Improving Anomaly Detection Process in Computer Networks Having Existing IDS Using Additional Behavioral Layer, Optimized Back Propagation Neural Network and Mobile Agents (With Multi Class Attack Detection)

Ph.D. Synopsis

Submitted To
Gujarat Technological University

For The Degree
Of
Doctor Of Philosophy
In
Computer Science

By
Bhavin Shah
Enrollment No: 119997493013
(Computer Science)

Supervisor :
Dr. Bhushan H. Trivedi,
Director,
GLS Institute of Computer Technology,
Gujarat Technological University,
India.

Co-Supervisor :
Dr. Jeanna Matthews,
Associate Professor,
Mathematics & Computer Science Department,
Clarkson University,
USA.

Index

1 Abstract

As per current annual report published in 2015, market leading companies in the network security area like Cisco, Symantec and Sophos, clearly state that attackers are using more advanced and sophisticated tools. Accordingly, though there is a decrease in the number of zero day attacks, their impact has been increased. One of such unknown attack or zero day attack is a multi class attack in which attacker attacks by combining the characteristics of two or more attacks. To detect multi class attacks along with single class attacks, we proposed a multi layered model in which existing IDS detects known attacks and additional IDS detects multi class attacks. Based on the literature survey and experiments being conducted on such multi layered IDS, hike in the response time has become a major challenge. The hike in response time increases the packet dropping rate, in turn raising the false alarm rate of multi layered IDS.

To reduce the response time, the proposed model uses Optimized Back Propagation Neural Network (OBPNN) as a high speed detection engine, reduced and normalized data and client-server architecture which uses light weight Jade based mobile agents. Experiments on the proposed model shows that OBPNN based detection engine can process network traffic 16 times faster than the maximum packet transfer rate of 100 Mbps network. The recorded payload size of the agent is 2KB which is very less in comparison to 26KB recorded by other authors. Also, the recorded round trip time of agent is 110 ms, which is 4.42 seconds recorded by others. Enhancements in the processing speed, agent size and mobile agent round trip time, could able to lower the response time of the attack detection process. Beyond this,the high speed additional behavioral layer has the capability to detect land and back multi class attack. Hence, the model not only addresses the problem of identifying multi class attacks, but also reduces the response time to a greater extent, thus improvinig the performance of the dection rate.

2 Brief description on the state of the art of the research topic

Over the last two decades, researchers have done work on network attacks and their identification, which is based on single class classification, where the network traffic can be classified as one of the defined classes for different attacks. However, no effort has been put towards the multi class classification of network traffic, so that in case of combined attack, the classifier can identify the multiple classes indicating the concerned attacks. As a result, during the literature review of multi class attacks, we did not get any research paper, addressing multi

class attack classification. However, only few inventions in other fields claimed multi class classification. Patent No: CN 102722726 [32], Patent No: US6816456 [33] and Patent No: US20080320010A1 [34] claims multi class classification, where the input is classified into one of the multiple classes. Hence, these patents are not supporting multi class classification in true sense. Similarly, Patent No: US20100014762 [35] requires user calibration and Patent No: US006823323B2 [36] requires pre-existing multi class dataset for training and testing the multi class classifier. So, both the inventions are not capable to support multi class classification of attack due to a large number of real time network traffic suppose to be processed and non availability of multi class training and testing attack datasets.

For detecting multi class attacks, multi class classifier must be trained and tested using pre-existing multi class attack datasets. But, there does not exist any such multi class attack dataset. However, the multi class dataset can be generated from pre-existing single class records. But none of the research papers or inventions addressed the generation of multi class dataset from pre-existing single class records, which can be used to develop additional behavioral layer.
For improving existing capacity of IDS, usage of additional behavioral layer had been started since last decade. [10], [13], [14], [15], [27], [28], [29] and [30] are few examples of multi layered IDS. In [13], the authors proposed a multi layered model which uses frequent attack signatures list and reduces packet dropping rate from 7.68% to 1.7%. But the problem is, if attacks do not belong to frequent attack list, then complexity of attack detection process increases, which leads to high response time as well as high packet dropping rate. One more multi layered model with objective of misuse and anomaly detection is proposed by authors of [14]. Authors were able to achieve 94% anomaly detection rate. Major limitation of the model is the poor performance in online mode. Authors of [30] had also proposed a multi layered model which took 3.98 seconds as overall trip of the agent which includes sniffing, processing and migration of the agent. Similarly, authors of [10] recorded 4.42 seconds as the round trip time of the agent. Beyond this, from our detailed literature review on multi layered IDS in [10], [13], [14], [15], [27], [28], [29] and [30], we found high response time as one of the major challenge. More detail about literature review is available in our paper [37].

From our literature review, we concluded that none of the researchers or inventors discussed on generation of multi class dataset which in turn used to develop an additional behavioral layer for detecting multi class attacks. But our experiment and literature review

shows that, usage of additional behavioral layer increases the response time, further increasing the packet dropping rate and decreasing false alarm rate. Both these lacunas have been addressed in the proposed model.

3 Definition of the problem

- Detecting Multi class attack has been considered as a novel problem. A multi class attack is a combination of the characteristics of two or more attacks. Under such attack, the IDS may identify as any one of the single class attack. In this context, the problem is to develop such a robust model that can identify the attack as a multi class attack and also identify all the single class attack comprising the multi class attack.
- The proposed model should be accompanied with additional behavioral layer, and to train and test it accordingly so as to resolve the said problem. This addition leads to high response time which must need to be reduced.

4 Objective and scope of work

1) To generate multi class attack dataset from pre-existing single class attack dataset.
2) To use the generated multi class attack dataset for training and testing of the additional behavioral layer so as to detect multi class attack from real-time network traffic.
3) To reduce the response time of the multi layered IDS through optimization.

5 Original contribution by the thesis

The entire work in this synopsis, as well as thesis is the original work, with the patent and research papers as the back bone. The proposed model has been visualized as a collection of various modules, each of which with relevant publications. The details of the associated patent and papers are as follows:

Patent Applied:

1) Multi Class Classifier From Single Class Dataset, by Shah Bhavin and Bhushan Trivedi (2015, May 5). *Patent Number* 1794/MUM/2015.
   Available: https://ipindiaonline.gov.in/patentsearch/search/index.aspx

Paper Presented / Published:

2) Artificial Neural Network based Intrusion Detection System: A Survey. International Journal of Computer Applications 39, no. 6 (2012): 13-18.

3) Optimizing Back Propagation Parameters For Anomaly Detection, IEEE - International Conference on Research and Development Prospectus on Engineering and Technology (ICRDPET), 2013.
4) Data Set Normalization : For Anomaly Detection Using Back Propagation Neural Network, IEEE - International Conference on Research and Development Prospectus on Engineering and Technology (ICRDPET),2013.
5) Improving Performance of Mobile Agent Based Intrusion Detection System , IEEE International Conference on Advanced Computing & Communication Technologies-2015.
6) Reducing Features of KDD CUP 1999 Dataset For Anomaly Detection Using Back Propagation Neural Network , IEEE International Conference on Advanced Computing & Communication Technologies-2015.

Paper Submitted:

7) Detecting Multi Class Attacks in Intrusion Detection System, IEEE/ACM Transaction on Networking.
8) Improving Anomaly Detection Process By Detecting Multi Class Attack Using Additional Behavioral Layer, IEEE Transactions on Systems, Man, and Cybernetics.
9) Dataset Generation For Host-Based Intrusion Detection System From Dataset of Network Based Intrusion Detection System , International Conference on Communication and Networks (COMNET 2015).

6 Methodology of research, results / comparisons

6.1 Methodology of research

We used qualtitative and exploratory approach for this research work. During the literature review we referred various research papers, patents, annual reports of market leading companies like Cisco [3], Sophos [4] and Symantec [5]. In addition to this, we installed snort [16] which is an open source IDS and observed it's functioning. During this initial phase of literature review, we found researcheres had done work on single class attack classification and no attempt had been taken for multi class attack classification. Major reasons for this gap are unavailability of multi class classifier and unavailability of multi class dataset for training and testing such classifier.

During the literature review, we found research works based on additional behavioral layer for detecting any unknown attacks. Therefore, our second phase of literature review was mainly focused on additional behavioral layer. By comparing various IDS which uses additional behavioral layer, we found high response time as one of the major challenge. As a result of both phases of literature review, we proposed a model with the objectives 1) To detect multi class attack by providing additional behavioral layer and 2) To reduce the response time of such multi layered IDS. Architecture and deployment layout of the model is shown in Fig.1 and Fig.2. The model consists of four modules: 1) Existing IDS, 2) Additional IDS, 3) Mobile Agents and 4) IDS Manager. The Existing IDS is used to detect misuse attacks and the Additional IDS with the help of additional behavioral layer detects multi class attacks. Additional IDS has Feature Extraction, Normalization, Multi Class Attack Detection Engine and Connection Based Additional Behavioral Layer as the sub modules. For exchange of information between additional IDS and IDS Manager, model uses light weight mobile agents. Detail of each module is available in the Proposed Model Sub Section.

To fulfill the objectives, the proposed model has been implemented in two phases. In the first phase, the responce time is being reduced while the second phase dealt with detecting multi class attacks. In the first phase, model uses KDD CUP 1999 dataset [25] which is publicly available while in second phase, model generates its own dataset. During both the phases, same architecture and deployment layout which is presented in Fig.1 and Fig.2 are used. Model uses, Accuracy, Precision, Recall and Fscore as the performance measures.

6.2 The Model and its components

Architecture and deployment layout of the model is shown in Fig.1 and Fig.2. Model consists of four modules: 1) Existing IDS, 2) Additional IDS, 3) Mobile Agents and 4) IDS Manager.

6.2.1 Existing IDS

In the proposed model, existing IDS is used to detect misuse attack. Snort [16], Bro[17], Suricata [18], AIDE [19], OSSEC HIDS[20], Prelude Hybrid IDS[21], Samhain- HIDS [22] are few examples of IDS which can be used as existing IDS in the proposed model. Model uses snort as existing IDS.

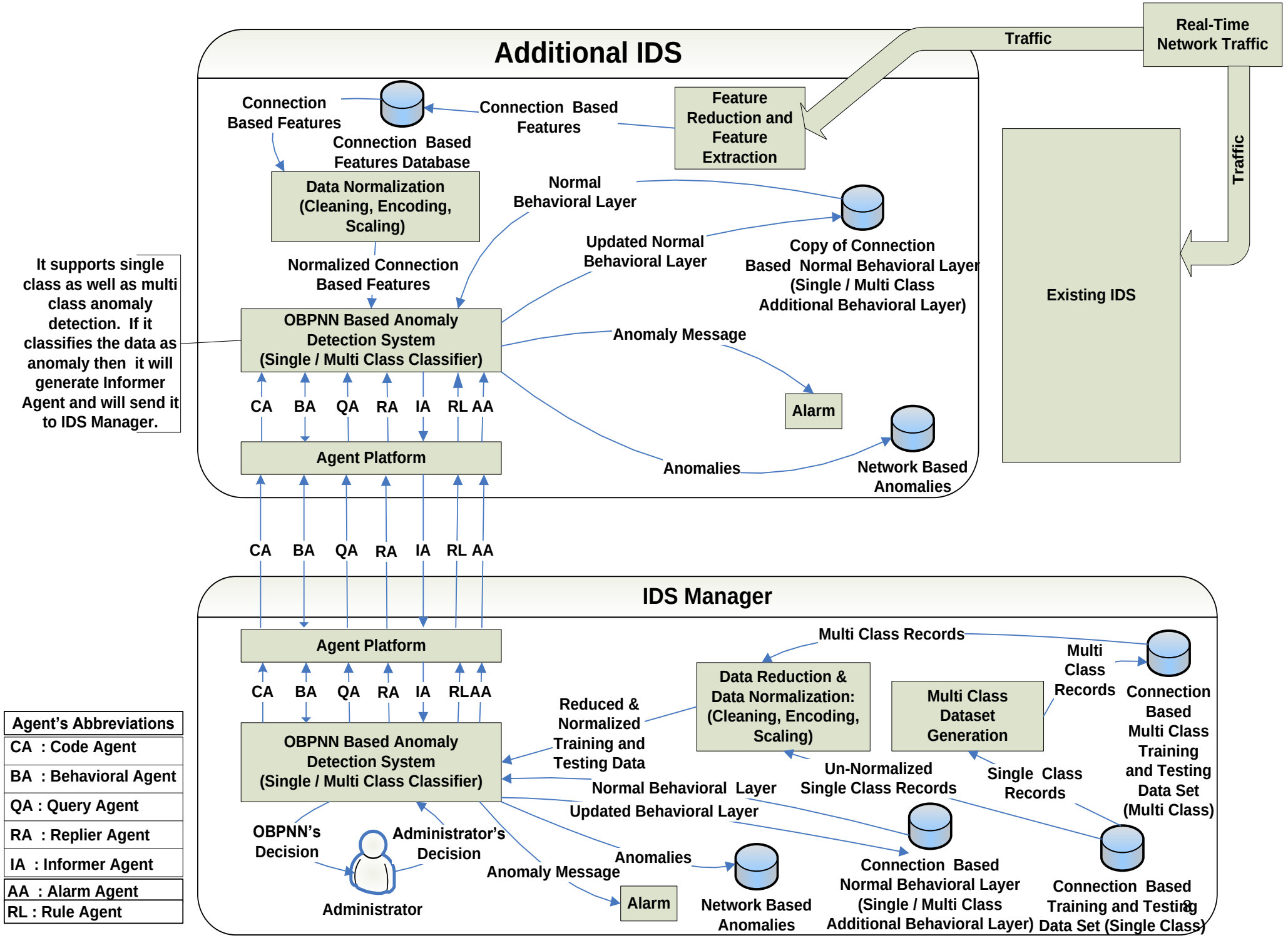

Fig.1. Architecture of the Proposed Model

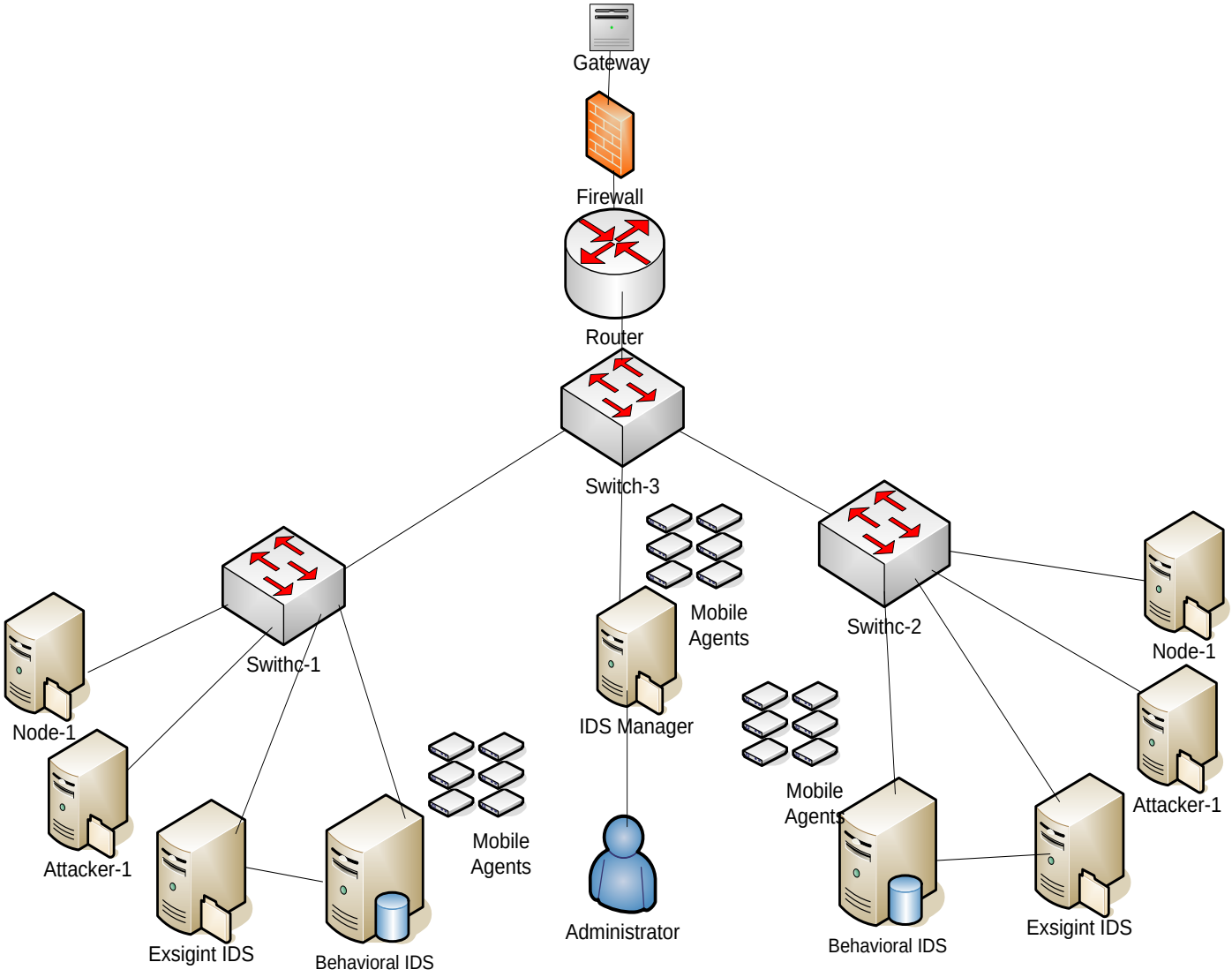

Fig.2. Deployment Layout of the Proposed Model

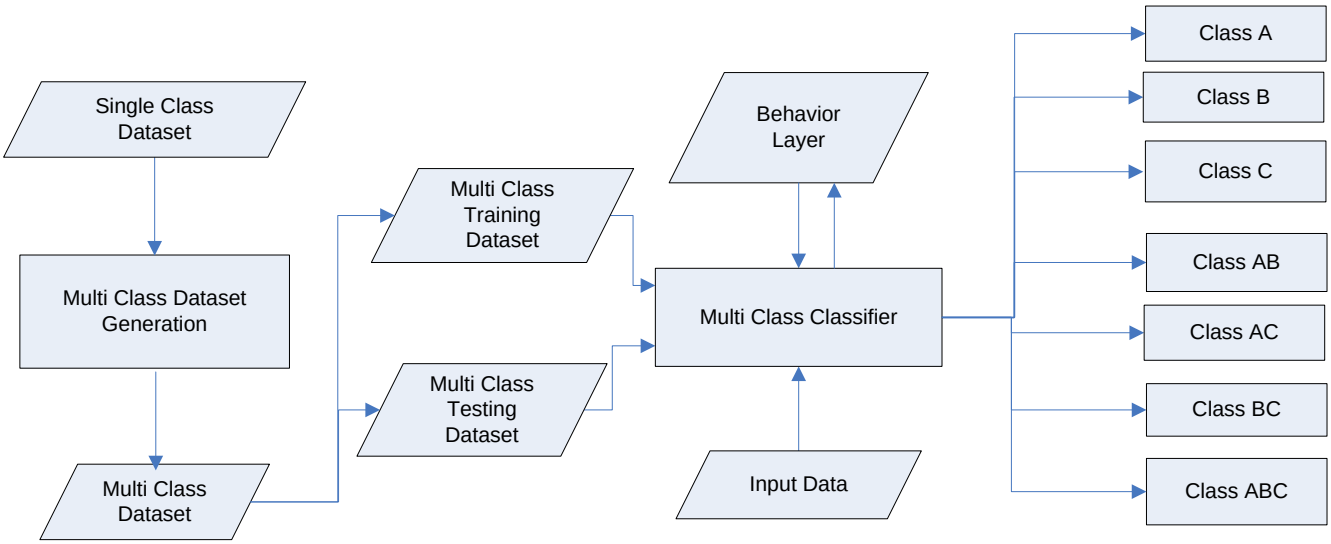

Fig. 3. Multi class classifier which uses multi class training and testing dataset which is generated from single class dataset

6.2.2 Additional IDS

Proposed model uses additional IDS with two objectives 1) To detect multi class attack and 2) To reduce response time. Following are sub modules of Additional IDS.

6.2.2.1 Feature Reduction

During first phase of impliemenation, model uses KDD CUP 1999 dataset. For feature reduction, model applies techniques presented by Tesfahun et al. [6] and reduces features of KDD CUP 1999 dataset from 41 to 22. Model with such redcued features improves performance and reduces processing time as well as complexity of proposed model [6] [7] [8] [9]. More details about feature reduction are available in our previous work of [31] and [37].

6.2.2.2 Feature Extraction

Set of features selected by feature reduction sub module is extracted by feature extraction sub module. Features are extracted from real- time network traffic and stored in file or database.

6.2.2.3 Data Normalization

Data which is supposed to feed to the detection engine is un-normalized which increases training time and response time[23]. To minimize training time and response time, we had already developed and tested data normalization model which is available in [12] and shown in Fig.4. Data Normalization model contains Encoding, Scaling, Lossless Size Reduction and Checking modules.

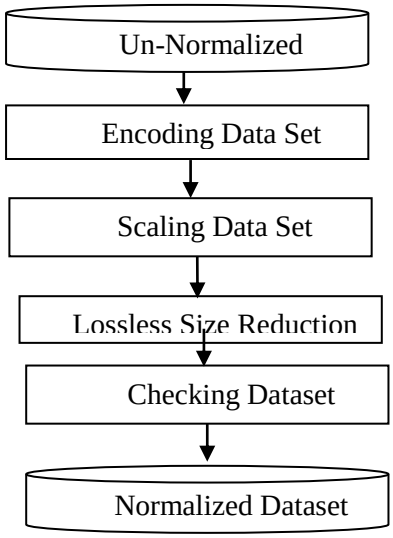

Fig.4. Data Normalization Model [12]

6.2.2.4 Detection Engine

To detect the intrusion, researcher uses various detection techniques like Back Propagation Neural Network (BPNN), Self Organizing Maps, Support Vector Machine (SVM), Radial Basis Function (RBF) and Simulated Annealing [2]. High speed detection engine which is capable to classify the data in to multiple classes are candidate for detection engine in the proposed model. Model uses BPNN as detection engine. Reasons for selection of BPNN as detection engine are available in our previous work of [2] and [37]. For further improvement in detection speed of BPNN, we had optimized parameters of BPNN which is available in [11]. BPNN with such optimized parameters is referred as OBPNN in this model.

6.2.2.5 Multi Class Classification

To achieve multi class classification of network traffic, model uses OBPNN. To train and test OBPNN, multi class training and testing dataset is required. As there does not exist any such dataset, model generates multi class training and testing datasets. More details about generation of multi class dataset and training and testing additional behavioral layer by generated multi class dataset is shown in Fig.3. More details about multi class dataset generation and multi class classification are available in our previous work [26].

6.2.3 Mobile Agent

To exchange information between various components, model uses mobile agents. Details about mobile agent, their attributes and usage are available in TABLE I.

TABLE I: List of Mobile Agents Used in the Model

Agent	Attributes	Usage
Informer Agent	ticket_no, normalized_data, node_decision	When additional IDS needs to pass data to IDS Manager, it sends Informer Agent with unique ticket_no, normalized_data and decision. ticket_no is used for unique identification of the data.
Replier Agent	ticket_no, admin_decision, updated weights	IDS Manager sends Replier Agent for sending reply to the node from which Informer Agent came. If decision is "not an attack" then updated weight field will be blank.
Alert Agent	normalized_data, decision	Whenever IDS Manager wants to alert other Additional IDS regarding current attack, it sends Alert Agent.
Query Agent	-----	To check whether Additional IDS is compromised or not, IDS Manager sends Query Agent to Additional IDS.
Behavioral Agent	behavioral_layer	To send behavioral layer (weights) between Additional IDS and IDS Manager.
Code Agent	OBPNN Code	To send OBPNN Code (Class File) from IDS Manager to the newly added Additional IDS.
Rule Agent	Rule File	To send the rules generated by administrator. IDS Manager sends Rule File to existing IDS via Additional IDS.

For improvement in detection speed, size of agent and response time in the model, following are the suggestions which we had implemented . More details are available in our previous work of [24].

- Size of chain of agent: Desinge the communication architercure so that size of chain of agent should be minimized.
- Detection technique: Use high speed detection technique like OBPNN.
- Size of payload: Instead of traditional detection technique, ANN based technique should be used as it requires less data. Further, data reduction and data normalization techniques must be used to for further reduction in payload size.
- Architecture: To reduce response time of mobile agent based IDS, use client –server architecture.

6.2.4 IDS Manager

Model used IDS manger to achieve following objectives:

- To check integrity of Additional IDS
- To take Administrator's view for the current attack
- To give confirmation of attack to Additional IDS
- To add and update Additional IDS
- To maintain a copy of network anomalies database

6.3 Results / Comparisons

To fulfill the objectives, model is implemented in two phase. In first phase, model is implemented for reducing the response time while in second phase model is implemented for detecting the multi class attack. In the first phase, KDD CUP 1999 [25] data set is used while in second phase, auto generated dataset of land and back class is used.

6.3.1 Feature Reduction

For the experiment related to reduction of response time, model uses KDD CUP 1999 dataset which has 42 features. Model applies feature reduction technique of Tesfahun [6] and reduces features of KDD CUP 1999 dataset from 41 to 22. To compare both the dataset, we did three comparisons. Results of Basic Comparison, N- Fold Validation and Testing Comparison are shown in TABLE II, TABLE III and TABLE IV respectively. Results of basic comparison clearly shows that reduced dataset outer perform on size, time and complexity parameters. Results of N-Fold (N=10) validation clearly shows that reduced dataset has better generalization

capacity. Further, results of Testing Comparison show that both models are equally compatible. From these three comparisons, it clearly shows that reduced dataset is better or is equally capable, and does not have any drawback as compared to full dataset.

TABLE II : BASIC COMPARISON OF REDUCED AND ORIGINAL DATASET

Criteria	BPNN With Reduced Features of KDD Dataset (Model -1)	BPNN With Full Features of KDD Dataset (Model-2)	Remarks
Number of Inputs	22[1]	41	46% Reduction
Number of Hidden Units in Layer 1	9	18	50% Reduction
Number of Hidden Units in Layer2	9	18	50% Reduction
Time Required For 40 Epochs (In Seconds)	1548	2882	46% Reduction
Dataset Size (In KB)	37961	58255	35% Reduction

TABLE III : RESULT OF 10 FOLD VALIDATION

Criteria	BPNN With Reduced Features of KDD Dataset	BPNN With Full Features of KDD Dataset	Remarks
Max Accuracy	96.7%	94.9%	1.8% Improved
Epoch No at Max Accuracy	3	3	No Effect
Precision at Max Accuracy	0.999729	0.999911	-0.00018 Degraded
Recall at Max Accuracy	0.97275	0.964004	0.008746 Improved
Fscore at Max Accuracy	0.985744	0.981162	0.004582 Improved

TABLE IV : TESTING COMPARISON OF REDUCED DATASET WITH ORIGINAL DATASET

Criteria	BPNN With Reduced Features of KDD Dataset (Model -1)	BPNN With Full Features of KDD Dataset (Model-2)	Remarks
Accuracy	91%	91%	No Effect
Precision	0.996699	0.99656	-0.00014
Recall	0.90059	0.89450	0.00608
Fscore	0.94615	0.94284	0.00330

6.3.2 Data Normalization

By applying normalization technique on KDD CUP 1999 dataset, we were able to reduce size of dataset by 28%. Such reduced dataset will improve performance in terms of hardware resource utilization, complexity and processing speed of the model [12].

6.3.3 Optimal Back Propagation Neural Network

Our experiment on OBPNN based detection engine shows that it is capable to process 80000 data records per second where each data record has 22 features [24]. This detection engine is 16 times faster than the maximum packet transfer rate of a 100Mbps network.

6.3.4 Mobile Agent

The model which is based on our solutions on mobile agents takes on an average 100 ms as the round trip time of agent, showing a better performance in comparison to the models presented in [30] [10] which takes 3.98 seconds and 4.42 seconds as the round trip time respectively. Hence, our solutions will reduce network traffic and response time to a large extent. Such reduced response time will also helps to reduce false alarm rate due to zero packet dropping rate.

7 Achievements with respect to objectives

- The outcomes of the first phase clearly indicated that our model is capable to process the network traffic 16 times faster than the maximum packet transfer rate of a 100 Mbps network.
- Our model takes on an average 100 ms as round trip time of agent while the model presented in [30] [10] takes 3.98 seconds and 4.42 seconds as a round trip time respectively.
- Model detects multi class attack of land and back class.

8 Conclusion

Multi class attack is a unknown attack in which attacker attacks by combing the characteristics of two or more attack classes. For detecting attacks, other than such multiclass attacks, IDS is widely used since last two decades. However to deal with such unknown multi class attack, existing IDS fails as it is not trained accordingly. Existing IDS generally detects only one out of all attacks and cannot see anything related to other attacks. Thus to deal with such attacks, we have proposed a multi layered model in which additional behavioral layer is used to detect multi class attacks.

Our literature review and experiments on multi layered IDS, shown high response time as one of the major challenge. To reduce the response time, the proposed model uses Optimized Back Propagation Neural Network (OBPNN) for high speed detection. Further improvement in

the detection speed is achieved by combining feature reduction, data normalization, light weight mobile agents and client server architecture.

The proposed model has been implemented in two phases. During first phase, the objective was to improve the response time. The results of the first phase clearly indicated that our model is capable of processing the network traffic 16 times faster than the maximum packet transfer rate of a 100Mbps network. Moreover, it takes on an average 100 ms as the round trip time of agent, showing a better performance in comparison to the models presented in [30] [10] which takes 3.98 seconds and 4.42 seconds as the round trip time respectively.

During the second phase of our implementation, we have added a behavioral layer to the model designed in the first phase. The behavioral layer is specifically designed for detecting multi class attacks. The results of our experimentation on real-time network traffic shows that we were able to detect multi class attacks of two different types; viz. land and back attack. Results also reiterate that the proposed model does not only detect multi class attacks using additional behavioral layer but also reduces the response time of detecting such additional attacks.

9 Copies of papers published and a list of all publications arising from the thesis

9.1 Paper presented / published

Sr.	Title	Journal / Conference	Remarks
1	Artificial Neural Network Based Intrusion Detection System: A Survey	International Journal of Computer Applications (0975 – 8887) Volume 39– No.6, February 2012	IF : 0.835 **Number of Citations Count:18**
2	Optimizing Back Propagation Parameters For Anomaly Detection	IEEE International Conference On Research And Development Prospects On Engineering And Technology -2013 (ICRDPET-2013) , 29- 30 March, 2013.	**Best paper award**
3	Dataset Normalization For Anomaly Detection Using Back Propagation Neural Network		Runner up paper
4	Reducing Features of KDD CUP 1999 Dataset For Anomaly Detection Using Back Propagation Neural Network	IEEE International Conference On Advanced Computing & Communication Technologies (ACCT-	**Best paper award**

5	Improving Performance of Mobile Agent Based Intrusion Detection System	2015),21-22 February, 2015	Runner up paper

9.2 Papers in communication

Sr.	Title	Journal / Conference	Remarks
6	Detecting Multi Class Attacks in Intrusion Detection System	IEEE/ACM Transaction on Networking	**IF : 1.811 Submitted on 27th August, 2015)**
7	Improving Anomaly Detection Process	IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS	**IF : 1.699 Submitted on 28th October, 2015**
8	Dataset Generation For Host-Based Intrusion Detection System From Dataset of Network Based Intrusion Detection System	International Conference on Communication and Networks (COMNET 2015)	Conference Date :26-27 December, 2015

10 Patents (if any)

Title	Multi Class Classifier From Single Class Dataset
Filed At	Indian Patent Office
Application No.	1794/MUM/2015
Application Date	5th May, 2015
Applicants & Inventors	Bhavin Shah, Bhushan Trivedi (Ph.D.)
Application Status	Patent is Published on Indian Patent Website &
Objection Received	NIL
Website Link	https://ipindiaonline.gov.in/patentsearch/search/index.aspx

11 Achievements

- Published / Presented 5 papers at international level
- One of the papers is cited by 18 authors.
- Two papers has been awarded as “Best Paper Award” in IEEE international conference
- Secured 100% score in machine learning course conducted by Stanford university (Coursera)
- Secured 2nd rank in CCNSP exam conducted by Cyberoam

12 References

[1] Wang, H. Q., et al. "Mobile agents for network intrusion resistance." Advanced Web and Network Technologies, and Applications. Springer Berlin Heidelberg, 2006. 965-970.

[2] Shah, Bhavin, and Bhushan H. Trivedi. "Artificial Neural Network based Intrusion Detection System: A Survey." International Journal of Computer Applications 39, no. 6 (2012): 13-18.

[3] Annual Security Report-2015",” Cisco, 2015.

[4] “Internet Security Threat Report-2015”, Symantec, April-2015.

[5] James Layne, "Security Threat Trends 2015", Sophos, 2015.

[6] Tesfahun, Abebe, and D. Lalitha Bhaskari. "Intrusion Detection Using Random Forests Classifier with SMOTE and Feature Reduction." *Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 2013 International Conference on*. IEEE, 2013.

[7] Zhang, Fengli, and Dan Wang. "An Effective Feature Selection Approach for Network Intrusion Detection." Networking, Architecture and Storage (NAS), 2013 IEEE Eighth International Conference on. IEEE, 2013.

[8] Das, Sanmay. "Filters, wrappers and a boosting-based hybrid for feature selection." ICML. Vol. 1. 2001.

[9] Kun, Gao, and Jin Sumei. "Research on the application of mobile agent in intrusion detection technology." Computer Engineering and Technology (ICCET), 2010 2nd International Conference on. Vol. 6. IEEE, 2010.

[10] Eid, Mohamad. "A new mobile agent-based intrusion detection system using distributed sensors." proceeding of FEASC (2004).

[11] Bhavin Shah, Bhushan H. Trivedi, Optimizing Back Propagation Parameters For Anomaly Detection, IEEE - International Conference on Research and Development Prospectus on Engineering and Technology (ICRDPET),2013.

[12] Bhavin Shah, Bhushan H. Trivedi, Data Set Normalization : For Anomaly Detection Using Back Propagation Neural Network, IEEE - International Conference on Research and Development Prospectus on Engineering and Technology (ICRDPET),2013.

[13] Uddin, Mueen, Kamran Khowaja, and Azizah Abdul Rehman. "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents." International Journal of Network Security & Its Applications 2.4 (2010).

[14] Ding, Yu-Xin, Min Xiao, and Ai-Wu Liu. "Research and implementation on snort-based hybrid intrusion detection system." Machine Learning and Cybernetics, 2009 International Conference on. Vol. 3. IEEE, 2009.

[15] Aydın, M. Ali, A. Halim Zaim, and K. Gökhan Ceylan. "A hybrid intrusion detection system design for computer network security." Computers & Electrical Engineering 35.3 (2009): 517-526.

[16] http://www.snort.org

[17] https://www.bro.org/

[18] http://suricata-ids.org/

[19] http://aide.sourceforge.net/

[20] http://www.ossec.net/

[21]https://www.prelude-ids.org/

[22]http://www.la-samhna.de/samhain/

[23] Kang, Boojoong, et al. "Rule indexing for efficient intrusion detection systems."Information Security Applications. Springer Berlin Heidelberg, 2012. 136-141.

[24] Improving Performance of Mobile Agent Based Intrusion Detection System ,Shah Bhavin and Bhushan H. Trivedi IEEE International Conference on Advanced Computing & Communication Technologies-2015.

[25] University of California, Irvine, KDD Cup 1999 Data SET, 1999, http://kdd.rcs.uci.edu/databases/kddcup99/kddcup99.htm.

[26] Bhavin Shah and Bhushan Trivedi, Detecting Multi Class Attacks in Intrusion Detection System, IEEE/ACM Transaction on Networking (Paper Submitted).

[27] Díaz-Verdejo, J.E., García-Teodoro, P., Muñoz, P., Maciá-Fernández, G., De Toro, F.:Una aproximación basada en Snort para el desarrollo e implantación de IDS híbridos (A Snort-based approach for the development and deployment of hybrid IDS). IEEE Latin America Transactions 5(6), 386–392 (2007)

[28] Hwang, K., Cai, M., Chen, Y., Qin, M.: Hybrid Intrusion Detection with Weighted Signature Generation Over Anomalous Internet Episodes. IEEE Transactions on Dependable and Secure Computing 4(1), 41–55 (2007)

[29] Wuu, L.C., Hung, C.H., Chen, S.F.: Building intrusion pattern miner for Snort network intrusion detection system. Journal of Systems and Software 80(10), 1699–1715 (2007)

[30] Xiu-liang, Mo, Chun-dong Wang, and Huai-bin Wang. "A Distributed Intrusion Detection System Based on Mobile Agents." Biomedical Engineering and Informatics, 2009. BMEI'09. 2nd International Conference on. IEEE, 2009.

[31] Shah Bhavin and Bhushan H. Trivedi, Reducing Features of KDD CUP 1999 Dataset For Anomaly Detection Using Back Propagation Neural Network , IEEE International Conference on Advanced Computing & Communication Technologies-2015.

[32] Multi-class support vector machine classification method based on dynamic binary tree, Wei Lei, Zhu Hong, Cheng Chunling, Wang Yashi, Sui Zongjian,(2012,06 05). Patent Number CN 102722726 [Online]. Available : https://patentscope.wipo.int/search/en/detail.jsf?docId=CN85338120 &redirectedID=true

[33] Methods and apparatus for network use optimization, Tse-Au, Elizabeth Suet Hing, (2000,02 04). Patent Number US6816456 [Online]. Available: https://patentscope.wipo.int/search/en/detail.jsf? docId= US40356329&redirectedID=true

[34] Sensitive webpage content detection, Li Ying, Mah Teresa, Tong Jie, Jin Xin, Sathe Saleel, Xu Jingyi (2007,05 14). Patent Number : US20080320010 A1 [Online]. Available: https://patentscope. wipo.int/search/en/detail.jsf?docId=US42659206&redirectedID=true

[35] Categorizer with user-controllable calibration, Renders Jean-Michel, Privault Caroline, Cheminot Eric H, (2008,07,17). Patent Number : US20100014762 [Online]. Available : https://patentscope. wipo.int/search/en/detail.jsf?docId=US43522913&redirectedID=true

[36] Automatic classification method and apparatus, George H. Forman, Port Orchard, Henri J. Suermondt, Sunnyvale. (2004,11 23). Patent Number : US006823323 [Online]. Available: http://www.uspto .gov/

[37] Bhavin Shah and Bhushan Trivedi, Improving Anomaly Detection Process By Detecting Multi Class Attack Using Additional Behavioral Layer, IEEE Transactions on Systems, Man, and Cybernetics (Paper Submitted).