DOS and Naivebyes model for U2R and R2L. This observation can be readily mapped to Assembly classifier topology as in figures 3. Table (9)

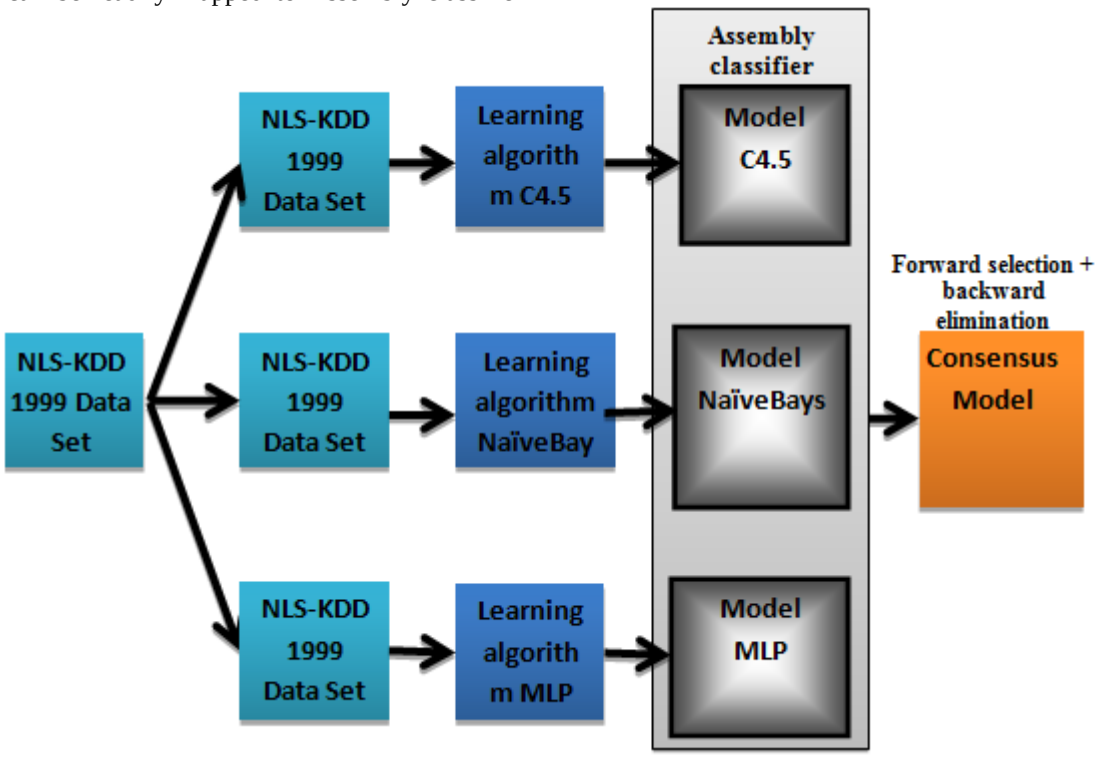

Figure 3: Assembly classifier topology

Suggests that the Assembly classifier model showed significant improvement inaccurac**y** rates for attack categories. Also the False Positive (FP) was reasonably small for all attack categories.

Table 10: Comparative detection performance of Assembly classifier.

Attack type	*C4.5%*	*Naïve Byes%*	*MNN %*	*Assembly classifier (C4.5, Naïve Byes, M LP)%*
Normal	97	86	93	97
DOS	81	71	74	72
PROBE	59	92	64	72
R2L	001	09	03	25
U2R	0	33	0	51

Table (10) shows the performance comparison of the proposed Assembly classifier model with others in literature. Table(10) summarizes the test results achieved for the five-class classification using C4.5 classifier, NaïveBays classifier, MLP classifier and the Assembly classifier of all three classifiers (C4.5, NaïveBays& MLP).

5. Conclusion

A simulation study was performed to assess the performance of a comprehensive set of machine learning algorithms on the NLS-KDD 1999 Cup intrusion detection dataset. Simulation results demonstrated that for a given attack category certain classifier algorithms performed better. Consequently, Assembly classifier model that was built using most promising classifiers for a given attack category was evaluated for probing, denial-of-service, user-to-root, and remote-to-local attack categories. The proposed Assembly classifier showed improvement in accuracy and false alarm rates for most of attack categories as compared to the NLS-KDD 1999 Cup winner. Furthermore, reduction in cost per test example was also achieved using the Assembly classifier model. However, none of the machine learning classifier algorithms evaluated was able to perform detection of user-to-root and remote-to-local attack categories significantly (no more than 51% detection for U2R and 25% for remote-to-local category). In conclusion, it is reasonable to assert that machine learning algorithms employed as classifiers for the NLS-KDD 1999 Cup data set do not offer much promise for detecting U2R and R2L attacks within the misuse detection context.

References

[1] Anderson. J. P. "*Computer Security Threat Monitoring and Surveillance*." Technical Report, James P Anderson Co., Fort Washington, Pennsylvania, 1980.
[2] Akbar, S., D.K.N. Rao, and Dr.J.A.Chandulal, *Intrusion Detection System Methodologies Based on Data Analysis.* International Journal of Computer Applications (0975 – 8887, 2010. **5– No.2, 2010**
[3] Denning D. An intrusion-detection model. IEEE Trans Software Engng 1987;SE-13(2):222–32.
[4] Kumar S, Spafford EH. *An application of pattern matching in intrusion detection.* Technical Report CSD-TR-94013, Purdue University; 1994a.
[5] Mahoney M, Chan PK. *An analysis of the 1999 DARPA/Lincoln laboratory evaluation data for network anomaly detection.* Sixth International Symposium on Recent Advances in Intrusion Detection; 2003. p. 220–37
[6] Tavallaee, M., et al,*"A detailed analysis of the KDD CUP 99 data set"*,Proceedings of the Second IEEE

Symposium on Computational Intelligence for Security and Defence Applications 2009, 2009.
[7] X. Xu, X.N. Wang, "Adaptive network intrusion detection method based on PCA and support vector machines," Lecture Notes in Artificial Intelligence, ADMA 2005, LNAI 3584, 2005, pp. 696-703.
[8] P. Gifty Jeya,M. Ravichandran,C. S. Ravichandran,"*Efficient Classifier for R2L and U2R Attacks*",International Journal of Computer Applications (0975 – 8887, 2012. **45**.
[9] PrabhjeetKaur ,Amit Kumar Sharma, Sudesh Kumar Prajapat*"MADAM ID FOR INTRUSION DETECTION USING DATA MINING*" IJRIM Volume 2, Issue 2 (2012) (ISSN 2231- 4334).
[10] Ron Kohavi and Ross Quinlan. *Decision Tree Discovery*. In Handbook of Data Mining and Knowledge Discovery
[11] I.H. Witthen, E. Frank, *"Data Mining: Practical Machine Learning Tools and techniques with Java Implementations*," Morgan Kaufmann Publishers, 1999.
[12] John, G.H., Langley, P.: *Estimating Continuous Distributions in Bayesian Classifiers*. In: Proc. of the 11th Conf. on Uncertainty in Artificial Intelligence (1995).
[13] Werbos, P.: Beyond Regression: *New Tools for Prediction and Analysis in the Behavioral Sciences*. PhD Thesis, Harvard University (1974)
[14] http://iscx.cs.unb.ca/NSL-KDD/.
[15] Elkan, C., *Results of the KDD'99 classifier learning.* ACM SIGKDD Explorations Newsletter, 2000. **1**(2): p. 63-64.