Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Protecting the WSN by Detecting and Disabling the Affected Sensor Nodes Using NN and SVM Approaches

Dr. G. Amudha[1], Dr. K. Ramkumar[2,*]

[1]Professor, Department of Computer Science and Business Systems, R.M.D. Engineering College, Tiruvallur, Tamil Nadu - 601 206,Mail: gav.csbs@rmd.ac.in

[2]Professor, Department of Computer Science and Engineering, SRMIST, Vadapalani Campus, Chennai, Tamil Nadu - 600 026.

*Corresponding Author: Dr.K.Ramkumar, Mail id: ramkumar1975@gmail.com

Article Info
Page Number: 74 - 89
Publication Issue:
Vol 72 No. 1 (2023)

Abstract

Maintaining Wireless Sensor Network (WSN) security is one of the most important ways to monitor real-time systems in general.Denial-of-Service (DoS) attack is one of the most important things that interfere with the safety of WSN; this is because the attack suddenly shut down the network. Moreover, this attack can mislead the results of the system. So this paper uses two types of techniques to detect attack in MAC layer.That is, it handles two of the most advanced systems in machine learning. One of them is the Neural Network (NN) and the other is the Support Vector Machine (SVM) method. In simulation, the parameters which are critical and normalized are calculated as well probabilities of the associated Denial of Service attack calculated in the test runs.The above calculated values are used as inputs for training the system in SVM and NN. In the simulation results, accuracy of the result by using SVM is more accurate compared to NN's method.Both Support Vector Machine and Neural Network methods are very useful in determining the percentage of possibility of DoS attacks in Wireless Sensor Network.

Keywords: WSN; Security; DoS; Machine Learning Techniques.

Article History
Article Received*: 15 October 2022*
Revised*: 24 November 2022*
Accepted*: 18 December 2022*

I. INTRODUCTION

The information regarding various events or an information about any objects are gathered by various sensors. Most sensors are used wirelessly to connect to a processing station and collect data. Environment where these sensors are deployed is been monitored, and these collection of sensors will be termed as wireless sensor network. Memory, security, Energy, computational skills and communication bandwidth are the main obstacles for WSN. There are a lot of obstacles when it comes to fixing safety concerns for WSN. Security enhancement techniques have requirements such as information storage and communication. They further control the sensor nodes. Also in Wireless Sensor Networks, because of variousconstraints due to centralized system having a focal point is the opposite of practical.

In-order to overcome the shortfall of the centralized WSNs , there is a necessity to the development of a decentralized systems. It is also critical to have a decentralized security solution which performs better. Many WSNs are overlooked as they active in hidden and distant places. It is therefore a very difficult task to prevent and continuously monitor the sensor nodes from attacks. WSN is used in a variety of applications such as military, health care, disaster relief operations, machine surveillance, biodiversity mapping, precision agriculture, and machinery[14].

But, the WSNs are greatly affected by a variety of attacks[14]. Therefore, it is very important to test the safety of WSN in such applications.There are two types of machine learning techniques are used in this paper, namely, SVM and NN. WSN performance can be improved by detecting DoS attacks and preventing them with these methods. The SVM and NN methods are used to operate monitoring nodes and stop work immediately if attacks are detected. Cyber attackers can listen to news, break sensor nodes, waste network resources, change data integrity, and inject fake messages. Distributed DoS (DDoS) attack or DoS attack is one of the most serious attacks that threaten WSN security.

DoS attacks can disable the web application and service, the web site. This attack is to shut down the network resources by sending too many fake requests. Proper traffic prevents access to the network until the attack stops. Prevent and avoid security threats, and detect unknown and known attacks, machine learning methods such as NN and SVM are heavily used.

This machine learning methods detect suspicious and unusual activities, and warning when intrusion occurs. In WSNs, the use of machine learning is more difficult than other types of network. This is because the sensors are small and the hardware used is cheap. Therefore, such routines are not practiced in WSN, to solve complex problems.

II. LITERATURE REVIEW

In WSN, many types of attacks are detected and classified by A. Kar and H. K. Kalita [1]. Enemies can launch a number of attacks, such as DoS, which attack the services of WSN. DoS attacks can occur in any layer of WSN [2] [3][14]. Preventing DoS attacks [14] is a critical issue in the security of the temporary sensor network [4]. Although cryptography methods are effective in preventing DoS attacks [5], due to resource constraints, they cannot be used in WSN. Even so, DoS attacks can be reduced by identifying malfunctioning nodes[14].

The MAC algorithm based on A Hybrid Intelligent Intrusion Detection System[15] (HIIDS) and fuzzy logic system, detected malfunctioning nodes [6] [7]. They are therefore used to diagnose DoS attacks.Fuzzy logic system based MAC algorithm only uses the fuzzy inference approach[14] to make a decision. The HIIDS system [15] uses an addition-based on NN approach to learn attack definitions. But the HIIDS have somewhat solved the problem of identifying the attacks.

In real-world applications, Marti Hearst said that the use of complex methods such as NN is difficult to analyze [8]. But with the SVM method, it can be learned more accurately, and it is very useful for mathematical analysis. On WSN's MAC layer, this proposed method compares SVM and NN's effectiveness in detecting and countering DoS-launched attacks by the enemy. The method of NN is trained using the Back Propagation (BP) method.Attack definitions are learned by sensor nodes.So if this algorithm finds attacks, they will cease to operate until the enemy moves away from their position.To improve WSN security, using machine learning techniques such as SVM and NN, WSN develops a protocol for safety. When it overcomes to attacks, only the affected sensor node is needed to temporarily close itself. The infected node reactivates when its attack ends, without affecting its neighboring nodes.

III. PROPOSED METHODOLOGY

1. Denial of ServiceAttack Detection

Network services are been damaged by means of Denial of Service attack. In a DoS attack, malicious nodes can be degraded by the demand for services provided by legitimate nodes. The MAC layer of the WSN is depending on Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) protocol[14]. This CSMA-CA protocol depends on the interchange of clear-to-send (CTS) and ready-to-send (RTS) control packets[14].When sending data to a source node, by sending it to the RTS packet, that starting the process. The RTS pocket silences any nodes that hear it. If the target node receives a RTS, it answers with CTS[16].

Like the Request To Send Packet, the Clear To Send Packet also instantly calms adjacent edges. When the Clear To Send and Request To Send exchange is complete [17], the source node transmits data without interfering with any other nodes.Data packets are positively acknowledged.In various layers of the protocol layer, different types of DoS attacks occur. In the Mac layer, there are three types of DoS attack:

1. The Exhaustion Attack
2. The Unfairness Attack
3. The Collision Attack

Exhaustion attack[14]:

When a sensor node receives a RTS control packet, it agrees with CTS control packet. Because attackers are normal ends, it is not possible to know whether the Routes packets are sent by normal nodes or by the attacker. Under this condition, this causes the enemy to send large numbers of RTS packets to the normal nodes. They agree with CTS packets, this discharging the battery life of the receivers.

Unfairness Attack[14]:

All channels have the same priority to access the same channel. Based on the FCFS (First Come First Serve) principle, the channel is assigned to the nodes. This means that for the first

tried nodes, first the access to channel is provided[18]. Under this rules, enemies send a large number of packets to waiting for a short time. This action prevents the use of a same channel.

Collision Attack[14]:

Before sending out CTS and RTS packets, to determine if that channel is dormant or busy, all nodes also feel the channels. When prevent packets of data and prevent conflict, only if the channel is inactive, that carries out data transfer. Under this command, enemies with sensor network packets, attacking by floods can cause conflict[19].

This proposed method, to find out the probability of attacks, the following uses some important parameters:

Collision Rate (C_R) : C_R is the number of collisions recognized by a node in a second[14].

RTS arrival Rate (R_R) : R_R is the no. of RTS packets accepted fortunately over a node in a second.[14].

Average waiting time (W_T): W_T is, before the exchange, in the MAC buffer is the wait time of a packet.[14]

The important parameters above are tracked for different probabilities of attack from 0.1 to 1. The value of the W_T is negligible compared to the C_R and R_R values. Therefore important parameters such as C_R and R_R are used to determine the probability of DoS attack.

In the NN-based method, the parameters R_R and C_R are denoted as inputs. And the probability associated with the attack is referred to as MLP (Multi-Layered Perceptron) targets. MLP is practiced by BP algorithm. At each end, the MLP is dependencies derived from trained MLP and activated with pre-defined weights.Every node, every minute, it sends the calculated values of its R_R and C_R to its MLP. This creates the output. If the output of MLP is greater than the preset threshold value P_T, the node closes itself temporarily[20].

In the SVM based method, the probability of an attack is divided into two categories. That is high and low.The most important parameters taken from these two classes are R_R and C_R, is trained to the SVM classifier. Each minute, every node, its main parameters are R_R and C_R, sends to a trained SVM classifier. The probability of an attack can be classified as high or low.

Detecting the high likelihood of an attack, the node will shut itself down once the attack is over and reactivated.

2. Neural Network Based Architecture[14]:

Multilayer Perceptron [14] is just one type of NN. MLP is the FFNN (Feed forward NN). The neurons are arranged in multiple layers. The last layer contains output units and the first layer contains input units. Other hug sizes are called hidden units. They are all hidden layers. Through the communications links that each neuron has enabled are combined with other neurons. In every communication link, there is a corresponding weight. The information in the neural network is represented by weights. Each neuron has a condition called activation[14]. The structure of the MLP used in this proposed method is given in Figure 1. It has a hidden cascade, wherein P_1 and P_2 are input units, $Q_1$is the output unit. Hidden unit R_1 also has dependencies. The bias on output unit Q_1 is indicated by V_{01}. The angle on hidden unit $R_1$is denoted by U_{01}.HTSF (Hyperbolic Tangent Sigmoid Function)[14]is the activation function applied to hidden layer. This function is defined in Fig.2. It is computationally identical to 1,

$$b = f(a) = \tanh(a) \qquad (1)$$

The linear function is the activation[14] function applied to output layer. This is demonstrated in Fig.3. This function is calculatedly complemented to 2,

$$b = f(a) = a \qquad (2)$$

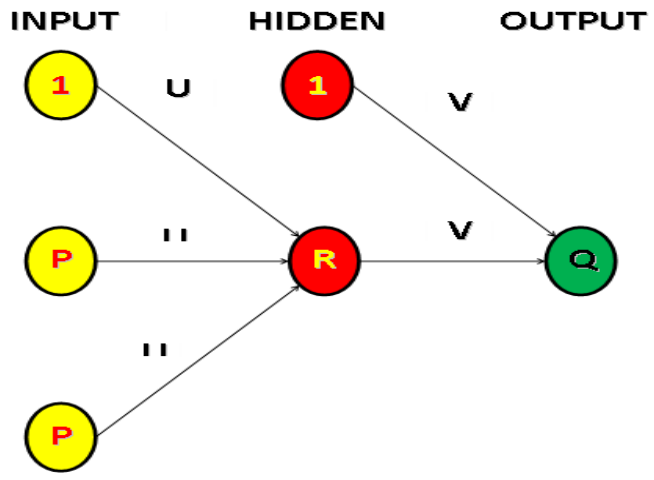

Fig.1: Structure of MLP

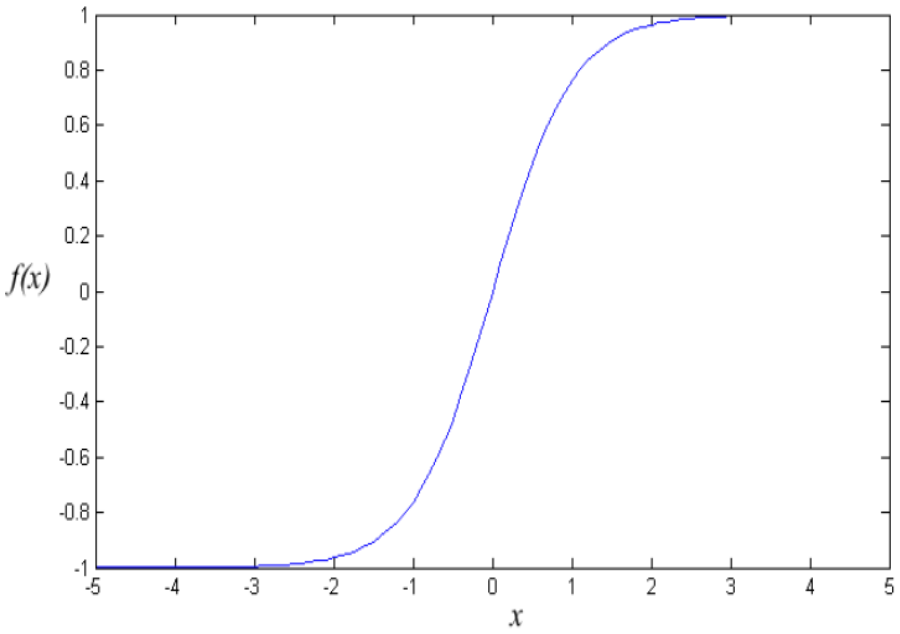

Fig.2: HTSF

Training Algorithm

MLP is practiced utilizing BP algorithm. It requires 3 steps:

1. Feedforward of an input pattern.
2. BP and calculation of associated error.
3. Weights adjustment.

Whenfeed forward, every i/p unit P_k, (k= 11, 12) receives i/p signal P_k and broadcasts it to the hidden unit R_1. R_1 collections its weighted i/p signals as expressed in 3,

$$R_{in} = U_{01} + \sum_{j=11}^{12} P_k U_{j1} \qquad (3)$$

As stated on Equation 4, R1 using its activation function, it calculates its output signal. This sends that signal to the output unit Q_1,

$$R_1 = f(R_{in}) \qquad (4)$$

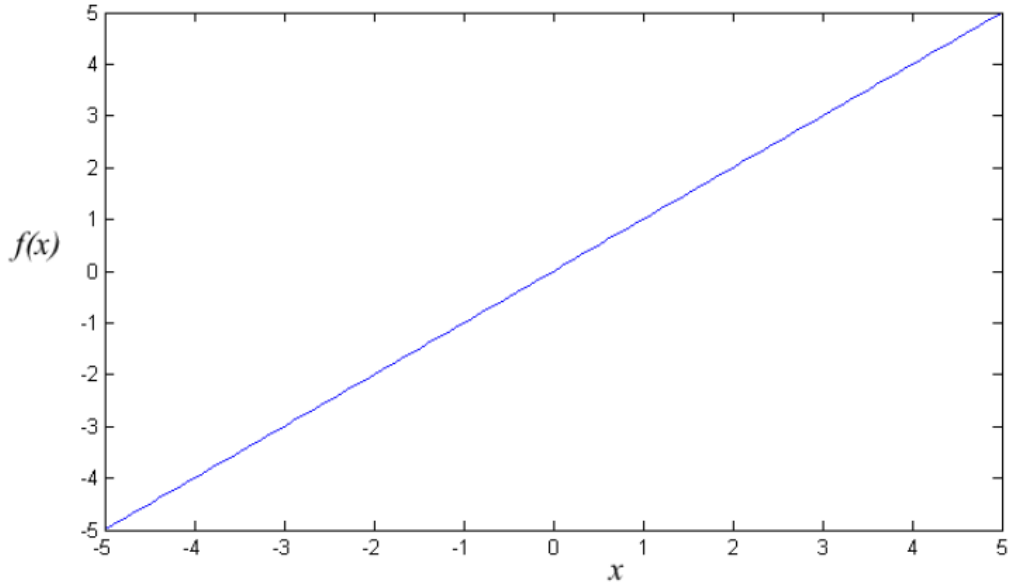

Fig.3: Linear function

As shown in equation 5, the output unit Q_1 compiles its inputs and weighs the input components.

$$Q_{in1} = V_{01} + R_1 V_{11} \quad (5)$$

As stated in equation six, Q_1 calculates its output signal using its activation function.

$$Q_1 = f(Q_{in}) \quad (6)$$

During training, Q_1 compares its target value to T_1. Based on this error, factor [14]F_1 is calculated. F_1 is used to spread the error in the output unit Q_1, to the hidden unit R_1. The weights between the hidden layer and the release layer is been refreshed by using the factor F_1. Similarly the weights between input stack and hidden stack are updated. NN takes several epochs to get the training through the BP. The BP algorithms mathematical basis is slash descent.

3. SVM Based Mechanism

SVM is the number one learning in classification learning. It is utilized for different purposes that mean classification, pattern recognition, denoising, etc. As for this paper, SVM is used to identify the probability of an attack. The input data for the training is provided to the learning machine. Training data is data that is labeled in binary form. This refers to the high and low probability of an attack. The SVM method of this learning machine is to find the maximum

separation hyperplane. And it is to discover the planes between two boundaries. It divides into two classes. One is the low probability of an attack and the other is the high probability of an attack. The lower probability of an attack is denoted as L or -1. And the higher probability of an attack is denoted as H or +1.

Notice the training data set pairs (A_j, $Z1_t$), j = 1, ..., x.

Where,

A = input vector with n dimensions

Z=target vector with m dimensions

In which $Z1_t$ belongs to {minus 1, plus 1} denotesa particular class where $A_i$owned.

Hyperplane with greatest separation $\rightarrow W_T A - \gamma 1 = 0$

The bounding hyperplanes $\rightarrow W_T A - \gamma = \pm 1$

with,

W = coefficient vector with n dimensions

$\gamma 1$ = biasing term

'L' vector or '-1' which satisfies the constraint $W_T A - \gamma 1 \leq -1$ and the input vector including to 'H' or '+1' class convincing the constraint $W_T A - \gamma 1 \geq 1$. In this scenario some errors are avoided, thus, some input direction has the potential to deviate from the respective boundary plane. A positive quantity is called as slack variable (ξ). It is subtracted or added to the input vector to convince the hindrances. Thus the new barriers can be written as follows,

$$W_T A - \gamma 1 + \xi \leq -1 \quad (7)$$

$$W_T A - \gamma 1 - \xi \geq 1 \quad (8)$$

SVM main goal is to effort for maximum margin between minimum number of input vectors and the bounding planes giving to error.Maximum margin is reached by decreasing the $\frac{1}{2} W_T W$. Minimum error is attained by reducing $\sum_{j=1}^{m} \xi_j$.

The main form of equation is given by,

$$\min_{\xi,W,\gamma} \frac{1}{2} W_T W + B \sum_{j=1}^{m} \xi_j \quad (9)$$

Subject to barriers,

$$Z_t (W_T A_j - \gamma) + \xi_j - 1 \geq 0,\ 1 \leq j \leq m \quad (10)$$

$$\xi \geq 0,\ 1 \leq j \leq m \quad (11)$$

Where,

'C' = the penalty parameter

The maximum margin and the sum of the error is been limited. The value of the penalty parameter gives the best generalization capacity to the classification algorithm. $\min_{\xi,W,\gamma} \frac{1}{2} W_T W + B \sum_{j=1}^{m} \xi_j$ is converted to double forms, and then solved, using such quadratic programming. The solution is based on Lagrangian amplifier. The main variables W, ξ and γ are calculated from these Lagrangian multipliers. If this algorithm wants a better solution, input space is converted to space φ (Aj) with more number of dimensions. Then the hyperplane is split as maximized in that space.

IV. RESULTS AND DISCUSSION

A. Numerical Results

Figure 4 shows the observation of important parameters in WSN. It consists of sixteen sensor nodes with unique identifiers ranging from one to sixteen. Through the control scheme, nodes CTS/RTS exchange data. Each node, every 0.16 seconds, tries to smuggle a packet with probability P. When two nodes are transmitted simultaneously, fights the receiver. The number of RTS packets receiving a node, the demand rate is measured as R_R. collision rate C_R gives the average number of collisions in a minute. Fifty test runs are conducted and the values of the parameters specified are calculated with different probabilities of DoS attack from 0.1 to 1.These values are then normalized.

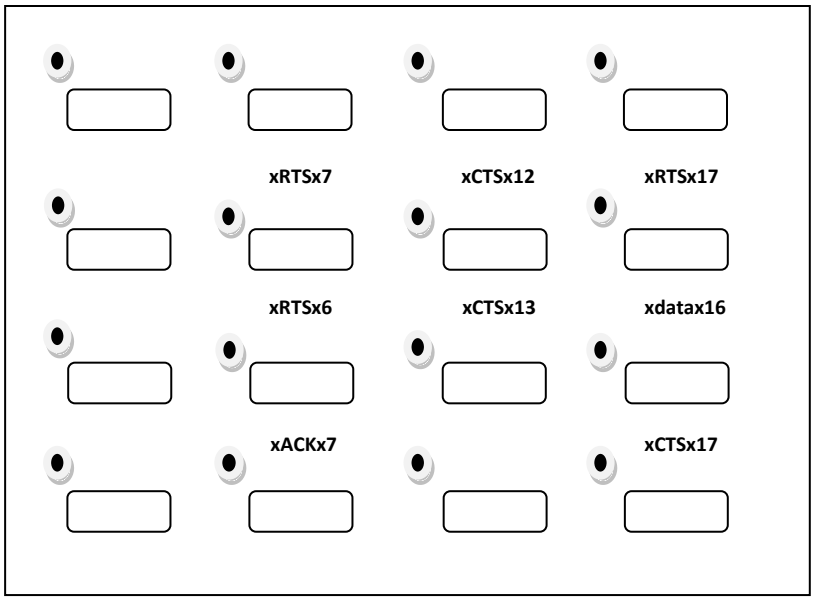

Fig.4: Computing Critical Parameters using WSN

In table 1, the values of these parameters are shown in different probabilities of attack.In the proposed method, the graphs show the values with normalization of these parameters. By increasing the probability of an attack, table 1 shows the increase of R_R and C_R. The normalized values of these parameters and the probabilities associated with them, in the SVM approach and the NN approach, training is used as input.

Table I: *Average of complex parameters over fifty test runs*

Probability of Attack	**C_R**	**R_R**
0.1	110.286	393.9
0.2	124.44	506.2
0.3	135.12	535.74
0.4	163.34	652.4
0.5	177.4	717.4
0.6	220.02	921.74
0.7	239.96	991.74
0.8	260.34	1056.48
0.9	280.88	1131.34
1	301.66	1190

B. Using the NN based method, protection against DoS attack

In figure five, it is shown that some nodes have stopped their work. Those nodes are the one who have detected the attack and are marked in red. These attacks are in the next minute, when no one attacks is detected, they are starting to all active and engaged in exchange activities.

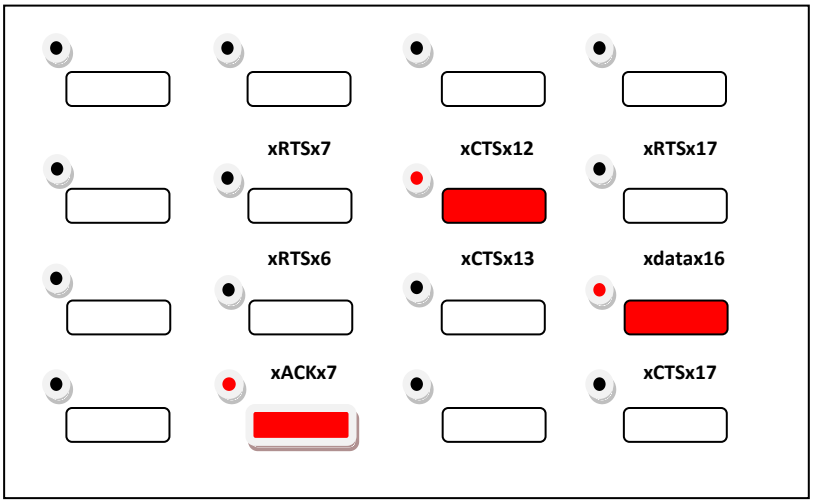

Fig.5: Attack Detection using NN

C. Using SVM protection of DoS attack

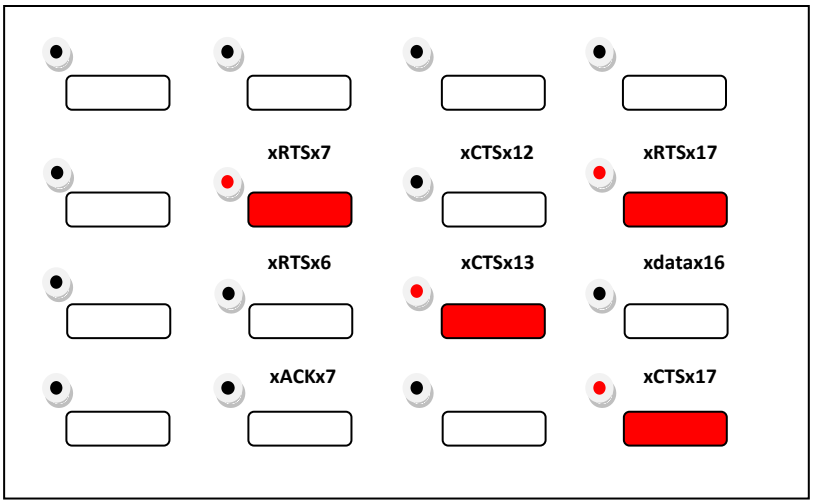

Fig.6: Attack Detection using SVM

The main parameters that are normalized are notifying the attack. The probability of an attack is classified as more or less. Turning off the detection of the attack in the figure also stopped working. We can see these ends are run with red LEDs. Similar to the NN system, if there are no attacks, all nodes will return to its normal function.

D. Performance Analysis

Figure 7 shows, in determining the DoS attack, the accuracy of the NN and SVM methods and the time them took. Accuracy depends on how correctly the algorithms detect attacks. Similarly, time is depends on the mechanisms are take how much time to detect attacks.

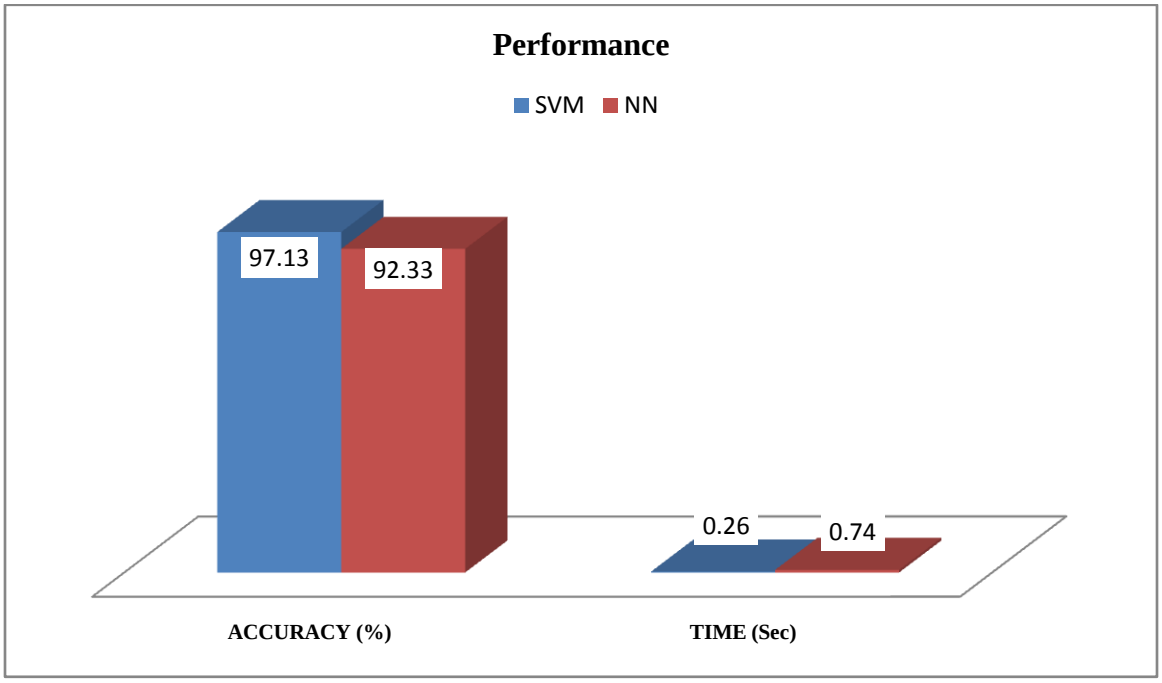

Fig.7: Performance Analysis

So, SVM's accuracy is 97.13 percent, and the accuracy of the NN is 92 percent. Therefore the accuracy of SVM is greater than that of NN. For SVM and NN, the time taken to detect DoS attacks is 0.26 and 0.74. So the SVM method is found in a much shorter time than NN.

CONCLUSION

Here, two types of machine learning methods, SVM and NN, were used to detect DoS attacks. All of these methods are based on a supervised learning system and trained with them. With this approach, if the attacking nodes stop working, power and network are not wasted.

Thus, money can be reduced and the life of the network extended. NN is a method of solving problems that a program cannot solve. SVM solves many complex problems based on the kernel method. When examining these two techniques, the accuracy of the SVM is 97% and the accuracy of the NN is 92%. Moreover, SVM took less time to detect attacks than the NN. So the SVM method has given much better results than NN.

REFERENCES

1. Waltenegus Dargie, Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", ISBN: 978-0-470-97568-8, November 2010.
2. Hemanta Kumar Kalita1 and Avijit Kar, "Wireless Sensor Network Security Analysis", International journal of computer science & information Technology (IJCSIT), vol. 1, no. 1, December 2009.
3. Harikrishnan, G., & Rajaram, A. (2006). Enhanced Packet Covering And Stitching Over Man In The Middle Attacks In Wireless Sensor Network.
4. Sridevi, A. P., & Rajaram, A. (2014). Efficient Energy Based Multipath Cluster Routing Protocol For Wireless Sensor Networks. *Journal of Theoretical & Applied Information Technology*, *68*(2).
5. Q. Ren and Q. Liang, "Fuzzy logic-optimized secure media access control protocol for wireless sensor networks," in Proc. IEEE Intimation Conference on Computational Intelligence for Homeland Security and Personal Safety, pp. 37 – 43, 2005.
6. Rathish, C. R., & Rajaram, A. Hierarchical Load Balanced Multipath Routing Protocol for Wireless Sensor Networks.
7. Rajaram, A., & Kannan, S. (2014). Energy Based Routing Algorithm For Mobile Ad Hoc Networks. *Journal of Theoretical & Applied Information Technology*, *61*(3).
8. D.-R. Tsai and C.-F. Chang, "A hybrid intelligent intrusiondetection system to recognize novel attacks," in Proc. IEEE 13th AnnualInternational Carnahan Conference on Security Technology, pp. 428 –434, 2003.
9. Joseph, S., & Rajaram, A. (2017). Efficient secure and fair cluster routing protocol: An improved bee colony optimization cluster based efficient secure and fair routing

protocol for mobile ad hoc network. *Journal of Computational and Theoretical Nanoscience*, *14*(7), 3503-3509.

10. K. Venayagamoorthy, R. V. Kulkarni, A. V. Thakur, and S. K. Madria,"Generalized neuron based secure media access control protocol forwireless sensor networks," in Proc. IEEE symposium on Computationalintelligence in multi-criteria decision-making, pp. 16 – 22, 2009.
11. Anitha, B., & Rajaram, A. (2014). Efficient Position Based Packet Forwarding Protocol For Wireless Sensor Networks. *Journal of Theoretical & Applied Information Technology*, *69*(2).
12. Harikrishnan, G., & Rajaram, A. (2017). Improved throughput based recognition connection denies for aggressive node in wireless sensor network. *Journal of Computational and Theoretical Nanoscience*, *14*(12), 5748-5755.
13. K. Venayagamoorthy, R. V. Kulkarni "Neural network basedsecure media access control protocol for wireless sensor networks," inProc. International Joint Conference on Neural Networks, pp. 13 – 16,June 2009.
14. Karthikeyan, T., & Rajaram, A. (2014). Efficient Multicast Data Replication Approach For Power Consumption In Manet. *Journal of Theoretical & Applied Information Technology*, *69*(2).
15. Rajaram, A., & Lingam, S. V. (2011). Distributed Adaptive Clustering Algorithm for Improving Data Accessibility in MANET. *International Journal of Computer Science Issues (IJCSI)*, *8*(4), 369.
16. S. Mithila.T, Hemalatha.T, and Soman.K.P, "Comparative study of linearand quadratic programming versions of svm on various real life datasets," International Journal of Recent Trends in Engineering, vol. 1,no. 2, pp. 23 – 25, May 2009.
17. Aswathy B. Raj , Maneesha V. Ramesh , Raghavendra V. Kulkarni and Hemalatha T," Security Enhancement in Wireless Sensor Networks using Machine Learning", IEEE 14th International Conference on High Performance Computing and Communications, DOI 10.1109/HPCC.2012.186, 2012.

18. Rathish, C. R., & Rajaram, A. (2017). Robust early detection and filtering scheme to locate vampire attack in wireless sensor networks. *Journal of Computational and Theoretical Nanoscience*, *14*(6), 2937-2946.

19. Sohail Saif, Priya Das, Suparna Biswas, Manju Khari, Vimal Shanmuganathan," HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare", Microprocessors and Microsystems,2022,104622,ISSN0141-9331

20. Kannan, S., & Rajaram, A. (2012). QoS Aware Power Efficient Multicast Routing Protocol (QoS-PEMRP) with Varying Mobility Speed for Mobile Ad Hoc Networks. *International Journal of Computer Applications*, *60*(18).