Detection of Spoofed IP nodes using BAT Algorithm and Extreme Learning Machine

Sabitha Banu. A, Padmavathi Ganapathi

Abstract: IP spoofing is known as the most important cyber-attack which is the source for DoS or DDoS attacks where the attacker is hidden inside the network and makes the computer resource services unavailable to the users. The attacker once done with spoofing the IP address will start to flood the system with keeping on sending requests and make the network bandwidth slow to the extent. This paper contains the literature study of the different types of defence mechanisms from different authors used few decades before to detect and mitigate the Spoofed IP nodes at router, host level and recently some author come up with ideas of using computational intelligence methods for detecting the different types of attacks in wireless communications which results in accurate prediction. This paper provides creating a threat model of detecting the Spoofed IP nodes among 105 network wireless communication scenario using computational intelligence algorithm, the features are selected from the simulated raw data and preprocessed by using BAT optimization algorithm and features are converted to ELM readable format and then they are trained and learned using Extreme learning machine algorithm to predict the accurate detection of the Spoofed IP nodes in the wireless communication network scenario. The proposed method provides high accuracy in detection of Spoofed IP nodes with respect to some performance metrics like end to end delay, throughput, packet delivery ratio, packet drop ratio and it is compared with the KNN-SVM exiting model proved the results.

Keywords: IP Spoofing, Feature Selection, BAT algorithm, Extreme Learning Machine.

I. INTRODUCTION

In Today's world Internet has been acting like a pillar for distributed applications where the client and server need not be in the same location for communication with each other. There are large number cyber-attacks increasing on regular basis. The major threat in cyber-attack world is IP Spoofing. According to CAIDA study from March 1, 2015 -Feb. 28, 2017 there are 30,000 number of spoofing attacks have been detected on every day and approximately Twenty-one million attacks targets on around six million IP addresses.

IP address spoofing is where the attacker modify the source address to conceal the sender's identity to mimic the system .Internet Protocol address spoofing is obtained from the model which only depends on internet packet forwarding in routers to the packet destinations. Internet Protocol address spoofing utilizes the flaws in the protocol stack layer 3 and layer 4 to make the goal inaccessible.

IP address spoofing is launched when the victim negligence of the IP packets validation in source address to validate the authenticity of the sender. It is the vulnerable point of IP spoofing. By spoofing the IP addresses, attacker bombards

- DDoS attacks
- Smurf Attacks
- Network Time Protocol (NTP) synchronization reflection
- DRDoS(Ditributed Reflection DoS)
- DNS request reflection
- TCP-SYN Flooding attack

The three different kinds of scenarios where the IP spoofing can be launched on:

- Host
- Router
- Flow

Of all network scenarios the flow-based attack is considered as MITM ("Man in the Middle Attack") which means the attackers capturing the packet flow through the routing devices like wireless access points, through that they can able to alter or change or modify the IP address to do their purpose.

Configuration and Services prone to IP spoofing are

- Remote Process Calls
- IP address authentication services.
- The R suites like Remote login (rlogin),Remote shell(rshell)
- X windows system

The Objective of this paper is to discover accurate detection of IP spoofed nodes among various wireless nodes in a network scenario using BAT algorithm to optimize the features needed for ELM.

There are many methods available in the literature to handle IP Spoofing. Section 2 is about the review of literature about IP spoofing using different detection and prevention mechanism. Section 3 is about taxonomy of computational intelligence techniques and few literatures on applying CI techniques to detect and prevent IP Spoofing. Of all the suggested methods, Computational Intelligence methods are very effective in providing accurate results.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

Sabitha Banu.A*, department of computer science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India. Email: sabithabanucbe@gmail.com

Padmavathi Ganapathi, department of computer science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India. Email: ganapathi.padmavathi@gmail.com

Section 4 is about the proposed methodology. Section 5 discusses about the Experiments and analysis of the outcomes and Section 6 ends with Conclusion.

II. REVIEW OF LITERATURE

There are different defence mechanisms used to prevent the network from IP Spoofing both in wired and wireless networks. Different kind of mechanisms deployed in the past is specified in the following Table 1.

Table I: Literature Survey of IP Spoofing Mechanisms

Author	*Defence Mechanisms*	*Location*	
B.Liu, J. Bi ,and A.V. Vasilakos[3]P. Ferguson,[4]F. Baker and P. Savola,[5]	Ingress and Egress Filtering	Router Level	Filters the path by using Access Control List(ACL) and unicast reverse path forwarding(uRPF)
Yao et.al[6]	Virtual Anti Spoofing Edge(VASE)		Filtering on path, end to end authentication.
K. Park and H. Lee,[7] Z. Duan, X. Yuan, and J. Chandrashekar,[8]	Distributed Packet Filtering(DPF) Inter domain Packet Filter(IDPF)	Router level Router level	If the packets are transmitted in an unexpected route they are dropped. filtering rules inside the domain are framed using “valley free feature” and filtering rules of BGP announcement.
A. Bremler-Barr and H. Levy[9]	Spoofing Prevention Mechanism (SPM)	Router Level	Autonomous system tag is attached with the packet denoting key (Source, Destination). Destination key is checked and deleted after receiving.
X. Liu, A. Li, X. Yang, and D. Wetherall[10]	Packet Passport Method	Router Level	Follows symmetric cryptography, Verifying the tokens placed in every packets for the valid source address. Distribution of symmetric keys for verification is taken care by the routing system.
J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang[11]	Source Address Validation Enforcement(SAVE)	Router Level	Provides information to routers that helps for verifying the source address. Router builds a table which filters it using the prefix and information of the path.
H. Lee, M. Kwon, G. Hasker, and A. Perrig[12]	BGP Anti-spoofing Extension (BASE)	Router Level	Every packets from the BGP router is market by giving a key and filtering the incoming packets by using that key.
H. Wang, C. Jin, and K. G. Shin[13]	Hop Count Filtering	Host Level	Validates the source prefix binded with hop count value. Produces False negatives. By modifying the TTL value HCF can be bypassed.
A. Yaar, A. Perrig, and D. Song[14]	Stack Path Identifier(Pi)	Host and Router	Every router assigns packet marking and Packets traveling the same route will be marked the same way. Even valid packets gets chance to drop due to attackers travelling in the same path.
D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen,D. Moon, and S. Shenker[15]	Accountable Internet Protocol	Host and Router	Cryptography using hash values

All the existing IP spoofing defence mechanisms are applied either in host or router level and in few methods cryptographic puzzles are used. There are some more common preventing mechanisms like packet filtering ,monitoring networks for malicious activity, configuring router and firewalls, providing robust verification authentication of all IP addresses, using network attack blocker, using IPv6 protocol, network protocols based on cryptography such as “HTTPS(HTTP Secure) ,SSH(Secure Shell) and TLS(Transport layer Security)”.

III. COMPUTATIONAL INTELLIGENCE TECHNIQUES

General Structural outline of Computational Intelligence Techniques is shown in the Figure 1. CI methods are basically classified in to five types [16] namely Fuzzy Sets, Artificial Neural Networks, Evolutionary Computing, Swarm Intelligence Artificial Immune System has given in Fig 2.. And Some Review of Literatures has been given below on CI techniques to detect IP spoofing and DoS attacks.

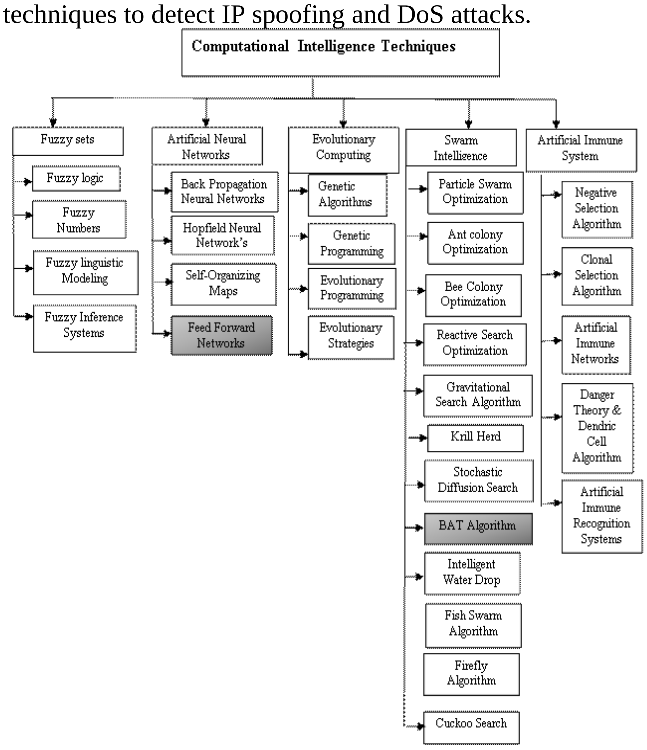

Computational Intelligence Techniques
Fuzzy sets
Fuzzy logic
Fuzzy Numbers
Fuzzy linguistic Modeling
Fuzzy Inference Systems
Artificial Neural Networks
Back Propagation Neural Networks
Hopfield Neural Network’s
Self-Organizing Maps
Feed Forward Networks
Evolutionary Computing
Genetic Algorithms
Genetic Programming
Evolutionary Programming
Evolutionary Strategies
Swarm Intelligence
Particle Swarm Optimization
Ant colony Optimization
Bee Colony Optimization
Reactive Search Optimization
Gravitational Search Algorithm
Krill Herd
Stochastic Diffusion Search
BAT Algorithm
Intelligent Water Drop
Fish Swarm Algorithm
Firefly Algorithm
Cuckoo Search
Artificial Immune System
Negative Selection Algorithm
Clonal Selection Algorithm
Artificial Immune Networks
Danger Theory & Dendric Cell Algorithm
Artificial Immune Recognition Systems

Fig. 1 Computational Intelligence Techniques Taxonomy

There are Few Literatures available for the detection of IP spoofed nodes applying computational Intelligence Techniques and it yields the high accurate results with minimal error rate show in the below Table 2.

Table II: Literature survey on CI Techniques to detect IP Spoofing

Author	*CI Techniques*	*Attacks and Accuracy rate*
A.Michalas, N.Komninos,N.R.Prasad [17]	Game theory and Nash equilibrium Game Theory with cryptographic puzzles	Developed co-operative IDS to upturn accurate results and detecting different new types of attacks. Encounter attacks like “DoS and DDoS” in MANET.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

M. A. Akbar and M. Farooq [18]	Evolutionary Algorithms like "Evolution radial basis function, Fuzzy Ada Boost, Genetic Classifier, Extended Classifier, Supervised Classifier, Continuous Ant Miner Classifier"	Detect SIP Flooding Attacks and effective in detecting, harmonic flood attack, chunk flood attack.
Herve Kabamba Mbikayi [19]	Evolutionary strategy and Game Theory	Detects anomalous connections
P. Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo [20]	FGA[Fuzzy Genetic Algorithm]	Detect unknown attacks Detection rate is above 95% and FPR <1%
A. Kannan, G.Q. Maguire [21]	Genetic Algorithm SVM and Fuzzy	Used for feature selection Detects DoS attacks at 98.3 % and error rate is 2.7%
Gupta, A., Pandey, O.J., Shukla, M., Dadhich, A., Ingle, A. and Ambhore, V [22]	Ant Colony Optimization	Detects UDP attacks. Detection Rate accuracy is 80%
Barani F., Barani A [23]	Artificial Bee Colony	Detect Flooding attack, Black hole and Wormhole attacks in MANET The rate of detection is 96.11% with False Positive Rate -1.45%
Ali, M.H., Al Mohammed, B.A.D., Ismail, A. and Zolkipli, M.F., [25]	Particle Swarm Optimization (PSO) and Fast Learning Network (FLN)	Detects DoS attacks at 98.11%
Q.Qian, J.Cai, R.Zhang [26]	Swarm Intelligence and Artificial Neural Network Artificial Bee Colony +BP ANN	Detects Malicious Activity ABC algorithm optimizes the features of BP neural networks during training process till reaches accuracy. Error rate is <.25% than traditional BP NN.
M. Barati, A. Abdullah, N I Udzir, R. Mahmod & N. Mustapha [27]	Artificial Neural network and Genetic Algorithm	Detection rate of 99.9%and FPR-0.002%
L.Jin, Y.Liu, L.Gu [28]	LVQ+ANN	Achieve a detection rate of 99.723% and FPR-0.277%
Javidi, M.M, Nattaj [29]	ANN+MPL	Detects DoS attacks at 96.6% and FPR-3.4%
M. Shojaei , N. Movahhedinia and B. T. Ladani [30]	ANN	Ddos attacks occurs in WIMAX networks TPR-85% and FPR-1.5%
Wang, D., He, L., Xue, Y. and Dong, Y [31]	Neighborhood Negative Selection(LRFC)	Detects flooding attacks efficiently. TN <8.5% and FN>=15%
Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam [32]	CSA	IDS for smart grid infrastructure.FPR-.7% and FNR-21.02%
Al-Dabagh, N.B.I; Ali, IA [33]	DCA	Perfect Detection rate and FPR - 0.17%
Hooks, D., Yuan, X., Roy, K., Esterline, A. and Hernandez, J [34]	AIS Generation Algorithm negative selection algorithm and clonal s election algorithm	Detection Rate are 86.86% (39 Features) Detection Rate is 77.23% (22 Features)
Tabatabaefar, M., Miriestahbanati, M. and Grgoire, J.C [35]	PSO+AIS ANN	Detect cyber-attacks at the detection rate of 99.1% and FPR-1.9% ANN classification methods for attack detection, identification, blacklisting, node reconfiguration. Detection rate-88.23%

From the above past literatures it is observed that rather than Machine Learning Techniques, applying Computational intelligence methods brings the accurate results for the all kinds of complex problems. The Proposed Method Hybrid combination of Extreme Machine Learning of Feed Forward Networks from ANN and BAT Algorithm of Swarm Intelligence can bring the accurate results in detection of the IP spoofed nodes in a wireless network and the results are compared relating to some performance Metrics like "packet drop ratio, packet delivery ratio, throughput ratio, end-to-end delay".

IV. PROPOSED IP SPOOFED NODES DETECTION APPROACH

There are various techniques and tools to detect the IP spoofed nodes in the wireless network. But our proposed hybrid detection of IP spoofed nodes is very simple and efficient with Fast Learning rate ,provides accurate results with minimal error and the most important it is very easy to implement. Let see the approach in detail.

A. Bat optimization approach

Detection of IP spoofed nodes are done by using one of the Nature inspired algorithms called BAT algorithm based on SI techniques. The bat algorithms works on finding the location of the prey and bats by raising some echo signals.BAT algorithm is very efficient and is applied for optimization, classification, and feature selection.

BAT Algorithm works on the basis of echolocation which shows the bats behaviour to discover way out for single and multi-objective optimization problem.BAT Algorithms is used in order to distinguish unusual traffic from ordinary traffic in the proposed strategy.

B. Behavior of bats

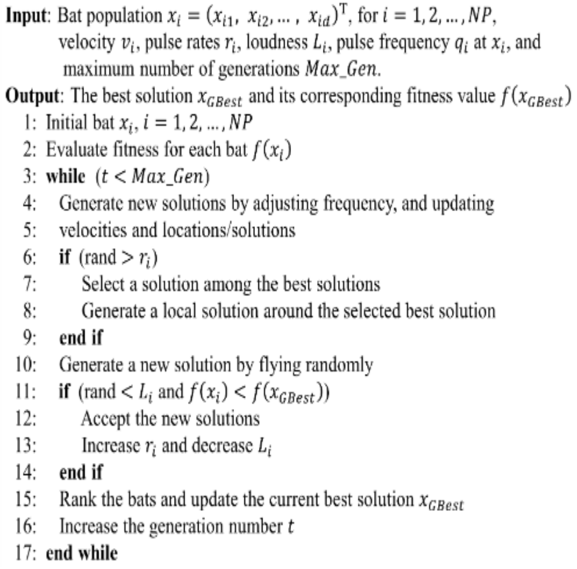
Even in full darkness bats discovers its food and can differentiate among different kinds of insects. The BAT algorithm is an evolutionary algorithm based on population where each bat is a solution. It describes the behaviour of the bats according to the location of the echo emitted. This echolocation behaviour of bats empowers them to identify where the prey is located by emitting some frequency sound pulses and it carefully listens sound pulses which returns back from the place where the food/prey is located or the neighbouring phenomenon's. During the time when a bat move towards close to the prey, the echo emittance is decreased and frequency sound pulse rate is increased. The 3 general rules of BAT algorithms:

(1) Entire Bats use echo based on location to feel distance, and in addition they predict the variation between prey and other unnecessary barriers in a few magical approach.

(2) Bats arbitrarily fly with Speed S_i at position P_i with specific Frequency F_{min}, fluctuating Wavelength $^{\delta}$ and echo vibration B_0 to hunt its food. Bats naturally fine-tune the frequency of the radiated pulses & fine-tune the pulse rate emitted signals R which depends on closeness of the object.

(3) In spite of vibration of the echo can be differed in various ways, it is pretended that the vibration of the echo differs against maximum (+ve) B_0 to a least constant rate B_{min}.

Initialize the population of bats. Modify the required parameters after initialization that are required for Fitness and finally the Fitness remains estimated for every individual Bat in the Population. Bat algorithm used for classification of IP Spoofing attacks from normal traffic is given below.



```
Input: Bat population $x_i = (x_{i1}, x_{i2}, \dots, x_{id})^T$, for $i = 1, 2, \dots, NP$,
       velocity $v_i$, pulse rates $r_i$, loudness $L_i$, pulse frequency $q_i$ at $x_i$, and
       maximum number of generations $Max\_Gen$.
Output: The best solution $x_{GBest}$ and its corresponding fitness value $f(x_{GBest})$
Initial bat $x_i$, $i = 1, 2, \dots, NP$
Evaluate fitness for each bat $f(x_i)$
while $(t < Max\_Gen)$
    Generate new solutions by adjusting frequency, and updating
    velocities and locations/solutions
    if (rand $> r_i$)
        Select a solution among the best solutions
        Generate a local solution around the selected best solution
    end if
    Generate a new solution by flying randomly
    if (rand $< L_i$ and $f(x_i) < f(x_{GBest})$)
        Accept the new solutions
        Increase $r_i$ and decrease $L_i$
    end if
    Rank the bats and update the current best solution $x_{GBest}$
    Increase the generation number $t$
end while
```

BAT optimization algorithm selects optimum features from the raw data by feeding the behaviour or pattern of DDoS attacks for detection purpose and those features are used for training and testing.

The advantages of using the BAT algorithm is it is very efficient, frequency is tuned randomly, automatic zooming on the nodes where promising solutions are found. Parameter tuning is done automatically which increases the performance of the system, solves complex network problems efficiently, accurate results in quick time, algorithms converges easily at the starting stage.

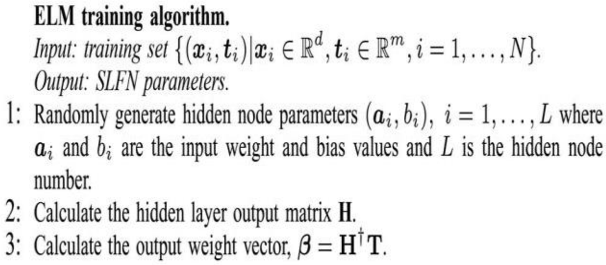
C. ELM approach

Extreme Machine Learning (ELM) can be used for selection of features at the first and the single layer of hidden nodes with parameters of the hidden nodes don't need to be tuned. Input weights are randomly assigned for the hidden nodes and output weights are learned in a single step. ELM has a high speed of learning rate compared with the other gradient neural networks. It produces good performance and learns thousand times faster than others neural networks. ELM works according the following steps:

- Data Pre-processing: Converting the raw TCP/IP data in to ELM readable format.
- Training Phase: ELM is trained with the feature selection data's.
- Testing Phase: Trained data is compared with tested data to find out the accuracy detection.

ELM shows a good performance when it is deployed in the proposed work which contains huge volume of network traffic data. Combination of BAT and ELM has produces high accuracy and minimal error.BAT algorithm optimizes the parameters so that the detection is accurate.

Pseudo Code for ELM



```
ELM training algorithm.
Input: training set $\{(\boldsymbol{x}_i, \boldsymbol{t}_i) | \boldsymbol{x}_i \in \mathbb{R}^d, \boldsymbol{t}_i \in \mathbb{R}^m, i = 1, \dots, N\}$.
Output: SLFN parameters.
Randomly generate hidden node parameters $(\boldsymbol{a}_i, b_i)$, $i = 1, \dots, L$ where
    $\boldsymbol{a}_i$ and $b_i$ are the input weight and bias values and $L$ is the hidden node
    number.
Calculate the hidden layer output matrix $\mathbf{H}$.
Calculate the output weight vector, $\beta = \mathbf{H}^{\dagger}\mathbf{T}$.
```

D. Proposed methodology

The wireless network is created and the network traffic generated between mobile nodes are simulated in ns2.TCP, UDP connection setup is done among all wireless nodes. Packets are exchanged between the nodes when the wireless nodes are in the range of the gateway and also when the nodes move away from the hearing range of the gateway the packets are dropped.

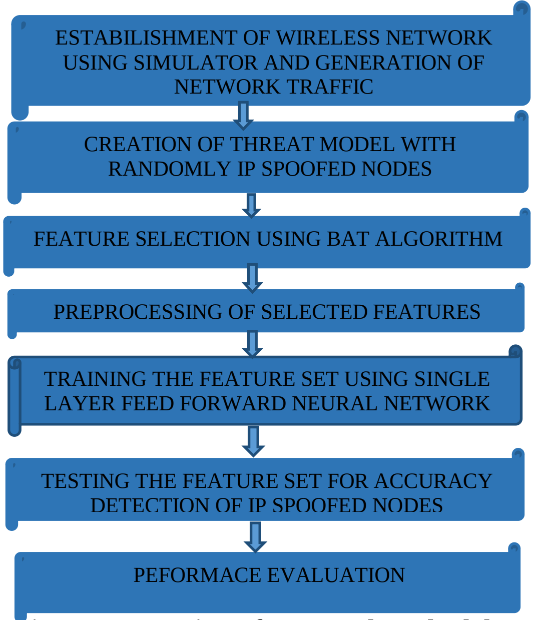

ESTABILISHMENT OF WIRELESS NETWORK USING SIMULATOR AND GENERATION OF NETWORK TRAFFIC
CREATION OF THREAT MODEL WITH RANDOMLY IP SPOOFED NODES
FEATURE SELECTION USING BAT ALGORITHM
PREPROCESSING OF SELECTED FEATURES
TRAINING THE FEATURE SET USING SINGLE LAYER FEED FORWARD NEURAL NETWORK
TESTING THE FEATURE SET FOR ACCURACY DETECTION OF IP SPOOFED NODES
PEFORMACE EVALUATION

Figure 2. Overview of Proposed Methodology

V. EXPERIMENTAL ANALYSIS AND RESULTS

A. Experimental Setup

An Experimental Setup of proposed works was made up by creating a wireless network with 105 mobile nodes and 4 gateways in NS2. NS2 is an open source simulator to design communication networks for research purpose.It is the best tool for implementing wired and wireless networks like VANET, MANET with different routing protocols like TCP ,UDP, FTP, DSR, HTTPs, TELNET,CBR,VBR. All mobile nodes should be configured before using them. They are given in Table 3.

Network components of mobile node Parameters are

- Type of Antenna
- Channel Type
- Link Layer(LL)
- MAC Layer

- Ad-hoc routing protocol
- Interface Queue(ifQ)
- Radio propagation Model

Additionally,

Table III. Simulation Parameters

option	available values	Default
Prop Type	Propagation/Shadowing ,Propagation/Two RayGround	""
Wired Routing	ON, OFF	OFF
txPower	<value in W>	""
topoInstance	<topology file>	""
rxPower	<value in W>	""
routerTrace	ON, OFF	OFF
propInstance	Propagation/Two RayGround, Propagation/Shadowing	""
phyType	Phy/wirelessPhy, Phy/Sat	""
MPLS (Multi protocol Label Switching)	ON, OFF	OFF
mobileIP	ON, OFF	OFF
macType	802.11,CSMA,CA,SAT,TDMA,unslotted aloha	""
macTrace	ON, OFF	OFF
ifqType	Queue, DropTail, PriQueue	""
initialEnergy	<value in Joules>	""
Adhocrouting	OMNIMCAST , FLOODING, TORA, AODV M-DART, DSR, PUMA	
Idle Power	<value in W>	""
energyModel	EnergyModel	""
channel	Channel/Wireless Channel, Channel/Sat	""
antType	Antenna/OmniAntenna	""
agentTrace	ON, OFF	OFF
llType	LL	""
addressType	flat, hierarchical	Flat

By setting up all the simulation parameters a wireless network is created and IP spoofing attacks are detected and the simulated network traffic is collected and the data is loaded in MATLAB for accuracy detection. MATLAB is a powerful tool for data analysis, optimization and visualization.

B. Results

A wireless network with 105 mobile nodes and 4 gateways are created and network traffic is generated.

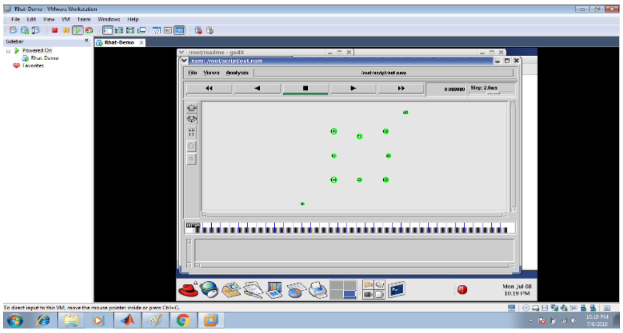
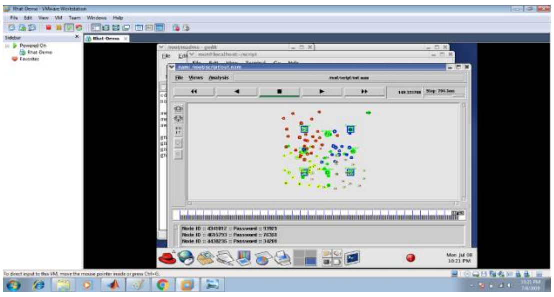
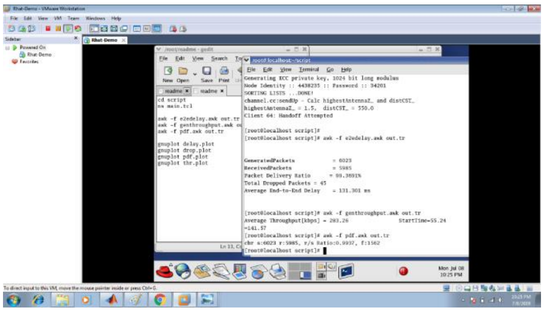


Fig 2.1 Capturing Generated Network Trafficking nodes



```
Node ID :: 4341812 :: Password :: 33921
Node ID :: 4615793 :: Password :: 76361
Node ID :: 4438235 :: Password :: 34201
```

Fig 2.2 Analysing the Grasped nodes



```
Generating ECC private key, 1024 bit long modulus
Node Identity :: 4438235 :: Password :: 34201
SORTING LISTS ...DONE!
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
Client 64: Handoff Attempted

[root@localhost script]#
[root@localhost script]# awk -f e2edelay.awk out.tr


GeneratedPackets            = 6023
ReceivedPackets             = 5985
Packet Delivery Ratio      = 99.3691%
Total Dropped Packets = 45
Average End-to-End Delay    = 131.301 ms


[root@localhost script]# awk -f genthroughput.awk out.tr
Average Throughput[kbps] = 283.26               StartTime=55.24
=141.57
[root@localhost script]# awk -f pdf.awk out.tr
cbr s:6023 r:5985, r/s Ratio:0.9937, f:1562
[root@localhost script]# ▌
```

Fig 2.3 Identifying overall Dropped and Received Packets

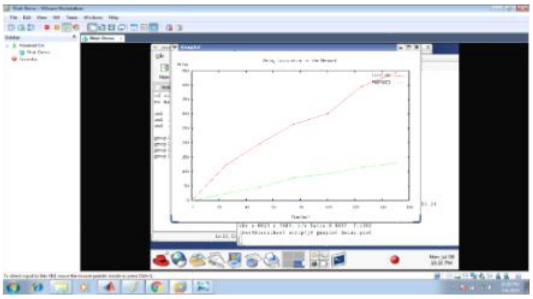
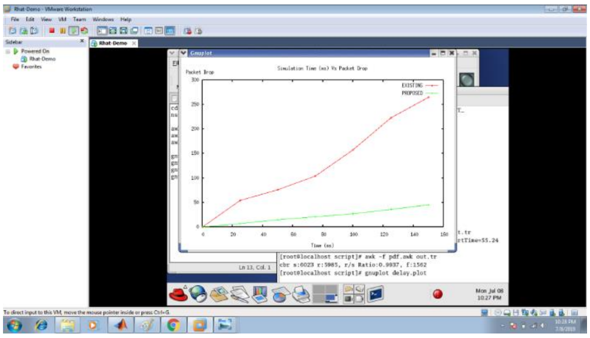
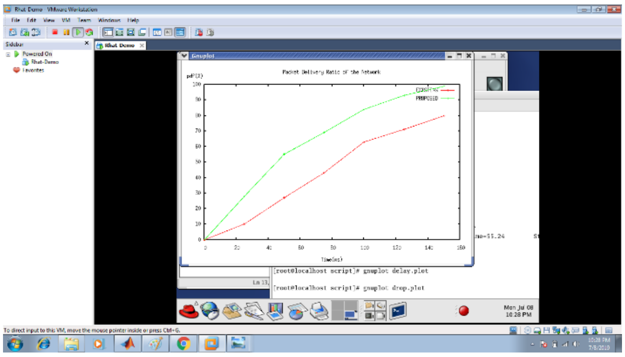


Fig 2.4 Calculating Delay Ratio of the network



```
[root@localhost script]# awk -f pdf.awk out.tr
cbr s:6023 r:5985, r/s Ratio:0.9937, f:1562
[root@localhost script]# gnuplot delay.plot
```

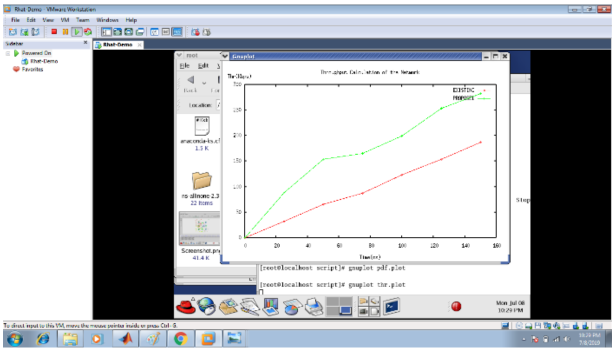
Fig 2.5 Investigating packets drop time



```
[root@localhost script]# gnuplot delay.plot

[root@localhost script]# gnuplot drop.plot
```

Fig 2.6 Consigned network packets delivery ratio in the network



```
[root@localhost script]# gnuplot pdf.plot

[root@localhost script]# gnuplot thr.plot
```

Fig 2.7 Throughput calculation of the network nodes

VI. PERFORMANCE COMPARISON

Comparing the proposed method and the existing Methods performance evaluated which is shown in Figure 2.8 and are outlined in the below sections using different metrics.

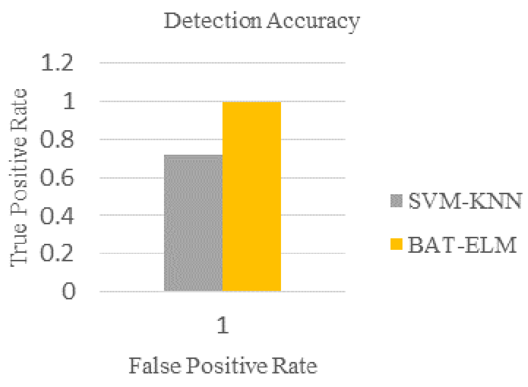


Fig 2.8 Detection Accuracy

A. End-to-End Delay Ratio

Travelled time throughout the network. The time when the packet is generated by the sender till it reaches the destination's application layer. The formula for calculating End to End Delay ratio is given below

Average End Delay=TD/TR

Where TD=Total no of Packets

TR= Packets Received.

PDR is shown in the Figure 2.9

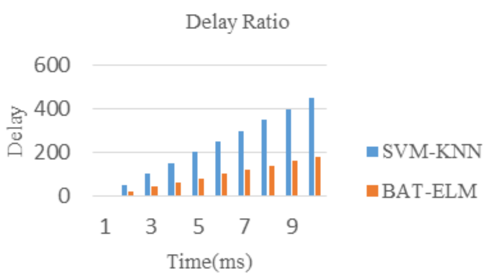


Fig 2.9 Delay ratio

B. Packet Delivery Ratio (PDR)

PDR is measured by transmitted packets by a CBR traffic source and the received packets by a CBR traffic sink. The formula used to calculate PDR is given below

PDR= (PR/PS) x 100%

PR stands for Packets Received and PS stands for Packets Sent.

PDR is shown in the Figure 2.10

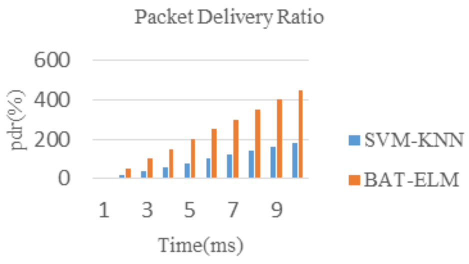


Fig 2.10 Packet Delivery Ratio

C. *Packet Drop Ratio*

The Difference between Packets Sent and Packets Received. The formula used to calculate Packet Drop Ratio is given below

PDR=Sent Packets-Received Packets

PDR is shown in the Figure 2.11

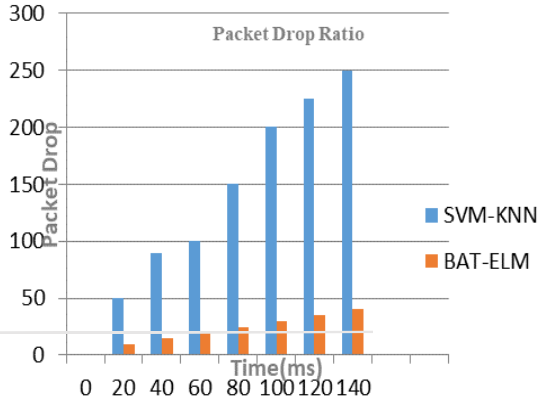


Fig 2.11 Packet Drop Ratio

D. Throughput Calculation

The time taken to send data from sender to receiver. Throughput denotes the effectiveness of the routing protocol. The formula used to calculate throughput is given below

$$TP=PR * PZ/SE$$

Where PR is Received Packets
PZ is Packet Size
SE is Simulation End Time
Throughput can be shown in the Figure 2.12

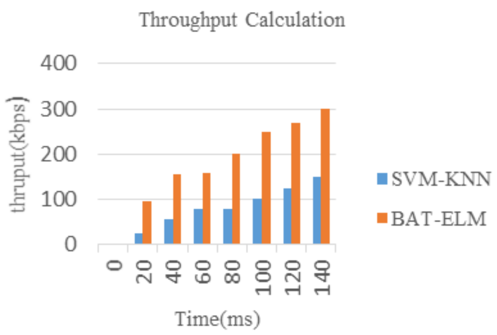


Fig 2.12 Throughput ratio

VII. CONCLUSIONS

In this paper a hybrid combination of BAT based ELM approach is used to detect IP spoofed nodes in a wireless network and the simulated traffic dataset is generated .Few features like latency, simulation time, No of TCP packets sent and received ,total no of bytes of a packets and packet loss is selected to train our ELM model. ELM approach randomly places the inputs and learns it in a "single layer feed forward neural network" and provides 100% detection accuracy results compared with SVM and KNN respectively under optimized parameter tuning. Our Proposed BAT Based ELM approach have got increased performance metrics in the form of Packet Delivery ratio, Delay, throughput and Packet Drop.

REFERENCES

1. Muhammad Aamir , Syed Mustafa Ali Zaidi," Clustering based semi-supervised machine learning for DDoS Attack Classification",Elseivier,2019,pp.1-11.
2. Chi cheng, Wee Peng Tayand ,Guang-bing huang,"Extreme Machine Learning for Intrusion Detection" , in WCCI 2012 IEEE world congress on Computational Intelligence,2012.
3. B. Liu, J. Bi, and A. V. Vasilakos, "Toward incentivizing anti-spoofing deployment", IEEE Trans. Inf. Forensics Secur., Vol. 9, No. 3, Mar. 2014, pp. 436–450.
4. P. Ferguson, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing," RFC2827, 2000.
5. F. Baker and P. Savola, "Ingress filtering for multi homed networks", BCP 84, RFC 3704, Tech. Rep., Mar. 2004.
6. G. Yao, J. Bi, and P. Xiao, "Vase: Filtering IP spoofing traffic with agility",Comput. Netw., Vol. 57, No. 1,2013, pp. 243–257.
7. K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets," ACMSIGCOMM Comput. Commun. Rev., Vol. 31, No. 4, 2001, pp. 15–26.
8. Z. Duan, X. Yuan, and J. Chandrashekar , "Constructing inter-domain packet filters to control IP spoofing based on BGP updates," in Proc.INFOCOM, 2006, pp. 1–12.
9. A. Bremler-Barr and H. Levy, "Spoofing prevention method", in Proc.24th Annu. Joint Conf. IEEE Comput. Commun. Soc., 2005, Vol. 1, pp. 536–547.
10. X. Liu, A. Li, X. Yang, and D. Wetherall , "Passport: Secure and adoptable source authentication", in Proc. Netw. Syst. Des. Implement.(NSDI), Vol. 8,2008, pp. 365–378.
11. J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "SAVE: Source address validity enforcement protocol," in Proc. 21st Annu. Joint Conf .IEEE Comput. Commun. Soc., Vol. 3, 2002, pp. 1557–1566.
12. H. Lee, M. Kwon, G. Hasker, and A. Perrig, "BASE: An incrementally deployable mechanism for viable IP spoofing prevention", in Proc. 2nd ACM Symp. Inf. Comput. Commun. Secur. , 2007, pp. 20–31.
13. H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering" , IEEE/ACM Trans. Netw., Vol. 15, No. 1, Feb. 2007,pp. 40–53.
14. A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DDoS attacks", in Proc. Symp. Secur. Privacy, 2003, pp. 93–107.
15. D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen,D. Moon, and S. Shenker , "Accountable Internet protocol (AIP)" , ACM SIGCOMM Comput. Commun. Rev., Vol. 38, No. 4, 2008, pp. 339–350.
16. FatihÇelik , Ahmet Zengin and Sinan Tuncel, "A survey on swarm intelligence based routing protocols in wireless sensor networks", International Journal of the Physical Sciences Vol. 5.No.14, 2010, pp. 2118-2126.
17. A.Michalas, N.Komninos , N.R.Prasad , "Multiplayer Game for (D)DoS Attacks Resilience in Ad Hoc Networks", in 2nd International Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2011,pp.1-5.
18. M. A. Akbar and M. Farooq," Application of evolutionary algorithms in detection of SIP based flooding attacks", In Proc of the 11th Annual conference on Genetic and evolutionary computation, GECCO 09, 2009,pp 1419-1426.
19. Herve Kabamba Mbikayi , "An Evolution Strategy Approach toward Rule set Generation for Network Intrusion Detection Systems (IDS)", International Journal of Soft Computing and Engineering (IJSCE), Vol. 2 Issue-5, 2012,pp. 201-205.
20. P. Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo," Network intrusion detection with fuzzy genetic algorithm for unknown attacks", in Information Networking (ICOIN), 2013, pp. 15.
21. A. Kannan, G.Q. Maguire ,"Selection Algorithm for Effective Networks", in IEEE 12th International Workshops, 2012 , pp. 416-423.
22. Gupta, A., Pandey, O.J., Shukla, M., Dadhich, A., Ingle, A. and Ambhore, V," Intelligent Perpetual Echo Attack Detection on User Datagram Protocol Port 7 Using Ant Colony Optimization", In Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, 2014, pp. 419-424.
23. Barani F., Barani A.,"Dynamic Intrusion Detection in AODV-based MANETs Using Memetic Artificial Bee Colony algorithm", IEEE Conferences: 2014 22nd Iranian Conference on Electrical Engineering (ICEE), 2014, pp. 1040-1046.
24. Q.Qian, J.Cai, R.Zhang," Intrusion Detection based on Neural Networks and Artificial Bee Colony in IEEE/ACIS 13th International Conference on Computer and Information Science,2014, pp.257-262.
25. Ali, M.H., Al Mohammed, B.A.D., Ismail, A. and Zolkipli, M.F.,"A new intrusion detection system based on Fast Learning Network and Particle swarm optimization", IEEE Access, 6, 2018, pp.20255-20261.
26. M. Barati, A. Abdullah, N I Udzir, R. Mahmod & N. Mustapha," Distributed Denial of Service Detection using hybrid machine learning techniques", International Symposium on Biometrics and Security Technologies, IEEE, 2014, pp. 268-273
27. L.Jin, Y.Liu, L.Gu ," (D)DoS attack detection based on neural network" , in International Symposium on Aware Computing, 2014, pp. 196-199.
28. Javidi, M.M, Nattaj, M.H,"A new and quick method to detect DoS attacks by Neural Networks", Journal of Mathematics and Computer Science, Volume 6, 2013, pp.85-96.
29. M. Shojaei , N. Movahhedinia and B. T. Ladani, "(D)DoS attack Detection in IEEE 802.16 based networks" , Wireless Networks, Vol.20,No.8,2014, pp. 2543-2559.
30. Wang, D., He, L., Xue, Y. and Dong, Y. ,"Exploiting Artificial Immune systems to detect unknown DoS attacks in real-time", In Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on Vol. 2, 2012, pp. 646-650.
31. Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids", IEEE Trans. Smart Grid, Vol. 2, No. 99, 2011,pp. 796-808.
32. Al-Dabagh, N.B.I; Ali, IA,"Design and implementation of artificial immune system for detecting flooding attacks," High Performance Computing and Simulation (HPCS), 2011 International Conference on, 2011, pp.381-390.
33. Hooks, D., Yuan, X., Roy, K., Esterline, A. and Hernandez, J., "Applying Artificial Immune System for Intrusion Detection." In 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService), 2018, pp. 287-292.

34. Tabatabaefar, M., Miriestahbanati, M. and Grgoire, J.C., "Network intrusion detection through artificial immune system". In Systems Conference (SysCon), 2017 Annual IEEE International, IEEE, 2017, pp. 1-6.
35. X. S. Yang, "A new metaheuristic Bat-inspired algorithm," in Nature Inspired Cooperative Strategies for Optimization (NICSO '10), , Springer, vol. 284,2010 pp. 65–74..
36. Mattijs Jonker ,Alistair King,Johannes Krupp,Anna Sperotto,Alberto Dainotti, Christian Rossow ," Millions of Targets Under Attack: a Macroscopic Characterization of the DoS Ecosystem" ,ACM.

AUTHORS PROFILE

Sabitha Banu. A., received her MCA in 2007 from Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She is currently pursuing her Ph.D. at Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. Her areas of interest are Network Security, Machine to Machine Communications, Cryptography and Wireless Communications.

G. Padmavathi, is the Professor in the Department of Computer Science at Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She has 29 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Wireless Communication, Network Security and Cryptography. She has significant number of publications in peer reviewed International and National Journals. Life member of CSI, ISTE, WSEAS, AACE and ACRS