International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Detecting Denial of Service Attack in Wireless Sensor Network using Energy Efficient Extreme Learning Neural Network (EEELNN)

A. Venkatesh, S. Asha

Abstract*: One of the effective communication technology is wireless sensor network technology which helps to monitor the surrounding information by sensed nodes. The effective utilization of sensed nodes is utilized in different applications such as military, health information, environmental monitoring, disaster relief and target analyze. The application requires the collection of information which may be collected from one location and transferred to the other location for making their process so easier. During the information transformation process, the network may affect by several intermediate attack, in which denial of service is one of the serious attack because it affects the entire network resources such as network energy, power, bandwidth. The unavailability of the resources reduces the entire sensor network performance. For managing the attack related issues, in this paper introduces the Energy Efficient Extreme Learning Neural Network (EEELNN) approach for overcoming the attack related issues. Initially the network transmitted zone is computed along with energy, power, bandwidth, neighboring node information and lifetime for eliminating the attack in sensor network. The computed information is processed and trained by extreme learning neural network that successfully predict the attack related data, node and network zone with effective manner that leads to improve the overall network performance. At last system efficiency is evaluated using simulation results such as detection rate, classification accuracy, false alarm rate and detection time.

Keywords* : Wireless sensor network, denial of service, Energy Efficient Extreme Learning Neural Network (EEELNN) approach, detection rate, classification accuracy, false alarm rate and detection time.

I. INTRODUCTION

The development of the technology and electronics placed a major role in the wireless sensor networks (WSN) [1] because it used to transmit the information from source to destination. During the information broadcast process, it utilizes the several autonomous characteristics while sensing, transmitting and receiving the information. With the help of the sensor characteristics it senses the surrounding situation that has been transmitted to the neighboring nodes via the embedded wireless radio in sensor nodes. Even though the network covers the large area by sensor nodes, the single node has only established the limited resources [2] but the sensor network consists of several thousands of nodes that used to collect the information also provide the valuable information to the destination. Due to the effective utilization of sensor nodes in different applications is utilized [3] such as health monitoring, military, ubiquitous monitoring, air quality prediction, target tracking and query-event application.

However, the wireless sensor networks utilized in different applications, it consists of only limited resources bandwidth, memory, energy and computing that leads to create the different passive and active attacks. Among the various attacks [4], cyber security is one of the most dangerous attacks because it affects the sensor network and make the resources unavailable while making the transaction. This DoS attack [5] may be occurred in different layers such as application (0verwheming sensor attack, deluge attack and path-based attack), transport (TCP SYN flooding attack, desynchronization attack), network (blackhole attack, vampire attack, misdirection attack, selective forwarding attack), physical (denial of sleep attack, exhaustion attack, collision attack, unfairness attack, interrogation attack) and link layer (jamming attack and tampering attack). The different types of attacks [6] leads to affect the entire sensor networks resources which may be cause the entire information transmission system. In addition to this, DoS attack affects the network CIA policy such as confidentiality, integrity and availability.

The main legacy of the paper is to eliminate DoS attack from the network by applying the effective technique because the resource and CIA security policy [7] must be managed while making the information broadcast due to the importance of the DoS attack in sensor network. So, in this paper analyze the energy efficiency routing protocol along with the extreme neural network [8] for analyzing the resources of the sensor nodes in sensor networks. The introduced method used to examine each node present in the network along with location, energy, power, and lifetime because the low energy sensor node may affect the entire communication process. Furthermore [19] the efficiency of the system assesses with the support of the experimental results in which the introduced system attains the low false alarm and high detection rate.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
A. Venkatesh*, School of Computing Science and Engineering, VIT University, Chennai, India.
S. Asha, School of Computing Science and Engineering, VIT University, Chennai, India.

Then the remaining instance of the paper is organized as follows, segment 2 discusses about the DoS attack in wireless sensor network. Section 3 evaluates the Energy Efficient

Extreme Learning Neural Network (EEELNN) based DoS detection process, Section 4 analyze the excellence of Energy Efficient Extreme Learning Neural Network (EEELNN) and concludes in section 5.

II. RELATED WORKS

This section discusses about various thoughts and ideas to recover the DoS attack in wireless sensor network. In [9] discussing the countermeasures and difficulties of DoS attack in the wireless sensor network. The DoS attacks entire network system and damage the network energy, battery power that leads to affect the entire network resource availability. So, the DoS attack has been eliminated by applying the energy efficiency routing protocol that successfully examines each node along with energy factor and the low energy node has been eliminated from the network before making the transaction. This energy efficient routing protocol also maintains the network security because it is difficult to access by the intermediate due to the successful examination of network nodes. In[10] introducing the message observation mechanism (MoM) for analyzing the network to catch and defense the DoS attack. The MoM method utilize the spatiotemporal information and the relationship between the data has been examined along with this similarity value is computed to detect the frequency and content attack in the network. In addition to this, MoM evaluate the route and rekey because the malicious node may interact while making the information transmission. So, the effective analyze of MoM process successfully detect and defense the DoS attack with effective manner.

In [11] analyzing various immune system based denial of service attack apprehension in wireless sensor network. The system analyzes the entire sensor network characteristics such as energy, power, battery and lifetime for train the immune system. In addition to this, the system utilizes the false alarm rate that helps to recognize the DoS attack with effectual. Then the excellence of the system is evaluated using tentative finish in which the immune system attains minimum false alarm rate but high DoS recognition rate. In [12] examines various data mining techniques such as k-nearest neighbor algorithm, random forest, support vector machine for catching the distributed DoS attack. The introduced machine learning techniques effectively examines and follows, cyber-attack patterns which used to prevent the DDoS attack in future direction. In addition to this, machine learning techniques analyze the issues; challenges involved by DDoS are examined effectively. In [13] proposing the intruder detector and manager system with traffic pattern filtering approach by applying the letter envelop protocol. For eliminating the DoS attack with effective manner, the method has been applied on the MAC layer. The algorithm maintains the network throughput, bandwidth and computation time because DoS attack mostly affect the network resources. Then [19] the competence of the system is evaluated with the help of tentative finish and deliberation.

III. ENERGY EFFICIENT EXTREME LEARNING NEURAL NETWORK (EEELNN) BASED DOS DETECTION

This section discusses about the Energy Efficient Extreme Learning Neural Network (EEELNN) based DoS detection process in the wireless sensor networks(WSN). The sensor network zone or area [14] has been selected for reducing the unauthorized activities initially. At the time of area selection process, sensor node energy has been computed which used to select the cluster head from the area. Depending on the intermediate and advanced nodes, the cluster head is selected. For every selected area, node (advancement and intermediate nodes) probability has been computed to select the cluster head in each zone. So, the advancement node optimal probability value is computed as follows.

$$p_{opt1} = \frac{k_{opt}1}{nm} \quad (1)$$

In eqn (1), k_opt 1 is represented as optimal number of clusters developed via the zone 1 and zone 3 (advancement nodes), the amount of advance nodes present in network is denoted as m and the total number of nodes in network is denoted as n. After computing thep_opt1, another probability value for intermediate node is examined in next zone which is done as follows,

$$p_{opt2} = \frac{kopt_2}{nb} \quad (2)$$

In eqn (2) kopt⟧ _2 is denoted as the optimal number of clusters in zone 2, the total number of nodes in network is n and b is intermediate nodes in network.

From the computed probability value, node energy is estimate. Let Ein, is the node initial energy, then the intermediate node energy is Eim=(1+μ) Ein and advancement node energy is Eia=(1+α)Ein. Depending on the initial energy, the total energy of advanced and intermediate node energy is computed. Then the advanced node zone energy is estimated as follows.

$$\begin{aligned} E_{tot1} &= nmE_{in}(1+\alpha) \\ &= nE_{in}(m+m\alpha) \\ &= nE_{in}m(1+\alpha) \end{aligned} \quad (3)$$

In eqn (3), α is represented as the energy of the node.
In addition to this, advanced node energy, intermediate node total energy is computed as follows.

$$\begin{aligned} E_{tot2} &= nE_{in}(1-m-b) + nbE_{in}(1+\mu) \\ &= nE_{in}(1-m+b\mu) \end{aligned} \quad (4)$$

In eqn (4), μ is represented as the energy of the node.

From the eqn (3) and (4), absolute energy of the network is estimated as follows.

$$\begin{aligned} E_{tot} &= E_{tot1} + E_{tot2} \\ &= nE_{in}m(1+\alpha) + nE_{in}(1-m+b\mu) \\ E_{tot} &= nE_{in}(1+m\alpha+b\mu) \end{aligned} \quad (5)$$

Based on the network energy, cluster head has been selected according to the particular conditions such as. If zone 2 intermediate nodes are considered as the cluster head, in time 1+μ for 1/p_opt2

(1-m+bμ) round in zone 2 iteration. If the zone 1 and zone 3 advance nodes are treated as cluster head if m(1+α) time with all 1/p_opt1 m(1+α) round in zone 1 and zone 3 iteration. So, the entire network cluster is

$$P_{opt} = k_{opt1} + k_{opt2} = nmp_{opt1} + nmp_{opt2} \quad (6)$$

After selecting the network clusters, node energy and absolute network energy, the minimum energy consumption node must be eliminated from the network for reducing the node failure, link failure and network failure. To broadcast the information without affecting the CIA security policy [15] of the sensor network, the process is continuously repeated. The computed network information energy, cluster information, network bandwidth and neighboring node information is maintained for improving the network efficiency. The collected information is processed by implementing the Extreme Learning Neural Networks. It is one of the effective supervised machine learning technique that used to detect the DoS attack related network features with minimum false rate. The network works according to the single layer feed forward network that consists of number of neurons, weights in between the connections and hidden layer. The utilized parameters are effectively used to reduce the computation complexity as well as improve the detection rate. Before analyzing the network features, neural network has to train according to the xenogenetic algorithm because it works according to the human brain and chromosome activity. The training process improves the overall DoS detection rate because of effective learning process. During the training process, the network utilizes the selection, crossover and mutation process. First the network features such as network zone, cluster information, energy, bandwidth and neighboring information is collected and create the neural network. After creating the neural network, fixed number of neurons, weights are chosen and the network is trained by applying the trainlm and trainscg training function. At the time of neural network training process, selection, crossover and mutation operators are used to chosen the weights as well as for optimizing the training parameter that used to reduce the false detection rate. Based on the trained features, incoming new network feature is analyzed and detected by applying the sigmoid activation function that is computed as follows.

$$G(a_i, x_j, b_i) = \frac{1}{1+e^{-(-a_i x_j + b_i)}} \quad (7)$$

Then the final classification is evaluated by applying the inverse operation technique to the output of the hidden layer. From the output, the network status has been identified easily also the neural network is trained by effective method which used to detect the intermediate attack with effective manner. Then the efficiency of the system is evaluated with the experimental results that are discussed as follows.

IV. RESULTS AND DISCUSSIONS

In this section analyze the excellence of the Energy Efficient Extreme Learning Neural Network (EEELNN) based DoS detection method. The EEELNN system is implemented in the NS2 simulation tool [19] and the obtained result is compared with the traditional DoS [19] detection methods such as Artificial Neural Network Based Detection (ANND) [16], multi-agent and refined clustering (MRC) [17] and entity-based fuzzy imperialist competitive clustering (EFCC) [18]. During this developing process, the system utilizes the following parameters that are shown in Table I.

Table- I: Simulation Parameter

Parameters	Values
Simulation Area	250 m2
Total No. of nodes	47 node (40 sensor node, 3 sink node, 6 relay node)
Medium Access Control	IEEE 802.15.4
Size of packet	40 bytes
Rate of Transmission	250kbps
Band Frequency	420MHz,868MHz, 2.4GHz
Channel mode	Log shadowing wireless model
Evaluation Parameters	classification accuracy, detection rate, false alarm rate and detection time
Simulation time	400sec
primary energy of normal nodes	0.5J
Primary energy of intermediate nodes	$(1+\mu)E_{in}$
primary energy of advanced nodes	$(1+\alpha)E_{in}$
Transmitting and receiving energy	50nJ/bit
probability value of advance node in cluster	0.2
probability value of intermediate node in cluster	0.105

Depending on the above simulations setup, the excellence of Energy Efficient Extreme Learning Neural Network (EEELNN) is analyzed using various performance metrics such as detection time, detection rate, classification accuracy, detection rate and false alarm rate which is discussed as follows.

A. Performance Metrics

Classification Accuracy (CA)-

CA is the process of defining amount of information which are correctly identified from the total amount of information. The CA is denoted in terms of true positive (TP), true negative (TN). Then the CA is computed as follows,

$$classification\ accuracy = \frac{TP+TN}{TP+TN+FP+FN} * 100\% \quad (8)$$

Detection Rate (DA)-

DA is the metric which is used to identify how accurately the unauthorized activities are happened in the network with effective manner which is computed as follows.

$$Detection\ Rate = \frac{TP}{TP+FN} * 100\% \quad (9)$$

False Alarm Rate (FAR)-

FAR is a measure used to detect the how the attacks are classified from the normal data which is estimated as follows.

$$FAR = \frac{FP}{FP+TN} * 100\% \quad (10)$$

Detection Time

It is the time taken to catch the DoS attack while broadcasting the information in the network.

B. Discussions

Depending on the performance metrics, the obtained results are evaluated in this section. The Energy Efficient Extreme Learning Neural Network (EEELNN) method effectively classifies the data while making the transaction. Then the obtained classification accuracy of different number of nodes are shown in Table II.

Table- II: Classification Accuracy

Number of Nodes	ANND	MRC	EFCC	EEELNN
10	82	83	85	91.23
20	83	84.3	85.6	92.34
40	83.5	84.8	86.7	94.3
50	84.1	85	86.98	95
70	85.3	85.6	87.32	96.2
80	84.78	86.2	87.68	96.78
100	86.4	86.8	88.32	97.6
120	87	89	88.98	98.2

The above Table II, clearly indicates that EEELNN method consumes high classification accuracy for different number of nodes such as 10,20,40,50,70,80,100 and 120. For overall, the EEELNN method consumes 95.20% when compared to other method such as ANND (84.515), MRC (85.58%) and EFCC (87.07%). The graphical representation of classification accuracy is shown in Fig. 1. which explained that the classification accuracy (normal and affected data packet) of the WSN network at the time of transmitting the information.

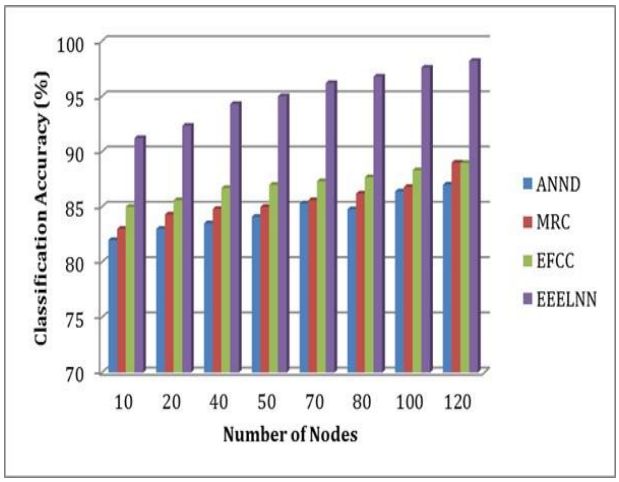

Fig. 1.EEELNN Classification Accuracy

The introduced EEELNN method successfully recognizes the packet with high classification rate which means it improves the overall detection rate means successfully recognize the attack affected data and node while making the transmission.

Table-III: Detection Rate

Number of Nodes	ANND	MRC	EFCC	EEELNN
10	83	85	87.3	94.6
20	86.4	87.9	91.42	95.7
40	88.2	91.3	93.78	96.3
50	87.5	93.2	94.1	97.4
70	88.8	92.5	93.65	97.8
80	89.1	94.3	95.21	98.2
100	85.6	91.2	93.2	99.4
120	83.8	92.2	94.35	99.6

The above Table III, clearly indicates that EEELNN method successfully detect the affected data with high detection rate for different number of nodes namely 10,20,40,50,70,80,100 and 120. For overall, the EEELNN method consumes 97.375% packet delivery ratio when compared to other method such as ANND (86.55%), MRC (90.95%) and EFCC (92.875%). Based on the Table III they obtained graphical representation of SQEZLMRP packet delivery ratio is shown.

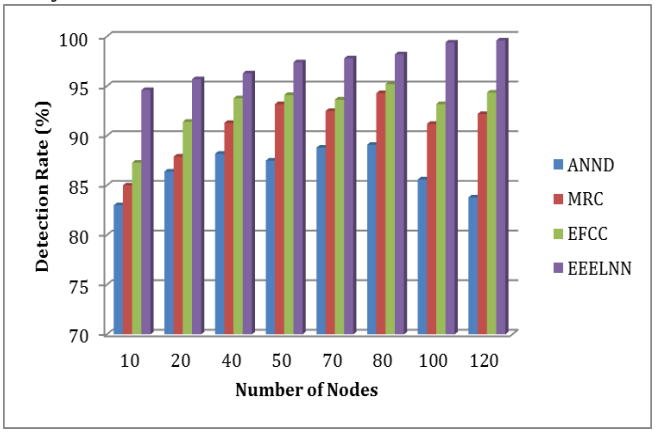

Fig. 2.Detection Rate

The above results are clearly shows that EEELNN methods successfully detect the abnormal activities and attacks with high classification rate and high detection rate. But the same time, the EEELNN method needs to reduce the false alarm rate. Then the obtained value is shown in Table IV.

Table-IV: False Alarm Rate

Number of Nodes	ANND	MRC	EFCC	EEELNN
10	0.542	0.493	0.321	0.046
20	0.587	0.501	0.402	0.0354
40	0.621	0.487	0.398	0.0435
50	0.547	0.489	0.378	0.0389
70	0.598	0.521	0.312	0.0462
80	0.531	0.423	0.364	0.0489
100	0.576	0.479	0.351	0.041
120	0.537	0.432	0.376	0.036

The above Table IV, clearly indicates that EEELNN method successfully transmit the data with minimum false alarm rate different number of nodes namely 10, 20, 40,50,70,80,100 and 120. For overall, the EEELNN method consumes 0.041 false alarm rate

when compared to other method such as ANND (0.56), MRC (0.47) and EFCC (0.36) Depending on the Table IV, the obtained graphical representation of EEELNN false alarm rate is shown in Fig. 3.

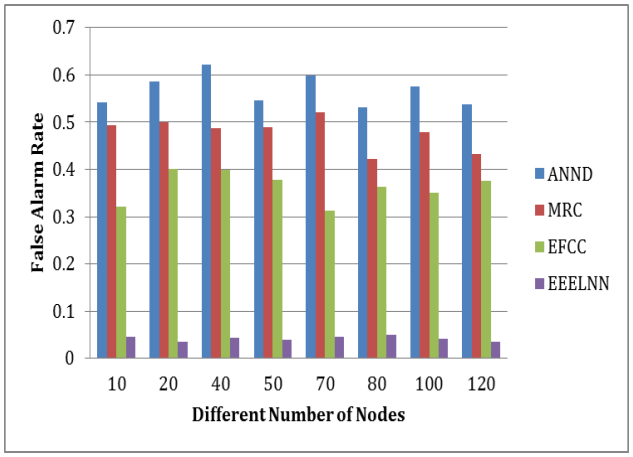

Fig. 3. False Alarm Rate

Depending on the results, the EEELNN method consumes minimum false alarm rate which helps to identify that EEELNN method successfully detect the DoS attack based data before transmitting data in the network. Even though the EEELNN method detects the attack related information with high accuracy, it should detect the attack with minimum detection time. Then the obtained detection time of different transmission node is shown in Table V.

Table -V: Detection Time

Number of Nodes	ANND	MRC	EFCC	EEELNN
10	57	52	48	41
20	64	61	53	51
40	79	65	64	62
50	112	98	88	83
70	147	121	104	92
80	175	138	113	100
100	210	169	145	114
120	264	175	162	121

In Table V clearly indicates that EEELNN method consumes minimum detection time for different number of nodes such as 10,20,40,50,70,80,100 and 120. For overall, the EEELNN method consumes 83ms when compared to other method such as ANND(138.5ms), MRC(109.875ms) and EFCC (97.125ms). The graphical representation of detection time is shown in Fig. 4.

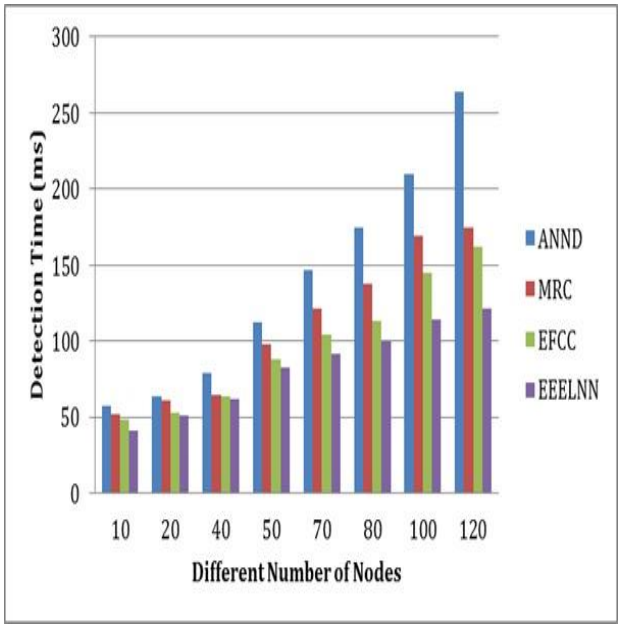

Fig. 4.Detection Time

Based on the discussions, the EEELNN method effectively detect the attack with minimum time, minimum false alarm rate, high classification and detection rate when compared to the other methods.

V. CONCLUSION

Thus the paper analyzes the Energy Efficient Extreme Learning Neural Network (EEELNN) based DoS detection process. Initially the network zone has been identified for reducing the unauthorized activities. From the detected zone, different advance and intermediate nodes energy has been computed for detecting the entire network energy. Along with the energy, neighboring node information, cluster head details are computed which is transmitted to the extreme learning neural network. The developed network train the features by utilizing the effective training function in which the network parameters are optimized by applying the xenogenetic parameters such as selection, crossover and mutation operator. After that incoming network features are examined and attack related features are detected by sigmoid activation function. Then [19] the excellence of the system is evaluated with the help of obtained experimental results in which the EEELNN method detect the attack with minimum false alarm rate (0.041), minimum time (83ms), high detection rate (97.37%) and high classification accuracy (95.20%) when compared to the other methods such as ANND, MRC and EFCC.

REFERENCES

1. E. Ekici, Y. Gu, and D. Bozdag, “Mobility-based communication in wireless sensor networks,” IEEE Communications Magazine, 2006, vol. 44, no. 7, pp. 56–62.
2. C. Chen, J. Ma, and K. Yu, “Designing energy-efficient wireless sensor networks with mobile sinks,” in Proceedings of the 4th ACM Conference on Embedded Networked Sensor Systems (SenSys '06), Boulder, Colo, USA, November 2006.

3. Peiris, V. (2013). "Highly integrated wireless sensing for body area network applications". SPIE Newsroom. :10.1117/2.1201312.005120
4. S.T.Zargar, J.Joshi and D.Tipper, ‖A Survey of Defense Mechanisms Against Distributed Denial of Service (DdoS) Flooding Attacks , IEEE Communication Surveys & Tutorials, 2013, vol.15, no . 4.
5. V.Priyadharshini and Dr.K. Kuppusamy, ‖, Prevention of DDOS Attacks using New Cracking Algorithm, ‖ International Journal of Engineering Research and Applications (IJERA), ISSN: 22489622, Vol. 2, Issue 3, MayJun 2012, pp.2263-2267
6. Virendra Pal Singh, Aishwarya S AnandUkey, and Sweta Jain. Signal strength based hello flood attack detection and prevention in wireless sensor networks. International Journal of Computer Applications (0975-8887), 2013.
7. M. Gunasekaran and S. Periakaruppan, "A hybrid protection approaches for denial of service (DoS) attacks in wireless sensor networks," International Journal of Electronics, 2017, vol. 104, no. 6, pp.993-1007.
8. Tang, Jiexiong, Chenwei Deng, and Guang-Bin Huang (2016). "Extreme Learning Machine for Multilayer Perceptron", IEEE Transactions on Neural Networks and Learning Systems. 27: 809–821.
9. David R. Raymond; Scott F. Midkiff, “Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses”, IEEE Pervasive Computing, 2008, Volume: 7, Issue: 1.
10. Yi-yingZHANG, Xiang-zhenLI, Yuan-anLIU, “The detection and defence of DoS attack for wireless sensor network”,The Journal of China Universities of Posts and Telecommunications Volume 19, Supplement 2, October 2012, Pages 52-56.
11. ShitalPatilaSangit, Chaudhari, “DoS Attack Prevention Technique in Wireless Sensor Networks”, Procedia Computer Science, Volume 79, 2016, Pages 715-721.
12. K.R.W.V.Bandara, T.S.Abeysinghe, A.J.M.Hijaz, D.G.T.Darshana, H.Aneez,.J.Kaluarachchi,K.V.D.L.Sulochana,andMr.DhishanDhammearatchi, “Preventing DDoS attack using Data mining Algorithms”, International Journal of Scientific and Research Publications, October 2016, Volume 6, Issue 10.
13. L. Arockiam, B. Vani, “Security algorithms to prevent Denial of Service (DoS) attacks in WLAN”,International Journal of Wireless Communications and Networking Technologies, volume 2, no 1, 2013.
14. L Qing, Q Zhu, M Wang, Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. Computer Communications: 2230-2237, 2006.
15. Gupta, B.B.; Joshi, C.; Misra, M. ―ANN Based Scheme to Predict Number of Zombies in a DDoS Attack‖. International Journal of Network Security, 2011, Vol.13, No 3, pp.216–225
16. N. A. Alrajeh, S. Khan, J. L. Mauri, and J. Loo, "Artificial Neural Network Based Detection of Energy Exhaustion Attacks in Wireless Sensor Networks Capable of Energy Harvesting," Ad Hoc & Sensor Wireless Networks, 2014, vol. 22, no. 1-2, pp. 109-133.
17. H.-b. Wang, Z. Yuan, and C.-d. Wang, "Intrusion detection for wireless sensor networks based on multi-agent and refined clustering," in Communications and Mobile Computing, CMC'09.WRI International Conference on, 2009, vol. 3, pp. 450-454: IEEE
18. S. Shamshirband, A. Amini, N. B. Anuar, M. L. M. Kiah, Y. W. Teh, and S. Furnell, "D-FICCA: A density-based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks," Measurement, 2014., vol. 55, pp. 212-226.
19. Torki Altameem, Mohammed Amoon, ”Crime activities prediction using hybridization of firefly optimization technique and fuzzy cognitive map neural networks,” Neural Computing and Applications,2018.

AUTHORS PROFILE

A. VENKATESH is a Research Scholar in the School of Computing Science and Engineering, VIT University, Chennai. he graduated B.Tech. from Anna University, Chennai and completed his M.E in Computer Science from Anna University, Chennai. Currently doing research in wireless sensor network security. His area of interest includes Network Security, Cyber Security and Block chain.

Dr. S. Asha is an Associate Professor in the School of Computing Science and Engineering, VIT University, Chennai. She graduated from Madras University, Chennai and completed her Ph.D from Anna University, Chennai. Her area of interest includes Network Security, Biometric Security, Computational Intelligence, Cloud Security and Cyber Security. She has published many papers in International Journals and Conferences. Currently she is working in Ambient Intelligent Group.