FEM – Hybrid Machine Learning Approach for the Detection of Sybil attacks in the Wireless Sensor Networks

V. Sujatha, E.A. Mary Anita

Abstract: ***Wireless Sensor networks finds its application in various areas such as habitat monitoring, home automation, industrial automation, military applications and health care etc. Even though Wireless sensor networks are omnipresence, they are vulnerable to the various security threats. Sybil attacks are considered to be one of the most important attacks for which the several detection algorithms and systems were designed and implemented. But still the existing algorithms need intelligence for better accuracy of detection. Hence new technique FEM(Fuzzy Extreme machines) is proposed which works on the hybrid Fuzzy and powerful Extreme learning machines for the detection of Sybil attacks. The experiments were conducted on real time Testbeds which consist of ARM as main CPU interfaced with CC2530 Zigbee transceivers and tested in LEACH environment. Results in terms of accuracy detection obtained from the FEM approach proves to be more vital when compared with the other existing classifier algorithms.***

Keywords: ***FEM, Fuzzy, Extreme Learning Machines, Sybil Attacks, LEACH***

I. INTRODUCTION

A wireless sensor network (WSN) consists of a large number of sensor nodes and a base station (BS). These sensors collect data and send them to the BS via radio transmitter. They have limited power and computational capacity. WSNs can be used in many applications such as military, biomedical, and environmental applications.

Even though Wireless Sensor Networks are implemented in thevarious application areas, data stealing in terms of the various attacks are the major threat to the users. One such threat is Sybil attack in WSN, which predominantly occurs during the routing as shown in Fig.1

In Sybil attack an individual identity appears as multiple simultaneous identities in the network as shown in Fig.2.In other words a particular node in the network is present at more than one place simultaneously. This attack was first observed in p2p networks. Sybil attack washes the original nodes and prevents the original nodes to use the resource completely which causes violations in the one-to-one mapping between entity and identity.

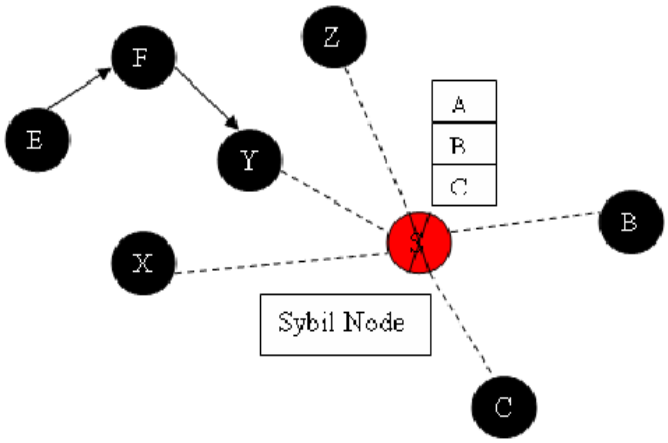

Fig. 1 Shows Sybil Attack occurrence in Wireless Sensor Network Systems

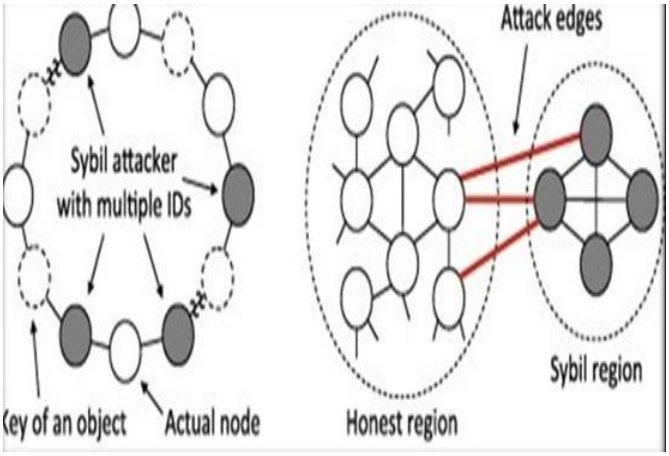

Fig. 2 Shows Sybil Attack occurrence as Multiple IDS in Wireless Sensor network Systems

Several machine learning algorithms such as Support Vector Machines(SVM), Naïve Bayes (NB) Classifier, Clustering techniques, Neural Networks (NN) were used for the detection of attacks in centralized wireless sensor networks which are listed in table I.

Revised Manuscript Received on May 07, 2019.
V. Sujatha, Research Scholar, AMET University, Chennai, India
E.A. Mary Anita, Professor/ CSE, S.A. Engineering College, Chennai

Table. 1 Illustration of the different Machine Learning algorithms for Detection of Attacks

Reference	Network Topology	Type of attacks	Machine Learning algorithms	Learning Model	Data Used	Accuracy
Kaplantzis et al. [16]	Flat	Selective Forwarding and Black Hole Attacks	SVM	Supervised	Simulation Data	80%
Sa and Rath [17]	Flat	Sybil attacks and other attacks	Naïve Bayes	Supervised	KDDCUp99 Datasets	98%
Warriach and Tei [18]	Flat	Blackhole attacks and selective forwarding	Hidden Markov Model	Supervised	Simulated Data sets	90%
Kaur and Singh [19]	Flat	Black hole attacks	J-48	Supervised	Simulated Data sets	89%
Culpepper et al. [20]	Flat	Sinkhole attacks	Cross validated algorithms	Supervised	Simulated Data sets	78%

The proposed FEM is the hybrid approach which works on the principle of fuzzy logic and extreme learning machines. The FEM uses the Fuzzy Logic principle in detection of the secured cluster head.With the fuzzy output, RSSI and distance are used for training the Extreme Learning Machine for the detection of the Sybil attack.

The experimental Test bed has been designed with the ARM as Central processor interfaced with the Zigbee transceivers for the collection of real time data which are used for the training and testing the algorithm.

II. RELATED WORKS

Udaya Suriyaet al [1]appliedMessage authentication and Passing method for checking the trustworthiness or otherwise for a Sybil node. The action of a node as a Sybil node with duplicate ID and information can happen only when the node has complete information about the other nodes. Verification of the node needs the application of CAM-PVM. Instead of wasting time for CAM-PVM to check each and every node, the message authentication and passing procedure is applied for authentication prior to communication. If a node does not have any authorization by the network or by the base station, it cannot communicate with any other node in the network. The message authentication and passing method is so effective and is known for more time consuming than any other method.Message authentication and Passing method requires modification and reduction in time consumption. The size of the network is not a constraint. The throughput of the network should be higher than the other security algorithm which is applied earlier in the network security

Sunil Ghildiyal et al [2]discussed about Limited processing capability and less power of WSN nodes to make them much susceptible for number of attacks. Nodes save limited resources and they have to be protected by some support from outside them like any powerful device within the network like BS. BS can only execute complex security processing and algorithms for security of entire network. Proposed solution against Sybil attack is based on pre-distributed keys of sensor nodes, embedded the time of manufacturing stage. Keys are pre-distributed as it is not recommended to distribute the keys through unsecured wireless network links. Solution resists Sybil attack but,base station processing and its I/O traffic is going toincrease heavily which is certainly a problem, is to beaddressed in future solutions .

RSSI based Sybil attack detection technique and their related issues indifferent networks framed by S. Abbas et al [3]. They also proposed a design whichuses only one-time localization to detect Sybil attacks.This novel aspect has the potential tosignificantly reduce the overhead of periodicdissemination of location information. A localization algorithmwith good accuracy was developed by them. Trust or Reputation mechanism tightly coupled with thelocalization process was used to give preference to the trusted node's reports.

S. Sharmila et al [4] studied a number of existing methodologies for the detection of Sybil attack and an algorithm is proposed for detection of Sybil attack in wireless Sensor Network. The throughput and packet delivery ratio of the network before and after detection is analysed for different traffic rates. It is found that throughput and packet delivery ratio after detection has improved.

K.-F. Ssuet al [5] developed a scheme in which the node identities are verified simply by analysing the neighbouring node information of each node. The analytical results confirm the efficacy of the approach given a sufficient node density within the network. The simulation results demonstrate that for a network in which each node has an average of 9 neighbours, the scheme detects 99% of the Sybil nodes with no more than a 4% false detection rate. The experiment result shows that the Sybil nodes can still be identified when the links are not symmetric.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

A. Vasudeva et al [6]have discussed the Sybil attack in context of how it can disrupt the head selection mechanism of the lowest ID based clustering scheme for routing in MANETs. The Sybil attack has been illustrated through two different ways: lowest ID Based Sybil Attack and Impersonation based Sybil Attack. In lowest ID based Sybil attack, a malicious node can become Clusterhead by presenting a Sybil node with lowest ID. The attack becomes more devastating and difficult to be detected if the malicious node presents its fake identities by varying the transmission power. It takes the advantage of varying the transmission power in two ways: First, it cannot be detected on the basis of same signal strengths of its Sybil nodes. Second, by decreasing the transmission power for different Sybil nodes, the message will not reach all the neighbours of the malicious node and hence it cannot be detected on the basis of the fact that if a set of nodes are seen together for a long period of time by an observer node, then they are suspected to be the identities of Sybil attacker

The different kinds of Sybil attacks including those occurring in peer-to-peer reputation systems, self-organising networks and even social network systems are discussed by N. Balachandaran et al [7]. In addition, various methods that have been suggested over time to decrease or eliminate their risk completely are also analysed along with their modus operandi.

G.Padmavathi et al [8] summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanisms widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed.

A framework been proposed by G Jing-Jing [11] in which the vulnerabilities from the Sybil attack for ad-hoc routing protocol were modelled in a mathematical approach and the formal analysis is carried out with a specific proof system under the extended strand space model in order to further verify the validate the threats from the Sybil attack.

C. Komar et al [12] introduced the notion of Trespassers' favourite paths (TFP) and provided a tool that can be used to forecast the detection probability of a surveillance network. The detection probability is reduced to the geometric line intersection problem and the boundary conditions of intruder trajectories for the border area and the favourite region are determined. The line intersection problem is solved using tools from the integral geometry and geometric probability. The effect of the favourable region on the detection quality under different conditions is calculated using probabilistic models. The accuracy of the proposed quality metric is validated by both analytical methods and simulation results.

A Random Password Comparison [RPC] method was proposed by R. Amuthavalli et al [13] that facilitates deployment and control of the position of a node thereby preventing the Sybil attack. The RPC method is dynamic and accurate in detecting the Sybil attack. This method improves data transmission in the network and will also increase the throughput

V. Rathod et al [14]presented the general concept of Wireless Sensor Network and security in Wireless Sensor Network. Current research so far focuses on the security of wireless sensor network. There are various mechanisms of security applied in the network by which their network is more prone to failure. They also described so many attacks that occur in Sensor Networks and also apply to Sensor node.

W. Niu et al [15] proposed a novel Context aware Service Ranking approach for WSN services. First, a Context-aware WSN based service ranking framework is proposed with the incorporation of both user QoS assessment and context QoS assessment. Then, the variations in the slow convergence user assessment and the quick-variating services of QoS context factors were further investigated. A fuzzy aggregation method is put forward to generate a comprehensive assessment for ranking. Finally, they presented a case study as a demonstration of the approach's efficiency.

III. PROPOSED ALGORITHM

Methodology of Working

The proposed algorithm works in two different Phases such as Tier –I and Tier –II as shown in Fig.3 as follows

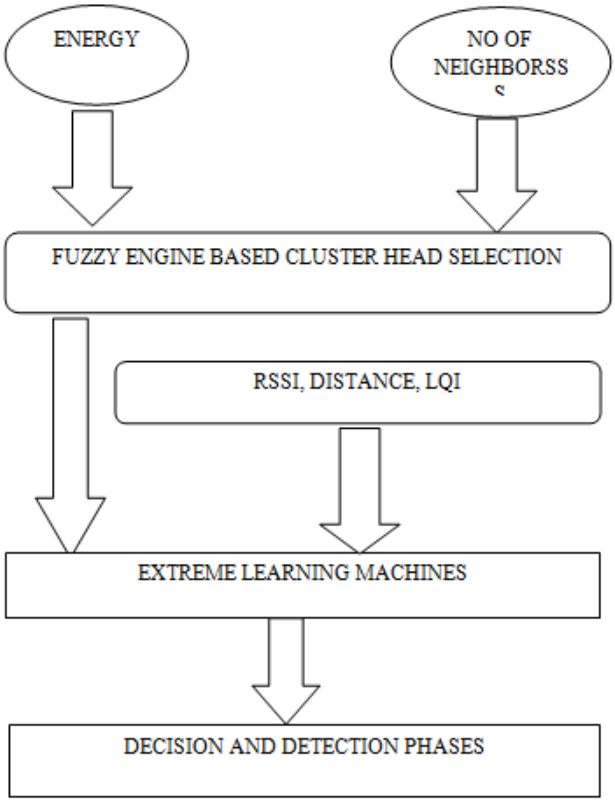

Fig. 3 Overall Architecture for the proposed FEM Systems

Tier -I Working Phase

In this Phase, two inputs are used for the selection of the Cluster Head in the network. Residual energy and No of neighbors are used as the Input parameters in which fuzzifiers were used for the detection of the Cluster head. Fuzzy rules for the selection of the cluster head is tabulated in Table-II

Table. 2 Illustration of Fuzzy Rule Sets for the Selection of the Cluster Head in FEM Phase-I working

Energy	No of Neighbors	Qualification level-CH
Low	Low	Selected_1
Low	Medium	Selected_2
Low	High	Selected_3
Medium	Low	Selected_4
Medium	Medium	Selected_5
Medium	High	Selected_6
High	Low	Selected_7
High	Medium	Selected_8
High	High	Selected_9

In order to evaluate the rules, the Mamdani Controller is used as a Fuzzy inference technique and the Centre of Gravity (COG) method is employed for defuzzification for the Cluster Head selection. After the selection of the secured Cluster head, RSSI, distance and LQI(Link Quality Indication)are calculated.

RSSI Measurement

Once the sensor nodes are deployed, the centralized sink broadcasts the hello messages at a certain power level to gather all the distance and RSSI information of the sensor nodes in the network. Each sensor node N_s can calculate the approximate distance from the sink, accordingto the received signal strength and can be measured directly from the expression giveninthe equation below.

$$D_{(N_s,BS)} = 10\left[\frac{(P_o - F_m - P_r - 10n\log(f) + 30n - 32.44)}{10n}\right]$$

Where P_o is the Power of the signal (dBm) in the zero distance, P_r is the Signal power (dBm) in the distance d, f is the signal Frequency in MHz, F_m is the Fade margin and n is the path-loss exponent. RSSI, distance, Secured Cluster head and LQI are considered as the inputs to the Extreme Learning Machine which is the second phase of the proposed algorithm.

Extreme Learning Machine Motivation

The Extreme Learning Machine uses the single hidden layer which leads to high training speed, good generalization or accuracy and universal function approximation capabilities. In ELM, the hidden layer mandatorily need not be tuned which is considered to be more advantage when compared with the other Neural network algorithms. The weights of the hidden layer are randomly assigned for training and testing. For a single-hidden layer ELM, the network output function is given in the following equation

$$f_L(\mathbf{x}) = \sum_{i=1}^{L} \beta_i h_i(\mathbf{x}) = \mathbf{h}(\mathbf{x})\boldsymbol{\beta}$$

where x ϵ R^d is an input vector of dimension d, $\beta = [\beta_1 \ldots \beta_L]^T$ is the vector of hidden to output weights, L the number of hidden layer neurons and $h(x)=[h_i(x),\cdots,h_Lx)]$ the vector of hidden layer outputs.

The L hidden layer outputs $h_i(x)$ are computed using a collection of nonlinear piecewise continuous functions in order to satisfy the requirements of universal approximation capability theorems given in the following equation

$$h_i(\mathbf{x}) = G(\mathbf{a}_i, b_i, \mathbf{x})$$

where G is the neuron function, $a_i \epsilon R^d$ are the hidden layer weights and $b_i \epsilon R^d$ the bias terms. A typical G function is the Sigmoid given in the below equation

$$G(\mathbf{a}_i, b_i, \mathbf{x}) = \frac{1}{1 + \exp(-(\mathbf{a}_i \cdot \mathbf{x} + b_i))}$$

In the proposed FEM architecture, ExtremeLearning Machine is used for the classification of the Sybil attack in which the following parameters listed in table III where used for our modeling

Table. 3 Illustration of Input features, learning parameters for proposed FEM Algorithm

Sl.No	Parameters used	Details
01	Input Parameters	1. RSSI
		2. Secured Cluster head
		3. Distance
		4. LQI
02	Output	Sybil attack (1)
03	Type of Extreme learning machines	Multi- Layer Perceptron
04	No of Hidden layer used	30
05	Activation Layer used	Sigmoidal

The Single hidden layer has been replaced with the Multi hidden layer for the better accuracy. The working of Multi-layered learning machine used in the proposed in FEM is shown in Fig 4

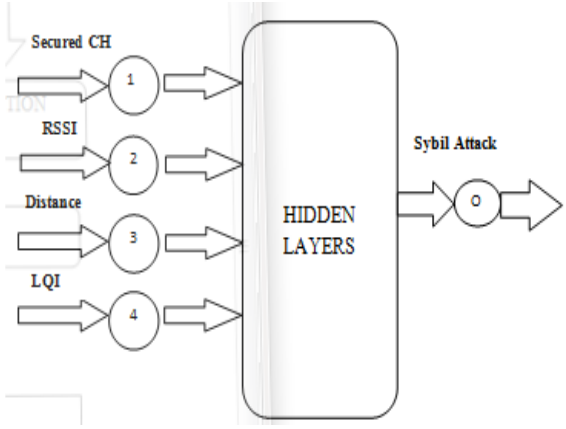

Fig. 4 Shows the Input, Bias weights and Output

Overall Working Mechanism of the Proposed Fem

Step 1: Collection of the Data Sets from the Experimental test beds

Step 2: Load the Data sets in the Central Sink Systems for training and Testing(70% Training and 30% testing)
Step 3: Set the threshold for the energy, RSSSI, no of neighbors ,distance
Step 4: Apply the Fuzzy rule sets for the selection of the Cluster head based on the Energy
Step 5: Train the network with the above inputs and set the different thresholds for the detection of Sybil attack
Step 6: Test the proposed FEM for the detection of Sybil attacks

IV. DATASET DECRIPTION

Experimental Setup

Table. 4 Hardware Details used for the Dataset Collection

Sl.No	Details of the hardware Used	Description
01	Main CPU	ARM/RISC based CPU
02	Transceivers	Zigbee Transceivers(CC2530)
03	Clock frequency used	12MHz
04	Sensors used	05
05	Features of Main CPU	Low Power CPU High performance
06	Mode of Interfacing	UART
07	No of Nodes used	10
08	Multiple Access Used	TDMA
09	Operating voltage	3.3V

The complete experimental setup used for the collection of dataset is shown in Fig 5

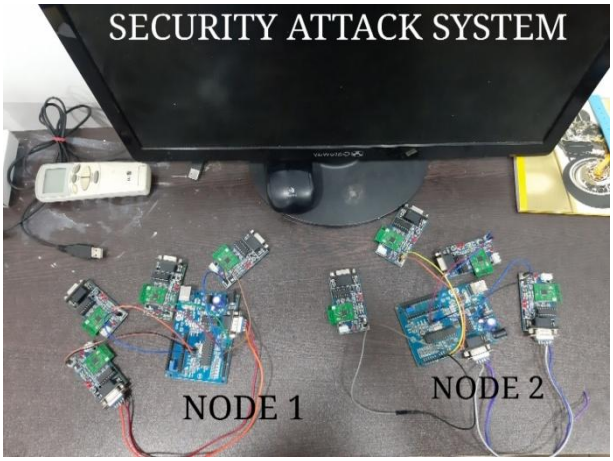

Fig. 5 Representation of the Experimental Setup Used for the Data Set Collection

V. DATASET DESCRIPTION

The peer-to -peer networking has been established between the Test beds and the sink which runs the MATLAB R2016a. The data sets were collected by running the Test beds for 24 Hours with 100 different Iterations which nearly constitutes 1540 data sets were used for training and testing the network are shown in Table V and VI.

Table. 5 Datasets used for Evaluating the proposed FEM Architecture(Trail-I)

Node.No	Cluster Head	Energy(mj)	RSSI(dbm)	Distance(m)	LQI	Detection of Attacks
01	01	5.0	-20	2	89	Normal
02	01	4.38	-20.8	2.1	88	Normal
03	01	4.58	-21.0	2.8	87	Normal
04	01	4.78	-22.0	3.2	86	Normal
05	01	4.88	-23.0	3.7	85	Normal
06	01	3.7	-23.5	3.2	84	Normal
07	01	3.6	-25.0	6.3	82	Normal
08	01	3.9	-20.7	2.6	83	Normal
09	01	3.7	-26.4	7.0	81	Normal
10	01	5.0	-26.6	7.1	81	Sybil Attack

Table. 6 Datasets used for Evaluating the proposed FEM Architecture(Trail-II)

Node No	Cluster Head	Energy(mJ)	RSSI(dbm)	Distance(m)	LQI	Detection of Attacks
01	01	5.0	-20	2	89	Normal
02	01	4.38	-20.8	2.1	88	Normal
03	01	4.58	-21.0	2.8	87	Normal
04	01	4.78	-22.0	3.2	86	Normal
05	01	4.88	-23.0	3.7	85	Normal
06	01	3.7	-23.5	3.2	84	Normal
07	01	3.6	-25.0	6.3	82	Normal

08	01	3.9	-20.7	2.6	83	Normal
09	01	5.0	-20	7.0	81	Sybil Attack
10	01	5.0	-26.6	7.1	81	Sybil Attack

Table V and Table VI represents the data collected from the experimental Test beds. In the Table V, Node 10 replicates itself with the same energy level and it is identified with the different RSSI, distance and LQI parameters. Table VI represents the node9 replicates by same energy, RSSI but with the different distance. In same way 100 trails were carried out to produce the datasets which are used for detection of the Sybil attack.

VI. RESULTS AND DISCUSSION

Performance Evaluation

To evaluate the performance of the proposed method, 70% of total datasets were given as training and 30% as testing in which the Accuracy, Sensitivity, Specificity and Computational Time Calculation are determined. The expression for the evaluation is as follows

$$\text{Accuracy} = \frac{\text{DR}}{\text{TNI}} \text{ x } 100$$

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP+TN}} \text{ x } 100$$

$$\text{Specificity} = \frac{\text{TN}}{\text{TP+TN}} \text{ x } 100$$

Where TP and TN Represents True Positive and True Negative values and DR& TNI represents Number of Detected Results and Total number of Iterations

Accuracy represents the Accuracy in detection of the Sybil attack and it has been compared with the other algorithms such as SVM, ELM and NB Classifiers.

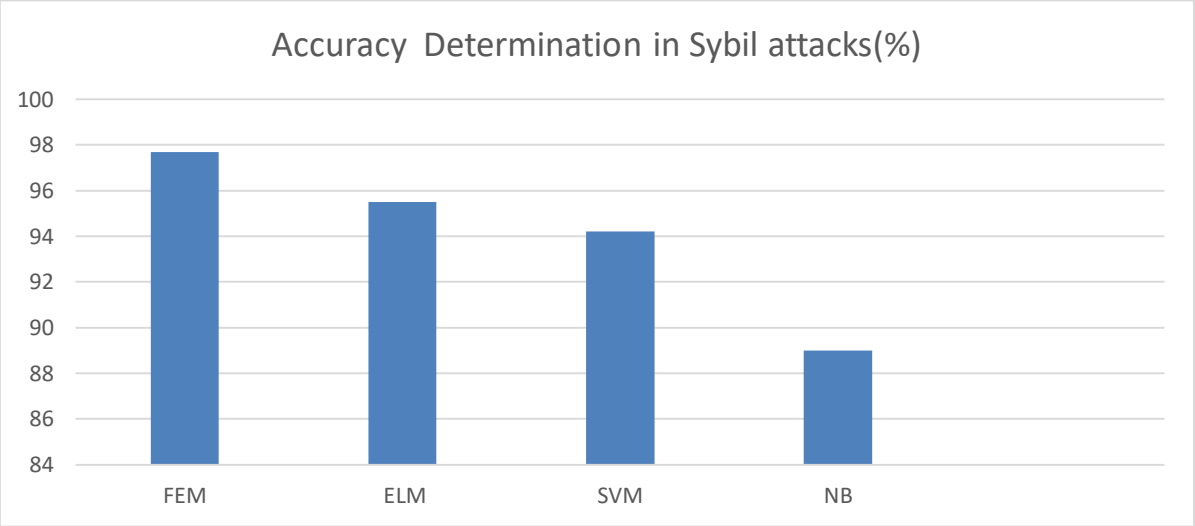

Fig. 6 Comparative Analysis of Accuracy detection for the different Classifier Algorithms

Fig 6 clearly shows the FEM 's accuracy detection of attacks is 99% where as other classifier algorithm such as ELM, SVM and NB has 98% ,96% and 92%respectively. Again the accuracy of proposed FEM algorithms has been subjected to10 iteration and compared with the other existing classifier algorithm.

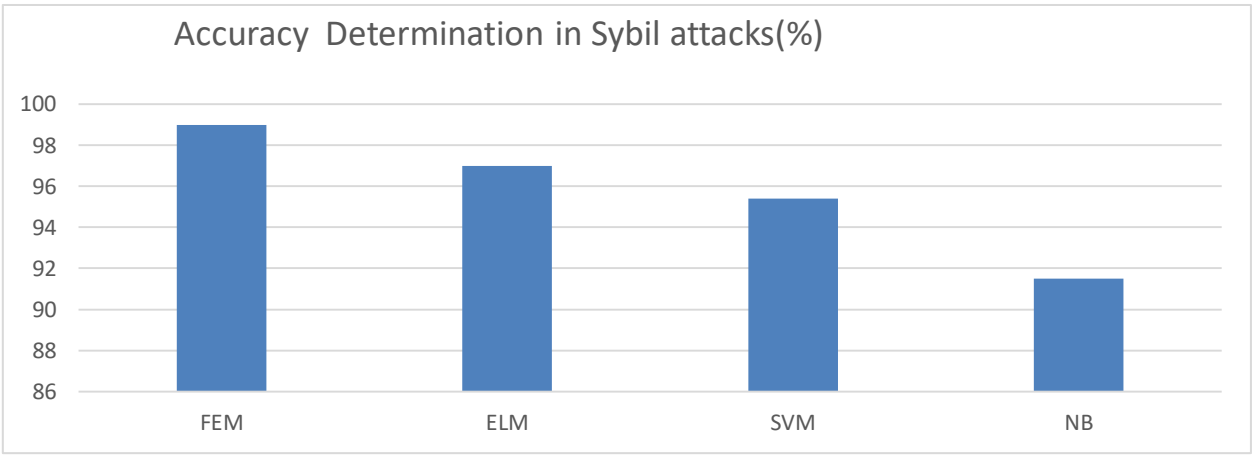

Fig. 7 Comparative Analysis of Accuracy detection for the different Classifier Algorithms(II iterations)

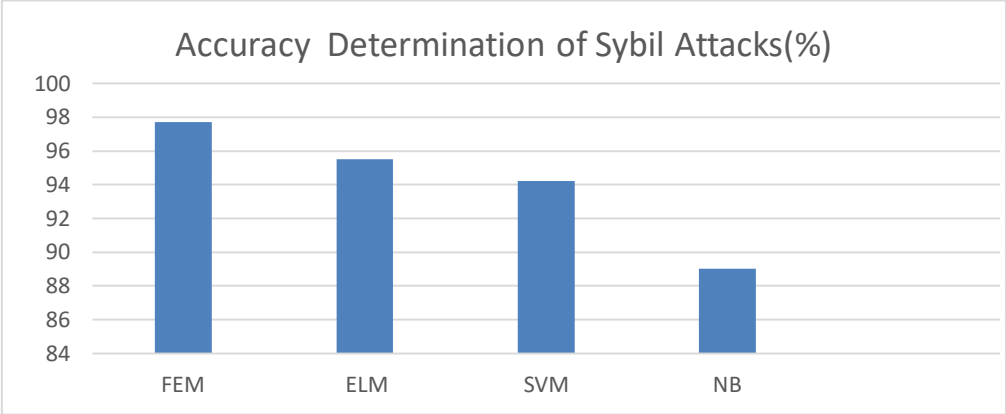

Fig. 8 Comparative Analysis of Accuracy detection for the different Classifier Algorithms(V iterations)

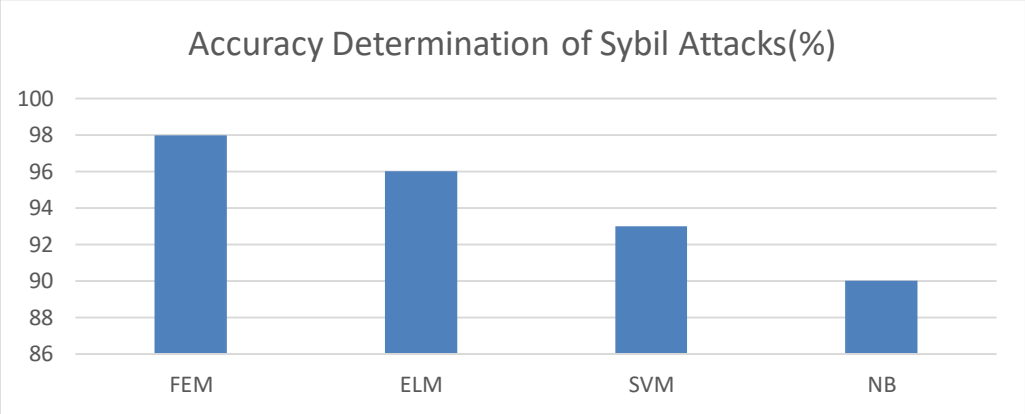

Fig. 9 Comparative Analysis of Accuracy detection for the different Classifier Algorithms(X iterations)

Fig. 6, Fig.7, Fig 8, and Fig 9 shows the comparative analysis of the proposed FEM algorithm with the different existing classifiers. Even at the Tenth Iteration, the accuracy of FEM remains as high as 96% whereas the accuracy of ELM is 94%, SVM is 92.5% and NB is 89%. After the 10 iteration and using Ten folded matrix, final accuracy of detection of each algorithms were calculated which are shown in Fig. 10

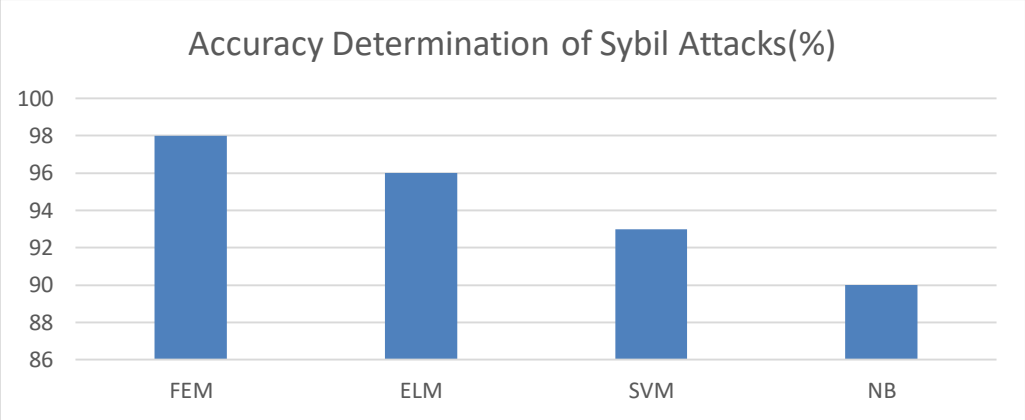

Fig. 10 shows the comparative analysis of the proposed algorithm with existing classifiers

Fig.10 shows the Final accuracy of detection for the proposed FEM algorithm and compared with existing algorithm. Accuracy of detection of Sybil attack in FEM is 96% when compared with the 94% of ELM, 92.5% in SVM and 89.5 % in NB classifiers.

VII. SENSITIVITY AND SPECIFICITY MEASUREMENTS

The Sensitivity and Specificity has been measured by using the confusion matrix of the tested data. The Sensitivity and specificity are measured for the proposed algorithm and compared with the existing algorithms which are shown in Fig.11

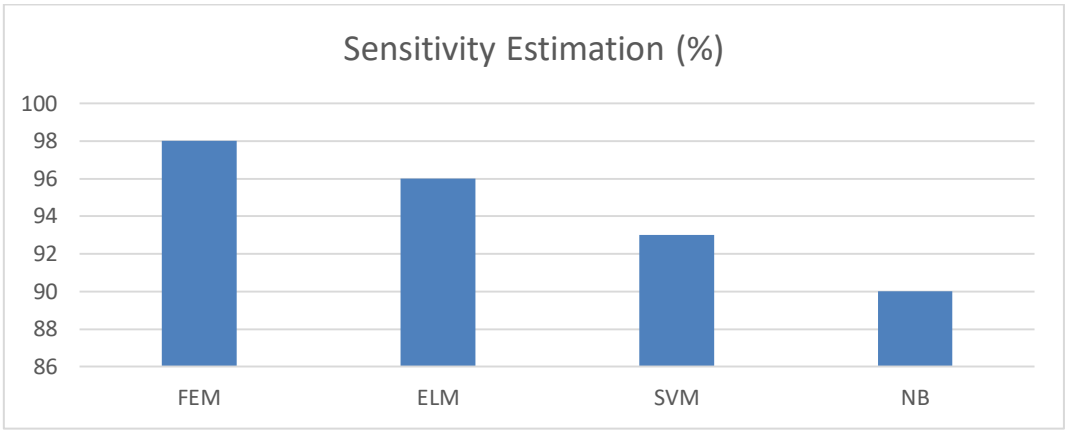

Fig. 11 Shows Sensitivity Estimation for the Proposed FEM algorithm compared with other Existing Clas1sifier algorithm

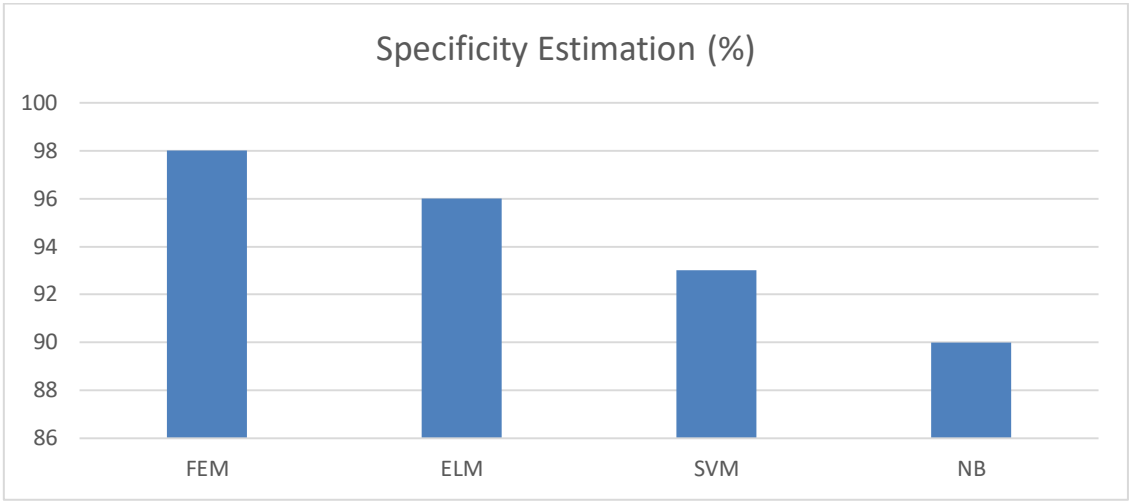

Fig. 12 Shows Specificity Estimation for the Proposed F1EM algorithm compared with other Existing Classifier algorithm

Fig.11 and Fig. 12 clearly shows the proposed FEM algorithm outperforms the other existing in terms of specificity and sensitivity estimation.

VIII. DETECTION TIME ANALYSIS

The Detection Time of Sybil attack has been calculated for the proposed FEM algorithm which are then compared with existing algorithm which are given in Fig. 13

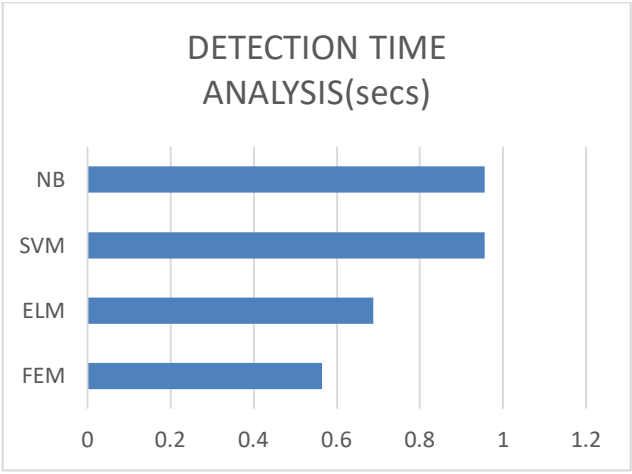

Fig. 13 Detection time Analysis for the Proposed FEM algorithm compared with existing classifier algorithm

Fig.13 shows the Detection Time analysis for the proposed FEM and compared with the other existing classifier. The Detection Time is low for the proposed FEM when compared with other existing algorithms. The proposed FEM algorithm proves to be more efficient when compared with existing classifier in detection of Sybil attacks. The accuracy of detection of Sybil attack is high as 97 % when compared with the other classifier algorithm. It also has less Detection Time in Sybil attack in which it increases the redundancy and network life time of the Wireless sensor network.

IX. CONCLUSION

The proposed algorithm FEM proves to be vital in terms of the detection of Sybil Attack when it is integrated in LEACH protocol of Wireless Sensor Networks. The experimental Test bed has also been designed successfully for dataset collection. Even though the proposed algorithm has higher efficiency when compared with the other existing classifiers, still the FEM can be further improvised by integrating the evolutionary algorithms to increase in accuracy of detection. Since WSN finds its applications in

Internet of Thins(IoT) for remote monitoring of the data, security breeches will be real threat in future networking. Integration of machine learning and deep learning algorithms will further increases the intelligence in the network which are used to overcome the security attacks.

REFERENCES

1. Udaya Suriya, Raj Kumar Dhamodharan and and Rajamani Vayanaperuma, " Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method", The Scientific World Journal, Volume 2015, pp.192-195, 2015.
2. Sunil Ghildiyal1, Ashish Gupta2, Nitesh Tomar3, AnupamSemwal, "Analysis of Sybil Attack in Wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 5,pp.845-848. May – 2014.
3. S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Signal strength based Sybil attack detection in wireless Ad Hoc networks," in Proceedings of the 2nd International Conference on Developments in eSystems Engineering (DESE '09), pp. 190–195, Abu Dhabi, UAE, December 2009.
4. S. Sharmila and G. Umamaheswari, "Detection of sybil attack in mobile wireless sensor networks," International Journal of Engineering Science & Advanced Technology, vol. 2, pp. 256–262, 2012.
5. K.-F. Ssu, W.-T.Wang, and W.-C. Chang, "Detecting sybil attacks in wireless sensor networks using neighboring information," Computer Networks, vol. 53, no. 18, pp. 3042–3056, 2009.
6. A.Vasudeva and M. Sood, "Sybil attack on lowest id clustering algorithm in te mobile ad hoc network," International Journal of Network Security & Its Applications, vol. 4, no. 5, pp. 135–147, 2012.
7. N. Balachandaran and S. Sanyal, "A review of techniques to mitigate sybil attacks," International Journal of Advanced Networking and Applications, vol. 4, pp. 1–6, 2012.
8. G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security, vol. 4, pp. 1–9, 2009.
9. L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 492–503, 2009.
10. H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: a near-optimal social network defense against sybil attacks," IEEE/ACM Transactions on Networking, vol. 18, no. 3, pp. 885–898, 2010.
11. G. Jing-Jing, W. Jin-Shuang, Z. Yu-Sen, and Z. Tao, "Formal threat analysis for ad-hoc routing protocol: modelling and checking the sybil attack," Intelligent Automation & Soft Computing, vol. 17, no. 8, pp. 1035–1047, 2011.
12. C. Komar, M. Y. Donmez, and C. Ersoy, "Detection quality of border surveillance wireless sensor networks in the existence of trespassers' favorite paths," Computer Communications, vol. 35, no. 10, pp. 1185–1199, 2012.
13. R. Amuthavalli and R. S. Bhuvaneswaran, "Detection and prevention of sybil attack in wireless sensor network employing random password comparison method," Journal of Theoretical and Applied Information Technologygy, vol. 67, pp. 236–246, 2013.
14. V. Rathod and M. Mehta, "Security in wireless sensor network: a survey," Ganpat University Journal of Engineering & Technology, vol. 1, pp. 35–44, 2011.
15. W. Niu, J. Lei, E. Tong et al., "Context-aware service ranking in wireless sensor networks," Journal of Network and Systems Management, vol. 22, no. 1, pp. 50–74, 2014.
16. S. Kaplantzis, A. Shilton, N. Mani, and Y. A. S¸ekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in 3rd IEEE International Conference on Intelligent Sensors, Sensor Networks and Information, 2007, pp. 335–340.
17. M. Sa and A. K. Rath, "A simple agent based model for detecting abnormal event patterns in distributed wireless sensor networks," in Proceedings of the ACM International Conference on Communication, Computing & Security, 2011, pp. 67–70.
18. E. U. Warriach and K. Tei, "Fault detection in wireless sensor networks: A machine learning approach," in 16th IEEE International Conference on Computational Science and Engineering (CSE), 2013, pp. 758–765.
19. G. Kaur and M. Singh, "Detection of black hole in wireless sensor network based on data mining," in Proc. 5th IEEE International Conference Confluence The Next Generation Information Technology Summit, 2014, pp. 457–461.
20. B. J. Culpepper and H. C. Tseng, "Sinkhole intrusion indicators in dsrmanets," in Proc. First IEEE International Conference on Broadband Networks, 2004, pp. 681–688.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication