DoS attack detection and hill climbing based optimal forwarder selection

Palamalai Radhakrishnan[1], Senthil Kumar Seeni[2], Dhamotharan Rukmani Devi[3], Tumuluri Kanthimathi[4], Devadhas David Neels Ponkumar[5], Vikram Nattamai Sankaran[6], Subbiah Murugan[7]

[1]Department of Electronics and Communication Engineering, Tagore Engineering College, Chennai, India
[2]Department of Mobile Application Development, Cognizant Technology Solutions, Buffalo Grove, Illinois, United States of America
[3]Department of Electronics and Communication Engineering, R.M.D. Engineering College, Chennai, India
[4]Department of Mechanical Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[5]Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India
[6]Industry Experts, Giesecke and Devrient America Inc, Cumming, United States of America
[7]Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Thandalam, India

Article Info

Article history:

Received Oct 4, 2023
Revised Jul 5, 2024
Accepted Jul 14, 2024

Keywords:

DoS attack
Fuzzy learning
Hill climbing
Optimal forwarder selection
Wireless network

ABSTRACT

Wireless networks are becoming a more and more common form of networking and communication, with several uses in many industries. However, the rising popularity has also increased security risks, such as Denial of service (DoS) attacks. To solve these issues, DoS attack detection and hill climbing (DDHC) based optimal forwarder selection in wireless network. The suggested method seeks to efficiently identify DoS attacks and enhance network performance by preventing the communication hiccups brought on by such attacks. Fuzzy learning method is suggested to analyze trends and find DoS threats. The node bandwidth, connectivity, packet received rate, utilized energy and response time parameters to detect the node abnormality. This abnormality decides the node's future state and detects the DoS attacker. A fuzzy learning algorithm is proposed to detect DoS attacks, which increases attack detection accuracy and lowers false alarm rates. Using the HC procedure, the proposed system transmits data from sender to receiver. Simulation results illustrate the DDHC mechanism increases the DoS attacker detection ratio and minimizes the false positive ratio. Furthermore, it raises the network throughput and reduces the delay in the network.

Corresponding Author:

Palamalai Radhakrishnan
Department of Electronics and Communication Engineering, Tagore Engineering College
Rathinamangalam, Chennai, Tamil Nadu, India
Email: krish75radha@gmail.com

1. INTRODUCTION

Intrusion detection in a wireless network refers to the capacity to identify illegal network access. Such illegal access gravely threatens the confidentiality, integrity, and availability of the system and the data it maintains [1]. Experts in this profession often use various methods that monitor network traffic to find anomalous activities, preserve data, and prevent adverse outcomes. Well-known cyberattacks such as denial of service (DoS) attempt to consume the computational resources of a host or network, rendering them unavailable to authorized users or adversely impacting the performance of their computer system.

Software exploits and flooding attacks are two types of DoS attacks [2]. In software exploits, the attacker uses server vulnerabilities to shut down services or significantly reduce server performance. Flooding attacks cause the issues mentioned above because the attacker exhausts system resources by submitting many erroneous requests [3].

An arithmetical optimization named hill climbing (HC) is utilized for local searching. HC search is a better solution in the locality (neighborhood) to confirm the present condition [4]. If it reaches the receiver with better quality, re-examine and quit else, revise the present state in prolonged condition. Afterward, iterate the steps till a result is decided or there is no appearance of recent operator residue in the present state. Moreover, two stages are proceeding in the loop. Firstly, the unapplied operator is selected and applied in the present state and builds the fresh state. Validating the fresh state is the next stage. A better state quality is selected from the above stages to present in HC [5]. It guides to quality of a solution invention. Several problems are managed, which is HC benefits. In this criterion, customization and alteration of the method is approved. For example, adaptation and discrete domains are operated. To raise the local searching capability, the HC cause is included in the introduced approach. HC is the simplest local searching procedure. Initially, it begins with an arbitrary solution and then shits iteratively from a root-to-child solution until no best-child solutions are recognized. By the necessary opinion of the HC technique, it raises the local searching ability.

Problem statement: a method using artificial neural networks (NNs) to identify DoS attacks (ANND) via management frames. The suggested method seeks to efficiently identify bogus de-authentication/disassociation frames and enhance network performance by preventing the communication hiccups brought on by such attacks [6]. In order to analyze patterns and characteristics in the management frames sent back and forth between wireless devices, the proposed NN method makes use of machine learning techniques. The system can develop the ability to precisely identify probable DoS attacks by training the NN. However, this mechanism increases the false alarm rate in the network. In addition, it can’t forward the data efficiently.

Work contribution: the contribution of DoS attack detection and hill climbing (DDHC) mechanism is specified below. The proposed mechanism utilizes a Fuzzy learning method to find out DoS threats. The node bandwidth, connectivity, packet received rate, utilized energy and response time parameters to detect the node abnormality. This abnormality decides the node's future state and detects the DoS attacker. Furthermore, the HC algorithm forms the optimal route by HC fitness function. This fitness function is computed based on node energy, node-link terminal time, the distance between two nodes, and hop counts. The highest fitness function node is elected as an optimal forwarder for data transmission in the WANET. A fuzzy learning algorithm is proposed to detect DoS attacks, which increases attack detection accuracy and lowers false alarm rates. The remaining portion of this paper is prepared as follows. The DDHC mechanism is introduced in section 2. Section 3 explains the simulation results, and section 4 concludes the article with a summary and future research of PHHO mechanism.

It is not surprising that a lot of research is done daily to defend networks against DoS attacks since this form of attack causes a wireless network to go down completely or partially [6]. Multiple categories may be used to categorize DoS attacks [7]. The mobile node’s limited resources are the focus of a flooding-based DoS attack, culminating in a denial of sleep attack and excessive battery backup use [8]. In a DoS attack using synchronize sequence number (SYN) flooding, the attacker sends several fake SYN packets, exceeding the target buffer and congesting the network. The following article is split into three sections: i) using Bayesian inference to describe SYN traffic mathematically; ii) demonstrating that Bayesian inference and exponentially weighted moving average are equivalent; and iii) creating an effective method for detecting SYN flooding attacks using Bayesian inference.

In order to improve the capacity to withstand attacks, this research suggests a secondary frequency control strategy based on intrusion detectors [9]. It evaluates the potential for false detection of intrusion detectors against DoS attacks since most of the current attack-resilient controllers assume the complete accuracy of intrusion detection systems. The real attack option can only be detected instead of presuming that a defense will be aware of it. Therefore, the suggested frequency controller changes its control gains based on the detected attack choice rather than the actual attack. A deep learning technique to build an intrusion detection and prevention system that can recognize and stop DoS attacks [10]. The deep learning model divides received packets to the web server into normal packets and DoS attack categories to reduce DoS attacks. This method enables you to switch between the system's DoS detection mode and the prevention mode, and it can visually and textually show information from captured and categorized packets [11]. DoS attack detection approach for addressing the performance problems caused by DoS attacks that use data plane development kit (DPDK) to embed intelligence [12]. This innovative framework is known as a DPDK-based DoS detection framework since DPDK offers quick packet processing and data plane monitoring. Additionally, the statistical anomaly detection technique, which uses DPDK to implement it as a virtual network function on the data plane, provides quick detection of DDoS attacks.

Framework for message queuing telemetry transport (MQTT) protocol DoS attack detection is tested using real-world, protocol-compliant scenarios [13]. A DoS attack detection system based on machine learning is used to defend MQTT message brokers against such attacks. A reliable, nonparametric, unmodified detection method for media-access control layer DoS attacks [14]. This method tracks the successful transmissions and terminal collisions in the network using truncated sequential Kolmogorov-Smirnov statistics. The efficient DoS attacks detection goal is to provide an effective intrusion detection system (IDS) for identifying DoS attacks [15]. This work presents a thorough empirical investigation aimed at assessing several Data mining approaches, which were initially tried utilizing all available data and assessed in terms of detection accuracy and time complexity. A feature selection method has also been used to decrease the area surrounding features and achieve a high accuracy rate. Attacks on availability, such as DoS, attempt to prohibit genuine users from using the network. Keep in mind that DoS attacks are distinct from selfish actions driven by potential rewards [16]. DoS attacks are simple to carry out, especially in the wireless realm, due to the broadcast nature of wireless networks. In addition, other 802.11-specific DoS vulnerabilities have recently been experimental. A DoS attack may be easily launched by an adversary due to the shared nature of the medium [17]. A rogue node may continuously broadcast a radio signal to prevent authorized users from using the medium and/or to obstruct reception. The malicious nodes are referred to as jammers, and this behavior is known as jamming. Jamming methods range from simple attacks that continuously transmit interference signals to more complex ones that target specific protocol weaknesses.

The issue of event-based fault identification for unmanned surface vehicles (USVs) subject to DoS jammer attacks is addressed [18]. A robust event-triggered mechanism is implemented to lessen the USV system's energy consumption and bandwidth use while reducing the impact of DoS attacks. Attacks using distributed denial of service (DDoS) floods are among the main worries for security experts. DDoS flooding attacks are often overt efforts to obstruct services from being accessed by authorized users [19]. Attackers often obtain access to many computers by assembling attack armies using the vulnerabilities of those machines. An attacker may launch a coordinated, massive attack on one or more targets after assembling an attacking army. The intrusion detection and prevention system is working on creating a complete defensive system against known and expected DDoS flooding attacks. The severity of the DDoS flooding attack issue and efforts to address it. By using reflection techniques, an intelligent attack circumvents blacklists, IP, packet-count or session/transaction-based rate limiting, and automatic message generation detection systems found in modern security perimeters [20]. It also creates legitimate traffic.

A blockchain-based method detects the network’s malicious node [21]. Many 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 applied linear aggregation method to combining 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 [22]. Trust assessment illustrates the diversity in disparate appliances. Although these methods can compute trust, they moreover broadcast huge appropriate arithmetical requirements for evaluation. Sporadically, it is nonflexible for apprehension samples. The collection of trust-relevant features and establishing the rule significantly concern the precision of trust evaluation. It ignores intelligence and active sustain [23]. A fuzzy trust model and artificial bee colony algorithms are proposed to compute the indirect trust. The artificial bee colony algorithm is functional to optimize the trust model to identify dishonest attacks [24]. A secure clustering with a fuzzy trust assessment approach handles communication uncertainty. In this approach, the fuzzy controller measures the trust. An adaptive trust threshold method is utilized to separate the malicious nodes from the network [25]. The scope of ML algorithm for cyber security concentrating on regions; for example, detections of intrusion, spam, as well as malware on computer network, to provide complete the complexities ML methods concentrate in defending cyberspaces from attack [26]. The IoT, that incorporates a several devices to offer elevated and intelligent services, has to defend user privacy and deal attacks, for example; spoofing attacks, DoS attacks, jamming, as well as eavesdropping [27].

2. PROPOSED METHOD

2.1. Fuzzy learning-based DoS attack detection

This mechanism uses the fuzzy learning algorithm to recognize and prevent an attack. To find the attack, the fuzzy learning method is used. This method combines the Q-learning with the fuzzy min-max action selection and reward function. The module that recognizes the malicious packet is hazy. The values crossing the threshold value are reported after comparing the present packet and a typical packet. It comprises a knowledge base, an expert analyst, a feature extractor, fuzzification, and the fuzzy inference engine. The threat profile is produced by the feature extractor using the network traffic.

The proposed system would increase system accuracy by basing the threat profile on packet received rate (PRR), response time (RT), bandwidth (B), connection (C), and energy utilization (E). These variables are the fuzzy system's input like P = {RT, B, C, E, and PRR}. Here, PRR stands for packet reception rate, E for energy consumption, B for packet length from sender to receiver, and C for the number of connections to a similar node. RT also represents a variance in the time difference between two links during a specific time window. The fuzzy inference engine's fuzzy rules to derive a new fact are stored in the knowledge base. According to the expert analyst, defuzzification impacts whether or not the examined packets are attacked. The fuzzy system's output, which depicts agent A(t)'s behavior, is abnormality. The definition of fuzzy rules is dependent on the fuzzy inputs. Modeling of the discovered attack activity takes into account the fuzzy state. The fuzzy logic (FL) controller, used by the FL agent, determines the weights to be given to each potential future state. The ideal cost may be attained through connection with the threshold value.

2.2. HC-based optimal route formation

Route discovery is the major problem in wireless networks. In the normal route discovery method, the sender forms the route by the shortest route. This route does not need awareness of the next-hop nodes; as a result, node failure or link failure occurs. Hence, the transmitted data packet will be dropped. To solve these issues, the HC method for detecting the best next hop nodes. The best-received result is next passed to the HC to speed up the search and defeat the slow convergence technique. HC is an iterative technique that initiates with a random resolution to a difficulty. Next, tries to decide on a better resolution by incrementally shifting a particular resolution component. While the adjustment makes a better solution, the incremental update is executed on the recent solution that is continual till no additional improvements can be established. Applying an HC fitness function, this method aims to decide optimal routes from sender to receiver. This fitness function is computed by the node energy, distance, node hop count, and link termination time. The procedure of the HC is given:

```
1. Preliminary solution = next node
2. Whilst $f(s\text{ender}) \leq f$ (next node) sender € Neighbours (next node) do
3. Make a sender € Neighbours (next node);
4. If fitness (sender) > fitness (next node), then
5. Replace the sender with the next node;
6. End If
```

2.2.1. Distance (D)

The distance metric is the sum of the node's links to all other neighboring. Distance is a significant parameter during forwarder selection from sender to receiver. Whenever a node detaches itself from its neighbour through a large distance (d), extra energy and power is necessary to transport information, leading to enhanced energy utilization as shown in (1).

$$D = \sum d(j,k) \tag{1}$$

2.2.2. Link termination time (LTT)

LTT indicates how extended a connection will stay dynamic. The LTT of two nodes represents the duration of the association of the two nodes within a transmission range. Distance represents that the forwarder node wants to travel to get out of range of the sender node. The longer this period of time travel, the more stable the connectivity between nodes. This period of time is decided by how rapidly the uneven node takes place and is computed by (2). The relative velocity is applied to discover the direction of the node movement and the relative velocity is computed by the (3).

$$LTT = \frac{Distance}{Relative\ Velocity} \quad LTT = \frac{Dis\tan ce}{\mathrm{Re}\,lative\ velocity} \tag{2}$$

$$Relative\ Velocity = \frac{Displacement}{time} \tag{3}$$

2.2.3. Residual energy (RE)

RE is a significant parameter to determine the relay node. The smallest amount of energy just one node utilizes preceding being selected as its forwarder; the higher its residual energy, the greater its probability of being selected as the transmitter. The RE computation is specified by (4).

$$RE = Initial\ Energy - Utilized\ Energy \tag{4}$$

2.2.4. Hop count

The hop count represents the count of hops or linking nodes, including the full of its connected neighbors. The count of the hop is minimum, and a lesser amount of energy is utilized; also, the data packet forwarding delay is minimum. Table 1 illustrates the algorithm of the DDHC approach. Initially, the next. node's distance is decided, then calculates the link termination time and residual energy. Finally, calculate the node hop count. The HC method fitness function (FF) for forwarder selection is given in (5).

$$FF = \delta_1(f_1) + \delta_2(f_2)+\delta_3(f_3) + \delta_4(f_4) \tag{5}$$

Here, $f_1$indicates node distance, f_2 indicates the link termination time, f_3 the residual energy, and f_4 the hop count. Here, $\sum_{j=1}^{4}\delta_j = \delta_j \in (0,1)$. The lowest fitness function node is replaced as the best forwarder node. Algorithm 1 determines the DDHC mechanism.

Algorithm 1. DDHC mechanism

```
Start
Input: PRR, RT, C, B, E, node distance, link expiration time, hop count
Output: DoS attack detection, best forwarder selection
DoS attack detection
Fuzzy learning algorithm do
Fuzzy Input: Compute PRR, RT, B, C, E
Fuzzy Output: Evaluate node abnormality
Predict node future states
Detect DoS attack
optimal route formation
HC algorithm do
fitness function computation
node distance
link expiration time
node residual energy
hop count
best forwarder selection
data transmission
receiver reaches the data
Stop
```

3. SIMULATION ANALYSIS

This paper uses the network simulator (ns)-2.28 [28] to measure the network performance of the ANND and DDHC approaches. Here, 200 wireless nodes are used for measuring the network performance and these nodes are moving arbitrarily. This approach uses 802.11 medium access control (MAC) for execution. The wireless nodes transmission range is 220 meters and 20 DoS nodes are arbitrarily distributed in the field. To evaluate the execution of the introduced approach, wireless nodes speed from 1 m/s and 5 m/s, correspondingly [29]. The function of the DDHC is measured by delay, lifetime, throughput and DoS detection ratio, and the false positive ratio of routing. These parameters specifies the performance of the Table 1 demonstrates the parameters and values for measuring the network performance.

Throughput shows the efficiency of the proposed method. It is defined as the data effectively forwarded through the transmission link. Figure 1 illustrates the ANND and DDHC approaches for Throughput established on wireless nodes. From Figure 1, the DDHC approach increases the throughput value when it marginally decreases the node count.

Table 1. Simulation parameters of DDHC

Parameters	Values
Simulation region	700*600 m^2
Wireless node count	200
DoS attacker count	20
Bandwidth	2 Mbps
Simulation time	500 Sec
Initial energy	1 Joule
Size of the packet	1024 bytes
Antenna	Omni directional
Range of transmission	220 m
MAC	802.11
Node distribution	Arbitrarily

Since the DDHC approach detects the DoS node and optimal forwarder, it efficiently transmits the data from sender to receiver. But, the existing approach raises the node count, and the throughput value is highly minimized because the ANND approach increases the false alarm and can't use the optimal route. A lifetime of the network is defined as the time that the energy of the first wireless node in the network turns to be entirely dead. Figure 2 explains ANND and DDHC approaches for false positive ratio.

From Figure 2, when the node count is raised, the false positive ratio also rises; but, in the ANND, if the number of wireless nodes rises, the false positive ratio is highly increased since it can't detect the DoS attack efficiently. However, the DDHC mechanism uses fuzzy Learning to detect the DoS attack efficiently. Figure 3 explains ANND and DDHC approaches for a lifetime based on wireless nodes.

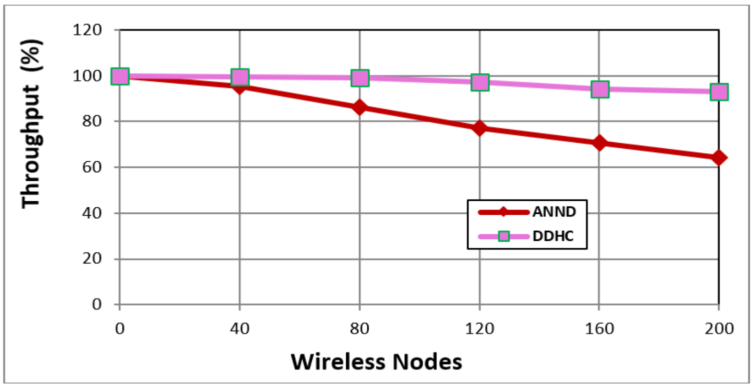

Figure 1. ANND and DDHC approaches for throughput

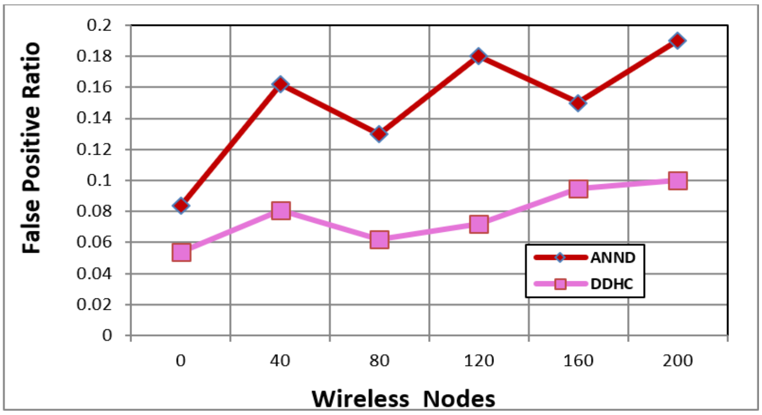

Figure 2. ANND and DDHC approach for false positive ratio

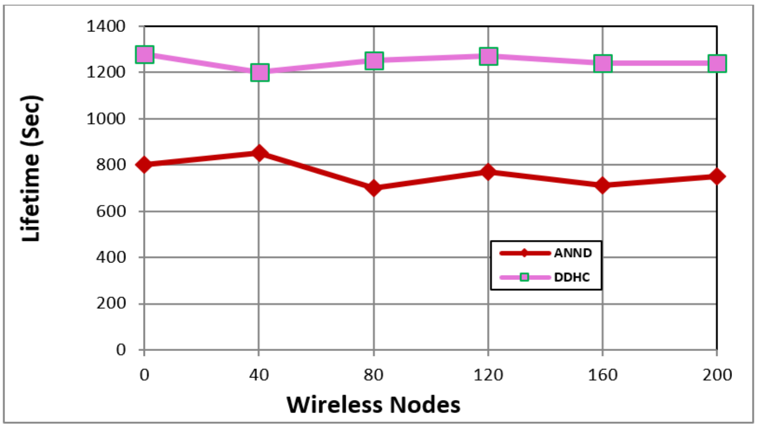

Figure 3. ANND and DDHC approaches for a lifetime

From Figure 3, the lifetime enhances as the amount of nodes rises; on the contrary, in the case of ANND, if the number of wireless nodes rises, the lifetime will reduce since with raising the amount of wireless nodes, more wireless nodes concentrate on transmitting the data, and it is extremely chanceful for a node to expire at any time. In addition, ANND cannot evade unnecessary packet communications. But, the DDHC approach transmits the data through an optimal route, thus enhancing the lifetime. Figure 4 explains the ANND and DDHC approaches DoS attack detection ratio.

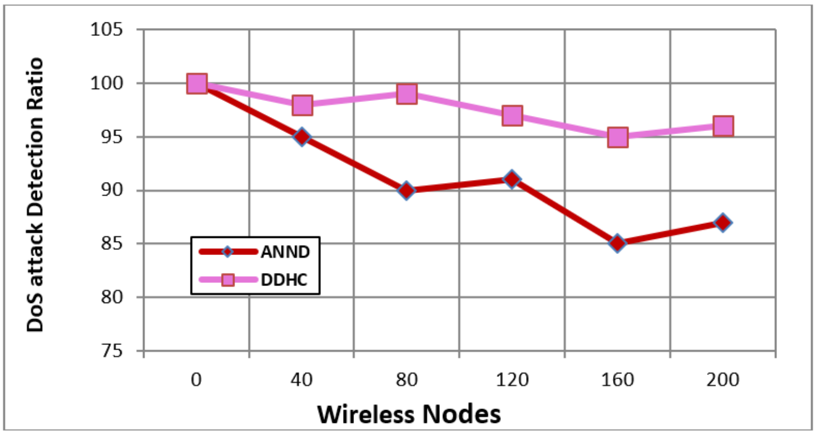

Figure 4. ANND and DDHC approaches for DoS attack detection ratio

Generally, the DoS attack detection ratio is minimized by increasing the wireless nodes count. But, the proposed DDHC mechanism slightly minimizes the detection ratio because it uses fuzzy learning based on node abnormality. This abnormality is measured by bandwidth, connectivity, energy utilization, PRR, and response time. But, the existing ANND mechanism increases the false alarm rate. Figure 5 demonstrates ANND and DDHC approaches Delay based on wireless nodes.

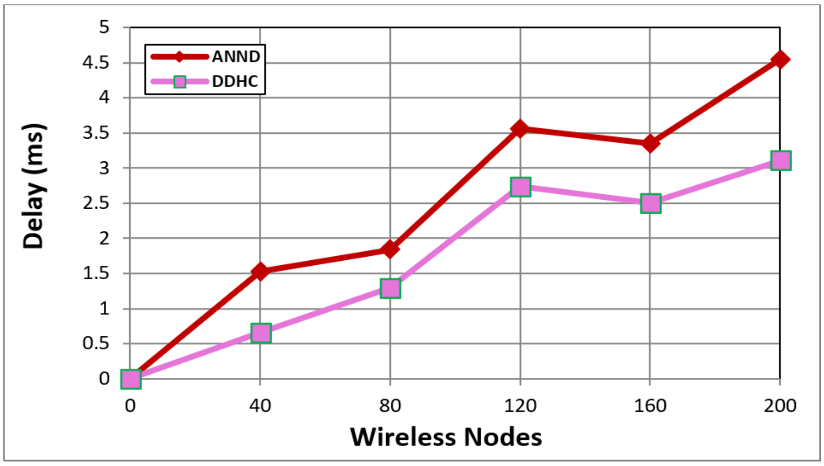

Figure 5. ANND and DDHC approaches for delay

From Figure 5, the ANND and DDHC mechanisms increase the delay value when raises the wireless nodes. In DDHC, the fuzzy learning method detects the DoS attack efficiently; furthermore, the HC method also selects the optimal forwarder, reducing the number of features and minimizing the network delay. HC method based choose the forwarder is minimized the network. But, the existing ANND mechanism raises the delay compared to the DDHC mechanism.

4. CONCLUSION

Dos attacks make the system perform worse. Data security and privacy are the two main concerns with wireless networks. Special preventative strategies are needed to defend against DoS attacks in wireless networks. The objective of this paper to detect the DoS attack and enhance routing efficiency. The fuzzy learning method is suggested to analyze trends and find DoS threats. The node bandwidth, connectivity, packet received rate, utilized energy and response time parameters to detect the node abnormality. This abnormality decides the node's future state and detects the DoS attacker. It decreases the number of false alarms and increases the system's accuracy. Finally, they select the optimal forwarder from sender to receiver by applying the HC method fitness function. This fitness function is computed based on the node energy, distance, node hop count, and link termination time. The application of this mechanism to utilized in military security. Experimental outcomes demonstrated that the DDHC mechanism raised the detection ratio and minimized the false positive ratio. In addition, it raised the network throughput and lifetime in the wireless network. The DDHC mechanism does not concentrate on energy efficiency. The clustering with improve network lifetime concept may be perform in future.

REFERENCES

[1] O. Can and O. K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," in *6th International Conference on Modeling, Simulation, and Applied Optimization, ICMSAO 2015 - Dedicated to the Memory of Late Ibrahim El-Sadek*, May 2015, pp. 1–6, doi: 10.1109/ICMSAO.2015.7152200.

[2] K. L. Narayanan, R. S. Krishnan, E. G. Julie, Y. H. Robinson, and V. Shanmuganathan, "Machine learning based detection and a novel EC-BRTT algorithm based prevention of DoS attacks in wireless sensor networks," *Wireless Personal Communications*, vol. 127, no. 1, pp. 479–503, Nov. 2022, doi: 10.1007/s11277-021-08277-7.

[3] M. Bogdanoski, T. Shuminoski, and A. Risteski, "Analysis of the SYN flood DoS attack," *International Journal of Computer Network and Information Security*, vol. 5, no. 8, pp. 15–11, 2013, doi: 10.5815/ijcnis.2013.08.01.

[4] Y. M. Raghavendra and U. B. Mahadevaswamy, "Energy efficient routing in wireless sensor network based on mobile sink guided by stochastic hill climbing," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 6, pp. 5965–5973, Dec. 2020, doi: 10.11591/ijece.v10i6.pp5965-5973.

[5] S. Sakamoto, E. Kulla, T. Oda, M. Ikeda, L. Barolli, and F. Xhafa, "A comparison study of hill climbing, simulated annealing and genetic algorithm for node placement problem in WMNs," *Journal of High Speed Networks*, vol. 20, no. 1, pp. 55–66, 2014, doi: 10.3233/JHS-140487.

[6] A. E. Abdallah *et al.*, "Detection of management-frames-based denial-of-service attack in wireless LAN network using artificial neural network," *Sensors*, vol. 23, no. 5, p. 2663, Feb. 2023, doi: 10.3390/s23052663.

[7] Ž. Gavrić and D. Simić, "Overview of dos attacks on wireless sensor networks and experimental results for simulation of interference attacks," *Ingenieria e Investigacion*, vol. 38, no. 1, pp. 130–138, Jan. 2018, doi: 10.15446/ing.investig.v38n1.65453.

[8] M. A. Elsadig, "Detection of denial-of-service attack in wireless sensor networks: a lightweight machine learning approach," *IEEE Access*, vol. 11, pp. 83537–83552, 2023, doi: 10.1109/ACCESS.2023.3303113.

[9] N. Nishanth and A. Mujeeb, "Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using bayesian inference," *IEEE Systems Journal*, vol. 15, no. 1, pp. 17–26, Mar. 2021, doi: 10.1109/JSYST.2020.2984797.

[10] S. Liu, P. Siano, and X. Wang, "Intrusion-detector-dependent frequency regulation for microgrids under denial-of-service attacks," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2593–2596, Jun. 2020, doi: 10.1109/JSYST.2019.2935352.

[11] J. F. C. Garcia and G. E. T. Blandon, "A deep learning-based intrusion detection and preventation system for detecting and preventing denial-of-service attacks," *IEEE Access*, vol. 10, pp. 83043–83060, 2022, doi: 10.1109/ACCESS.2022.3196642.

[12] J. E. Varghese and B. Muniyal, "An efficient IDS framework for DDoS attacks in SDN environment," *IEEE Access*, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.

[13] N. F. Syed, Z. Baig, A. Ibrahim, and C. Valli, "Denial of service attack detection through machine learning for the IoT," *Journal of Information and Telecommunication*, vol. 4, no. 4, pp. 482–503, Oct. 2020, doi: 10.1080/24751839.2020.1767484.

[14] A. L. Toledo and X. Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks," *IEEE Transactions on Information Forensics and Security,* vol. 3, no. 3, pp. 347–358, Sep. 2008, doi: 10.1109/TIFS.2008.926098.

[15] I. Almomani and M. Alenezi, "Efficient denial of service attacks detection in wireless sensor networks," *Journal of Information Science and Engineering*, vol. 34, no. 4, pp. 977–1000, 2018, doi: 10.6688/JISE.201807_34(4).0011.

[16] K. Bicakci and B. Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," *Computer Standards and Interfaces*, vol. 31, no. 5, pp. 931–941, Sep. 2009, doi: 10.1016/j.csi.2008.09.038.

[17] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 2, pp. 245–257, 2011, doi: 10.1109/SURV.2011.041110.00022.

[18] Z. Fei, X. Wang, and Z. Wang, "Event-based fault detection for unmanned surface vehicles subject to denial-of-service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 5, pp. 3326–3336, May 2022, doi: 10.1109/TSMC.2021.3064884.

[19] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Communications Surveys and Tutorials,* vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[20] I. M. Tas, B. G. Unsalver, and S. Baktir, "A novel SIP based distributed reflection denial-of-service attack and an effective defense mechanism," *IEEE Access*, vol. 8, pp. 112574–112584, 2020, doi: 10.1109/ACCESS.2020.3001688.

[21] L. K. Ramasamy, F. Khan K. P., A. L. Imoize, J. O. Ogbebor, S. Kadry, and S. Rho, "Blockchain-based wireless sensor networks for malicious node detection: a survey," *IEEE Access*, vol. 9, pp. 128765–128785, 2021, doi: 10.1109/ACCESS.2021.3111923.

[22] S. R. Sahith, S. R. Rudraraju, A. Negi, and N. K. Suryadevara, "Mesh WSN data aggregation and face identification in fog computing framework," in *Proceedings of the International Conference on Sensing Technology, ICST*, Dec. 2019, vol. 2019-December, pp. 1–6, doi: 10.1109/ICST46873.2019.9047708.

[23] F. Amin, A. Ahmad, and G. S. Choi, "Towards trust and friendliness approaches in the social internet of things," *Applied Sciences (Switzerland)*, vol. 9, no. 1, p. 166, Jan. 2019, doi: 10.3390/app9010166.

[24] B. Pang, Z. Teng, H. Sun, C. Du, M. Li, and W. Zhu, "A malicious node detection strategy based on fuzzy trust model and the ABC algorithm in wireless sensor network," *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1613–1617, Aug. 2021, doi: 10.1109/LWC.2021.3070630.

[25] L. Yang, Y. Lu, S. X. Yang, T. Guo, and Z. Liang, "A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4837–4847, Jul. 2021, doi: 10.1109/TII.2020.3019286.

[26] C. S. Ranganathan, R. Raman, K. K. Sutaria, R. A Varma, and S. Murugan, "Network security in cyberspace using machine learning techniques," in *7th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2023 - Proceedings*, Nov. 2023, pp. 1755–1759, doi: 10.1109/ICECA58529.2023.10394962.

[27] R. K. Vanakamamidi, N. Abirami, C. Sasi Kumar, L. Ramalingam, S. Priyanka, and S. Murugan, "IoT security based on machine learning," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 683–687, doi: 10.1109/SmartTechCon57526.2023.10391727.

[28] M. J. Kumar, S. Mishra, E. G. Reddy, M. Rajmohan, S. Murugan, and N. A. Vignesh, "Bayesian decision model based reliable route formation in internet of things," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 3, pp. 1665–1673, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1665-1673.

[29] M. Amru *et al.*, "Network intrusion detection system by applying ensemble model for smart home," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 3485–3494, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.

BIOGRAPHIES OF AUTHORS

Dr. Palamalai Radhakrishnan is a professor in Electronics and Communication Engineering presently working in Tagore Engineering College, Chennai. He received his Ph.D. Degree from Anna University. He received M.E Degree in Faculty of Information and Communication Engineering, Anna University, Chennai. He has published a number of research papers/ articles in peer review Journals. He also presented various academic as well as research-based papers at several national and international conferences. He has a teaching experience of more than 24 years and is a life member of IETE. His research areas include signal processing, VLSI, embedded systems, image processing, and IoT. He can be contacted at email: pradhakrishnan@tagore-engg.ac.in.

Mr. Senthil Kumar Seeni senior architect in Cognizant Technology Solutions US corp, Tech-savvy and innovative professional with extensive experience developing mobile applications for various platforms, including iOS. Expertise in mobile app analysis, design, development, testing, bug fixing, maintenance & app publishing, technical writing, and CI/CD automation build process. Adept at managing and delivering projects on time, within budget, and to client satisfaction. Excel at developing software solutions and architecture best practices for mobile platforms. He pursued his Post graduate in Manufacturing Engineering under Annamalai University, Tamil Nadu. He has authored or coauthored around 5 research papers in various international conferences. He has strong passion in gaining more leadership and managerial skills along with his determined and goal-oriented tasks. He can be contacted at email: sseeni@gmail.com.

Dr. Dhamotharan Rukmani Devi is professor in the Department of Electronics and Communication Engineering and Overall Academic Coordinator at R.M.D Engineering College She obtained B.E. in Electronics and Communication Engineering in the year 1992 from IRTT, affiliated to Bharthiyar University, M.S in Electronics in the year 1997 at BITS, Pilani, M.E. in VLSI design in the year 2006 at R.M.K. Engineering College affiliated to Anna University and Ph.D. in the year of 2013 under Anna University in the area of VLSI Design. She has 30 years of teaching experience in both Undergraduate and Postgraduate level. She has guided many B.E. and M.E. projects. Eight Scholars completed Ph.D. under her supervision and six Scholars pursuing Ph.D. Her areas of interest include VLSI, Embedded, image and video processing and networks. She has published 63 journal articles, 5 book chapters, 5 books, 6 patents, and 2 patents granted. She has delivered many lectures as resource person for many workshops, seminars and faculty development program sponsored by AICTE and Anna University. She is a life member of many professional societies like IEI and senior member of IEEE. She can be contacted at email: rdrukmani319@gmail.com.

Dr. Tumuluri Kanthimathi is an Assistant Professor in the Department of mechanical Engineering and professor In-Charge Academics at Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram, Guntur Dist., Andhra Pradesh, India. She obtained B.E in Mechanical Engineering in the year 2000 from Sir C.R.R College of Engineering. Eluru in the 2000, affiliated to Andhra University, M.Tech. in Thermal Engineering in the year 2011 from JNTU Hyderabad and Ph.D. in the year 2024 from JNTU Hyderabad in the area of heat Transfer. She has 16 years of teaching experience in both Undergraduate and Postgraduate level. She has guided many B.E. and M.E projects. She has published 22 articles in various National and International Journals. She has expertise in the subjects like thermodynamics, fluid mechanics, heat transfer, and applied thermodynamics. She has memberships in ISHRAE and SAE professional bodies. She can be contacted at email: pkanthi1978@gmail.com.

Dr. Devadhas David Neels Ponkumar received M.E. in Digital Communication and Networks Engineering and Ph.D. in Information and Communication Engineering from the Anna University, Chennai is currently working as Professor in the ECE Department of Vel Tech Rangarajan and Dr. Sagunthala R&D Institute of Science and Technology, Chennai. He is having more than 20 years of academic experience and 10 years of Industrial experience in India and Saudi Arabia. He has a stint in Singapore too. He has Cisco certification in Network Administration, Cyber security and certifications in Cyber Forensics, Data Science and Big Data Analytics. He has more than 40 research publications in reputed journals and many international conferences. He has authored books in cybersecurity, ethical hacking, digital forensics, block chain, cryptography and wireless communication systems. He has 8 utility patents published in IoT domains and 5 design grants in IoT domain. He has a UK Design patent and South African Innovation patent under his kitty of achievements. He has won laurels as best scientist, best senior faculty, distinguished academic leader, Top 100 Engineers in India in 2022, Eminent Teachers of India in 2023. He can be contacted at email: drdavidneels@veltech.edu.in.

Mr. Vikram Nattamai Sankaran is a highly skilled and qualified professional with extensive experience in telecommunications, IoT, and Cyber Security. He has a robust background as a seasoned leader in technical project management within the industry. He is currently working at Giesecke + Devrient Mobile Security in Atlanta GA USA. Vikram holds a Bachelor of Engineering degree in Electronics and Communication Engineering from Anna University Chennai and Master of Engineering in Electrical Engineering/Information Technology from Rosenheim University of Applied Sciences Germany. With a strong academic and research background, he has contributed significantly to the field, publishing numerous papers in reputable journals and presenting at international conferences. Vikram is known for his passion for leadership development and achieving ambitious goals. He can be contacted at email: vikramnns@gmail.com.

Subbiah Murugan is an Adjunct Professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India. He published his research articles in many international and national conferences and journals. His research areas include network security and machine learning. He can be contacted at email: smuresjur@gmail.com.