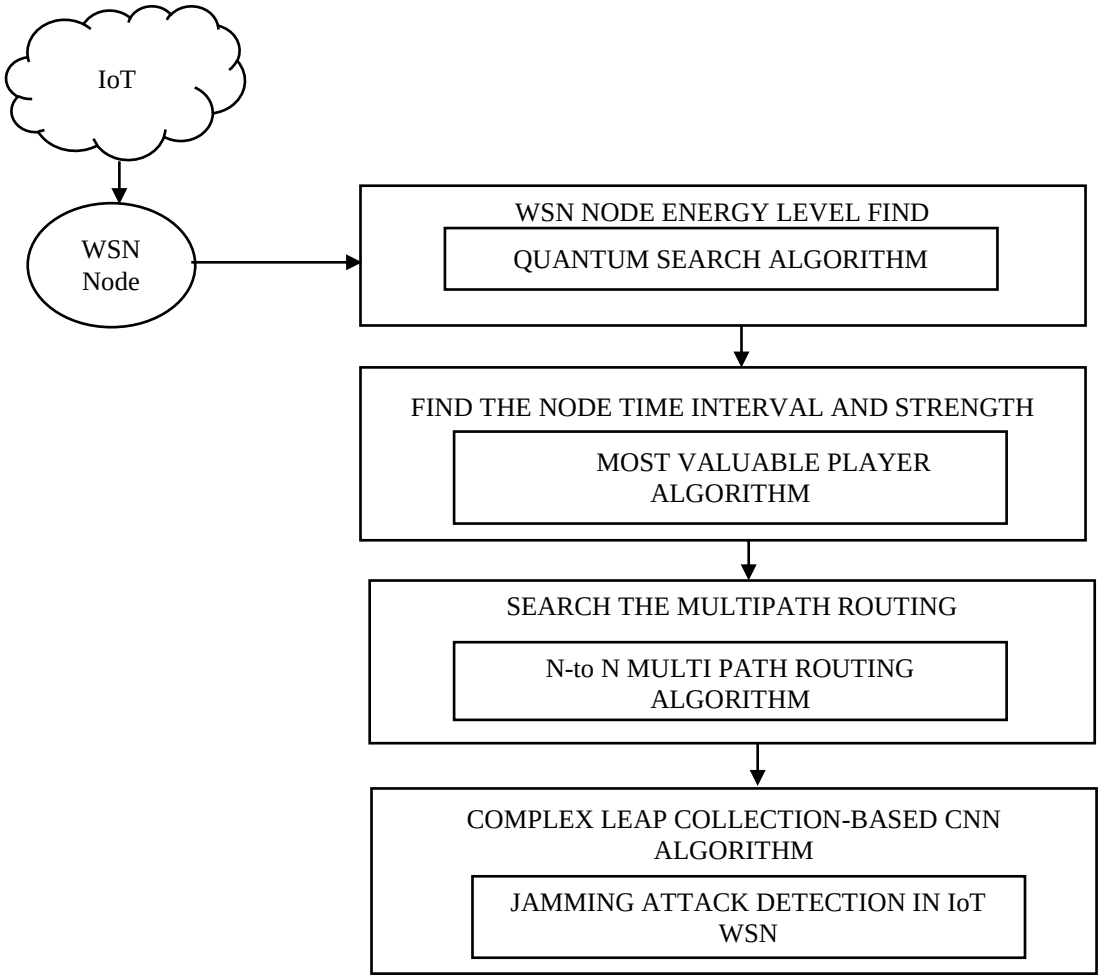

Figure. 2 Proposed architecture

A. Network node deployment

In IoT-based WSN, more than 100 nodes have been created randomly, and from that starting node, the packet data can be transmitted to the end node. Communication takes place based on the origin node to the end node. It also clearly shows the node simulation and information exchange taking place using simulator tools. Another process called NS2 is implemented. It collects network overhead, delays, maximum throughput and energy consumption, and network-related information.

B. WSN Node Energy Level

It would help to find the energy level of each node. Each node takes some energy for data transmission. Data transfer to each node needs more feeding and gain interference detection based on IoT; network overhead might be a find there. A Quantum search algorithm is used to find the energy levels of each node. It is the network for the best IOT wireless application support. It is the network for the best IOT wireless application support. The energy model is as follows:

$$E_{tx}(l,d) = \begin{cases} l * E_{elec} + l * \in fs * d^2; d < d_0 \\ l * E_{elec} + l * \in fs * d^4; d < d_0 \end{cases} \quad (1)$$

For receiving the data to explain the ratio

l -bit message for a distance d,

$$E_{tx}(l) = l * E_{elec} \quad (2)$$

E_{elec} is the electronic energy t

E_{tx} (Energy level using one frame)

$$E_{elec}(l) = E_{tx}(m-1)ch + l * E_{elec}d^2 + E_{tx}(l) + \in_{mp} + d^4 \quad (3)$$

Many nodes have been distributed in the same types; the k calculates the intermediate node $m = \frac{N}{k}$. Here split the energy node and the number of energy nodes

$$E_{elec} = lE_{elec} + l * \in fs * d^2 \quad (4)$$

MVPA (the most valuable player algorithm) is one of the most recent improvement calculations. Sporting events influence it. It is utilized in a variety of fields, consistently producing excellent outcomes. A relative report was done between improvement calculations propelled by games, including MVPA. In electromagnetism, the MVPA came first for unimodal problems and second for multimodal issues, along with two other algorithms. It was utilized for proficient energy administration in a microgrid with discontinuous environmentally friendly power and capacity.

Algorithm 1. MVPA pseudocode.

Input node N;

Initialization

for fixture=1: MaxNFix

for i = 1:TeamsSize

TEAMi = Select the team number i from the league's teams

TEAMj = randomly select another team j from the league's teams where j 6= i

TEAMi = TEAMi + rand × (FranchisePlayeri − TEAMi) +2 × rand × (MVP − TEAMi)
If TEAMi wins against TEAMj
TEAMi = TEAMi + rand ×
TEAMi − FranchisePlayerj
Else
Node Time Interval and Strength
TEAMi = TEAMi + rand × FranchisePlayerj − TEAMi
End if
Check if there are players outside the search space
End for
End for`
Here, the algorithm (TEAMi = TEAMi + rand × FranchisePlayerj – TEAMi) is used for finding multipath routing.

C. N-To N Multi Path Routing Algorithm

The consequences of our restoration show that the proposed N-to-N multipath detecting convention is exceptionally proficient and that the mixture of information assortment conspires, given it gives an additional solid and secure information assortment administration in remote sensor organizations. It is the creation of multipath routing protocols that are both effective and efficient. Techniques for multipathing between a single pair of sources and destinations were discussed. This category encompasses the majority of current multipath routing protocols. A brand-new N-to-N multipath discovery protocol is presented in this article as a response to the communication pattern in a sensor network. We offer the circulated convention in this segment and assess its path-finding abilities.

Algorithm 1: N-To N Multi Path Routing Algorithm
/*All unfinished flow in the network*/
Data: F= TEAMi
Link_state_old /*old network topology */
Result: Link_state_new
Link_state_new = f; /*Initialization*/
while f in F do
Calculate f current time delay, available
bandwidth and packet loss rate;
/* path (f) is the path transmission function*/
if the Link is in the path (f), then
if f is in Link_state_old, then
Calculate the available bandwidth;
else
Routing performance
else
Rerouting;

Here in this algorithm, find out the time delay, energy consumption, pack loss rate, and routing performance are calculated

D. Jamming Attack Detection in IoT WSN

A form of deep learning neural network architecture based on a collection of intricate hops inspired by computer vision-friendly CNN techniques. Study the impact of the duration of the interference on the network's performance, and evaluate how the detection algorithm works. The classification of interference attack detection can be seen in the following diagram.

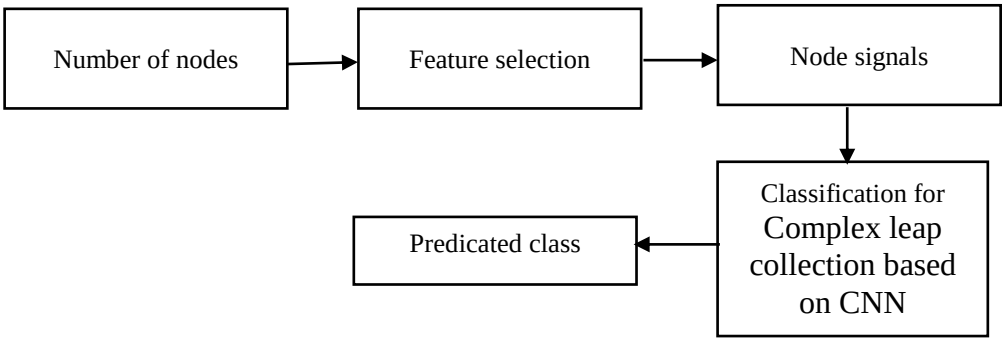

Figure.3 Classification for Complex leap Collection based CNN

Figure.3 defines the classification of node signals. The first collects the movements, and the feature selection selects signals and then applies the classification methods. Finally, find the jamming attack detection performance calculated using various methods.

Classification for Complex leap Collection based CNN

$$\sum f\,(E_{elec)} = lE_{elec} + l * \in fs * d^2 \quad (5)$$

$$f(E_{complex)} = Collection\,(\sum f\,(E_{elec)}) \quad (6)$$

$$f(E_{leap)} = Leapfilter\,(f(E_{complex)}) \quad (7)$$

Here $\sum f\,(E_{elec)}$ is the electronic energy filter, $f(E_{complex)}$ is collecting the complex packets, $and\ f(E_{leap)}$ is jamming attack detection. These is classification performance finally steps.

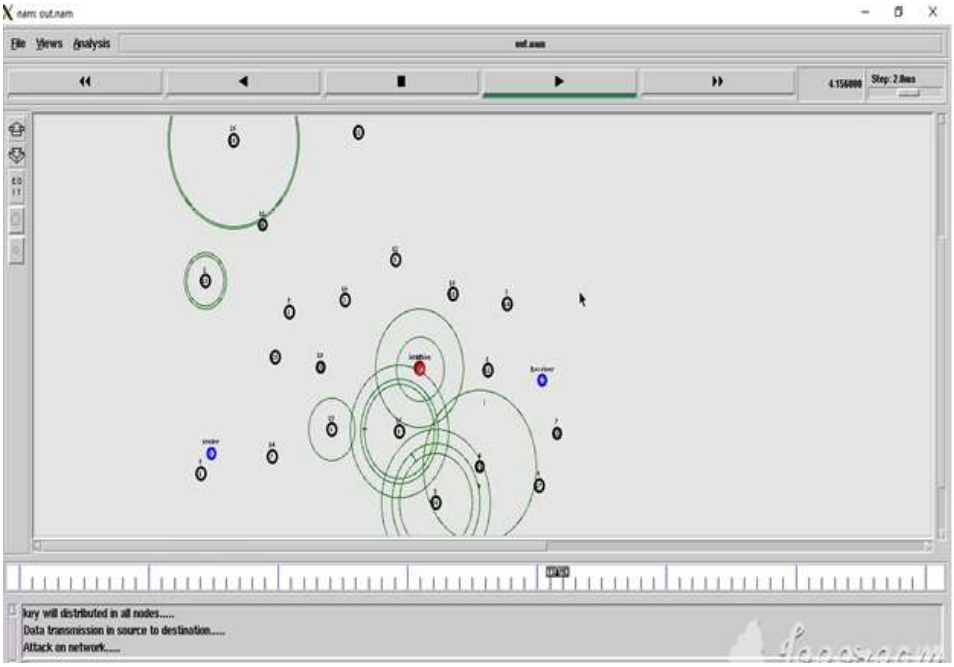

Figure.4 Simulation Result of NS2 jamming attack

Figure.4. Define the example sample result for the NS2 simulator using 100 nodes, running the node jamming attack, which appears on the screens output window.

4. Result And Discussion

The proposed system is compared to various learning algorithms, GANs, RNNs, LSTMs, and CNNs to reach. Still, Complex leap collection-based CNN classification is the best accuracy for jamming attack detection. THE N-To N Multi Path Routing Algorithm method determines the accuracy of energy consumption, jamming detection, and delay performance. N-to-N multipath routing, Shortest Propagation Delay-Based (SPDB), and MACA-Based MAC Protocol must be compared to the following algorithms.

Table 1 Simulation parameters of the proposed method

Parameters	Value
Tool	NS2
Language	TCL
Number of nodes	100
Traffic Model	CBR (Constant Bit Rate)
Simulation time	10mis
Network topology	Hybrid network

Table 1 displays that the simulation parameters outperform one of the measured analog conditions, in which the proposed method's various parameters evaluate their performance. The wireless sensor network's performance is the subject of this chapter. The performance is based on the analysis and calculation of WSN using a variety of approaches.

Receiving node $h_{ij}^{p} = \begin{cases} l & dg_i^p < d_{max} \\ \infty & dg_i^p \geq d_{max} \end{cases}$ (5)

Here $dg_i^p < d_{max}$ *is* received by the nodes,

Network delay performance

$\sum_p t_p < t_{delay}$ (6)

Power consumption.

$T_i = \frac{E_{in}}{\sum_p C_i^p \geq l, \forall i}$ (7)

Here equations (5),(6),(7), the performance outcome looked at the various versions of network energy consumption, transmission delay performance, packet Loss Rate Analysis, Routing Performance, and jamming detection performance.

Figure. 5 Transmission Delay performance analysis

WSN transmission delay is compared to various routing algorithms and protocols in Figure 5. For 200 kbps, the MAC protocol based on MACA has a time delay performance of 69%, the SPDB protocol has a commission of 79%, and the N-to-N Multipath routing protocol has a version of 89 % for 200 kbps.

Figure.6 Energy consumption rate analysis

The power consumption of WSNs in comparison to that of various routing protocols and algorithms is shown in Figure 6. At 200 kbps, the MACA-based MAC protocol performance is 67%, the SPDB protocol performance is 74%, and the N to N multipath protocol performance is 89.8%.

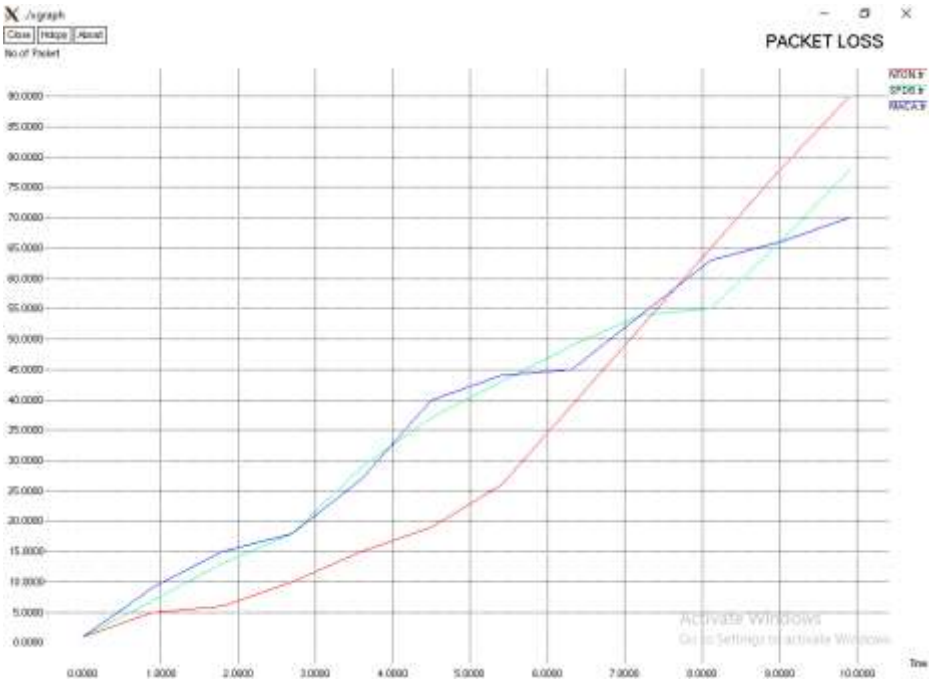

Figure 7 Packet Loss Rate Analysis

The packet loss rate of the WSNs is contrasted with that of different steering conventions and calculations in Figure 7. The MACA-based MAC protocol has a dead-loss rate of 95.1%; the dead-node loss rate for the SPDB protocol is 92.1%, and the slow node loss rate for the N to N multipath routing algorithm protocol is 85.2%. The proposed N-to-N multipath routing protocol performance has been compared to other methods like SPDB, and the MACA-based MAC protocol, as shown in Figure 8.

Figure 9 Analysis of Routing Performance

Figure 9 defines the WSN's routing performance compared to various routing protocols and algorithms. The MACA-based MAC protocol has a routing performance of up to 200kbps of 94%; the SPDB protocol has a routing performance of up to 200kbps of 97%, and the N to N multipath routing algorithm protocol has a routing performance of up to 200kbps of 97.9%

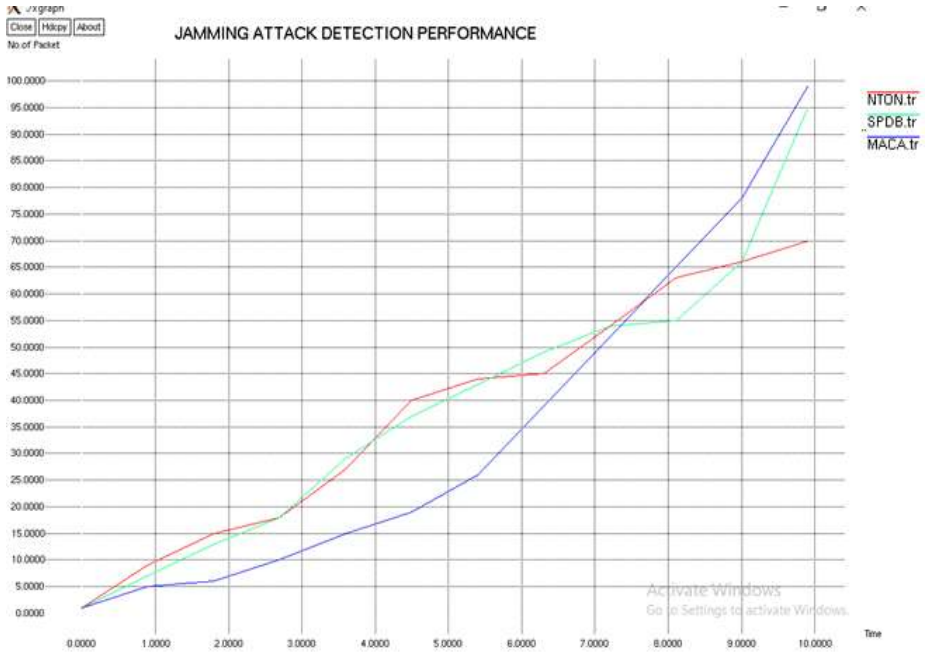

Figure. 10 Jamming Attack Detection Performance

Figure.10 says about IoT-based WSNs jamming attack detection performance. The performance of GANs method is 78% of the detection; the RNNs method is 89% of the detection; the LSTM method is 91% of the detection; the CNNs method is 91% of the detection, CNN-based complex leap collection method is 99.2% of the detection.
Likewise, a CNN-based complex leap collection method classifier is utilized to picture the presentation of the classifiers. It compromises the actual positive rate (TPR) and the false positive rate (FPR) at various grouping edges. As displayed in the situations above, TPR is the extent of perceptions accurately anticipated as confident, be that as it may, FPR is the extent of perceptions erroneously expected as sure.
TPR=TP/(TP+FN)
FPR=TP/ (TN+FP)
As displayed in the situations over, the TPR is the extent of perceptions that are accurately anticipated as confident. Notwithstanding, FPR is the extent of perceptions that are falsely predicted as positive.

5. Conclusion

The IoT-based wireless sensor network has been giving the best result for jamming detection performance. Jamming attacks are primarily performed in time intervals and signal strength based on IoT WSN. The cost for node communication and overhead is the problem in IoT WSN. The proposed will use the Deep learning-based Complex

Leap Collection based CNN method to detect the jamming attack. The RNNs method performs 89% of the detection; the LSTM method is 91% of the detection; the CNNs method is 91% of the detection; the CNN-based complex leap collection method is 99.2% of the detection. These system has been the solution for reducing transmission delay and reduced Energy consumption, reducing the Packet Loss Rate, and increasing the multipath routing performance. The present system of N to N Multipath routing has a better solution. Prefer the CNN-based complex leap collection method classifier has given the IoT-based WSN jamming detection well performance result.

References

1. S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao and H. Zhou, "Delimitated Anti Jammer Scheme for Internet of Vehicle: Machine Learning Based Security Approach," in IEEE Access, vol. 7, pp. 113311-113323, 2019, doi 10.1109/ACCESS.2019.2934632.
2. S. Ali, M. A. Khan, J. Ahmad, A. W. Malik and A. your Rehman, "Detection and prevention of Black Hole Attacks in IOT & WSN," 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 2018, pp. 217-226, doi: 10.1109/FMEC.2018.8364068.
3. A. Chhabra, V. Vashishth and D. K. Sharma, "A game theory based secure model against Black hole attacks in Opportunistic Networks," 2017 51st Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 2017, pp. 1-6, doi: 10.1109/CISS.2017.7926114.
4. P. Hemalatha and J. Vijithaananthi, "An effective performance for Denial of Service Attack (DoS) detection," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC), Palladam, India, 2017, pp. 229-233, doi: 10.1109/I-SMAC.2017.8058345.
5. S. Sharma and S. Gambhir, "CRCMD&R: Cluster and Reputation-based cooperative malicious node Detection & Removal scheme in MANETs," 2017 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2017, pp. 336-340, doi: 10.1109/ISCO.2017.7856012.
6. C. Ioannou, V. Vassiliou, and C. Sergiou, "An Intrusion Detection System for Wireless Sensor Networks," 2017 24th International Conference on Telecommunications (ICT), Limassol, Cyprus, 2017, pp. 1-5, doi: 10.1109/ICT.2017.7998271.
7. N. Aschenbruck, J. Bauer, J. Bieling, A. Bothe and M. Schwamborn, "A security architecture and modular intrusion detection system for WSNs," 2012 Ninth International Conference on Networked Sensing (INSS), Antwerp, Belgium, 2012, pp. 1-8, doi: 10.1109/INSS.2012.6240521.
8. N. Aschenbruck, E. Gerhards-Padilla, and P. Martini, "Simulative Evaluation of Adaptive Jamming Detection in Wireless Multi-hop Networks, "IEEE 30th International Conference on Distributed Computing Systems Workshops, Genoa, Italy, 2010, pp. 213-220, doi 10.1109/ICDCSW.2010.57.
9. B. Ahuja, D. Mishra, and R. Bose, "Optimal Green Hybrid Attacks in Secure IoT," in IEEE Wireless Communications Letters, vol. 9, no. 4, pp. 457-460, April 2020, doi: 10.1109/LWC.2019.2958910.

10. C. Fu, Q. Zeng, H. Chi, X. Du and S. L. Valluru, "IoT Phantom-Delay Attacks: Demystifying and Exploiting IoT Timeout Behaviors," 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Baltimore, MD, USA, 2022, pp. 428-440, doi: 10.1109/DSN53405.2022.00050.
11. M. Tarkowski, M. Rzymowski, L. Kulas and K. Nyka, "Improved jamming resistance using electronically steerable parasitic antenna radiator," IEEE EUROCON 2017 -17th International Conference on Smart Technologies, Ohrid, Macedonia, 2017, pp. 496-500, doi: 10.1109/EUROCON.2017.8011161.
12. H. Pirayesh, P. Kheirkhah Sangdeh and H. Zeng, "Securing ZigBee Communications Against Constant Jamming Attack Using Neural Network," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4957-4968, 15 March15, 2021, doi: 10.1109/JIOT.2020.3034128.
13. B. Kihei, H. Wilson and M. Fall, "Experimental Results of Detecting Primitive Jamming Attacks using Machine Learning in Vehicle-to-Everything Communication Networks," 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2021, pp. 530-535, doi: 10.1109/WF-IoT51360.2021.9595326.
14. X. Wang et al., "Mean Field Reinforcement Learning Based Anti-Jamming Communications for Ultra-Dense Internet of Things in 6G," 2020 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 2020, pp. 195-200, doi: 10.1109/WCSP49889.2020.9299742.
15. M. S. Abdalzaher, M. Elwekeil, T. Wang and S. Zhang, "A Deep Autoencoder Trust Model for Mitigating Jamming Attack in IoT Assisted by Cognitive Radio," in IEEE Systems Journal, vol. 16, no. 3, pp. 3635-3645, Sept. 2022, doi: 10.1109/JSYST.2021.3099072.
16. Y. E. Sagduyu, Y. Shi and T. Erpek, "IoT Network Security from the Perspective of Adversarial Deep Learning," 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 2019, pp. 1-9, doi: 10.1109/SAHCN.2019.8824956.
17. A. Jagannath, J. Jagannath and A. Drozd, "High Rate-Reliability Beamformer Design for 2×2 Mimo-OFDM System Under Hostile Jamming," 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 2020, pp. 1-9, doi: 10.1109/ICCCN49398.2020.9209635.
18. H. A. Bany Salameh, S. Almajali, M. Ayyash and H. Elgala, "Spectrum Assignment in Cognitive Radio Networks for Internet-of-Things Delay-Sensitive Applications Under Jamming Attacks," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1904-1913, June 2018, doi: 10.1109/JIOT.2018.2817339.
19. B. Lyu, D. T. Hoang, S. Gong, D. Niyato and D. I. Kim, "IRS-Based Wireless Jamming Attacks: When Jammers Can Attack Without Power," in IEEE Wireless Communications Letters, vol. 9, no. 10, pp. 1663-1667, Oct. 2020, doi: 10.1109/LWC.2020.3000892.