International Journal of Pure and Applied Mathematics
Volume 117 No. 21 2017, 947-952
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A SUPERVISED LEARNING APPROACH USING SUPPORT VECTOR MACHINE FOR INTRUSION DETECTION SYSTEM IN MANET

[1]S. Vimala,[2] Dr. V. Khanna,[3]Dr.C.Nalini

[1]Research Scholar, Bharath University, Chennai, India

[2]Dean, Informatics, Bharath University, Chennai, India

[3]Professor,Department of CSE,Chennai,India

***Abstract*- T**he network-based intrusion detection system has been proposed and executed with the assistance of the Support Vector Machine which gives viable guidelines for grouping of normal and abnormal events. This approach has been actualized for host which involves arrange have intrusion detection system. Intrusion detection can be mechanized by making the framework take in utilizing support vector classifiers from a training set. An advantage of Machine Learning is that the systems are fit for summing up from known attacks to varieties, or even can recognize new sorts of intrusion. Late research concentrates more on the hybridization of strategies to enhance the detection rates of Machine learning classifiers. Real time dataset is used in the experiments to demonstrate that Support Vector Classifier can greatly improve the classification accuracy and the approach achieves higher detection rate with low false alarm ratio and is sustain for large datasets, follow-on in a successful Intrusion Detection System. Compared with other classifier algorithms, support vector classifier has the advantage of utilizing the sparseness and reduces the false alarms while still maintaining desirable detection rate. Contrasted and other classifier algorithm, support vector classifier has the benefit of using the meager condition and diminishes the false alerts while as yet keeping up alluring detection rate.**

.

Keywords: MANET, Support vector Machine , Intrusion Detection System, Classification

1.INTRODUCTION

A Self-configuring network, ad-hoc is a decentralized type of wireless network in connecting mobile nodes forms one of the distinguishing characteristics, dynamic topologies. It is known that each node in any network acts both as a router and a hostdue to lack of infrastructure. This type of wireless nature of communication raises several security problems.For instance, the mobile nodes which communicate directly with each other and without the aid of access points have no fixed infrastructure. They form an arbitrary topology, where the routers are free to move randomly and arrange themselves as required.At this stage, each node or mobile device is equipped with a transmitter and receiver[10][13]. They are said to be purpose-specific, autonomous and dynamic. This compares greatly with fixed wireless networks in which there ad-hoc network.As far as the relying Nodes on establishing the communicationare considered,they act as a router.As such, in a mobile ad-hoc network, a packet can travel from a source to a destination either directly, or through some set of intermediate packet forwarding nodes. In this type routing protocols stuck between any pair of nodes in an ad hoc network can be hard because the nodes can move randomly and can also join or leave the network.So, Ad-hoc networks are highly vulnerable to security attacks and dealing this is challenging task for the developers.In order not to impede the attempt, the difficulties examined for the future predicament[1].

The main reasons for this difficulty are; "Shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among nodes, limited availability of resources, and physical vulnerability." When considering the security of a network, we examine it under the headings:(i) ‘availability’ which remains operational at all times, (ii)‘confidentiality’ that prevents information to be made known to certain users, (iii)‘authentication’, the ability of a node to identify the node with which it is communicating,(iv) ‘integrity’ which guarantees the message not to be corrupted during transfer the files, and the last is (v) the ‘non repudiation’through which sender cannot deny sending the message. Phenomenally, an ad-hoc network needs extra security requirements because of its lack of proper infrastructure and the dynamic relationship between the nodes in the network. The accountability here is very difficult to determine as there is "no central authority which can be referenced when it comes to making trust decisions about other parties in the network." ‘Intrusion’ is another enumeration here has its definition as “any set of actions that attempts to compromise the integrity, confidentiality or availability of resources”. Intrusion Detection Systems (IDS) are mainly used to detect and call attention of suspicious behavior[2][3].

It is important to state the function of IDS here. IDS works on three processes/modules, these are collection of information, detection and response.At firstly, collection of data which is done from end to end all or selective nodes in the networks at user level, network level and application logs. Secondly, detection processes is done through some detection engines/techniques viz. anomaly, misuse and specification based. The third and the last one is response nessage to all

the benign nodes. To the convenience the existing IDS architectures for MANETs is categorized into four :i) Stand Alone IDS -a single participating node in detection by running IDS independently using node's local data exclusively, ii) Cooperative - every node participating in the detection by sharing audit information with other nodes to detect more accurately, iii) Distributed IDS - network divides in clusters, each cluster has its cluster head and cluster nodes and iv) Mobile Agent based IDS where collection and detection are done through agents in cooperative or hierarchical manner[4][5].

The chapter is organized as follows: In Sect.2, we discuss the related work. In Sect. 3, we present linear separable support vector machine. In Sect. 4, experimental setup of our systems is described. In Sect.5, we summarize the conclusion.

2. RELATED WORKS

The use of SVM for the detection of DoS attacks have been discussed in [6]. The performance of the proposed method has been validated experimentally and shown that proposed SVM-based detection approach achieves very high detection accuracy. However, the performance improvement of the network environment with the use of the suggested algorithm has not been analyzed. A proactive detection mechanism is proposed in [7] for Distributed DoS (DDoS) attacks with reducedcomputational complexity. The approach applies detection methodologies on each received packet to filter malicious data packets during the pre-attack phase. In [15]observed that SVM and Decision Tree performed as stand-alone detectors and as hybrids [16]. Two hybrids models were examined, a hierarchical model (DT-SVM), with the DT as the first player to produce node information for the SVM in the second layer, and an ensemble model comprising the stand-alone techniques and the hierarchal hybrid. For the ensemble approach, each technique is given a weight according to detection rate of each particular attack type during training. Thereafter, when the system is tested, only the technique with the largest weight for the respective attack prediction is chosen to output the classification. The approaches were tested on the KDD Cup '99 data set[8].

In [17] proposed an autonomous host-based ID for detecting sinking behavior in an ad hoc network. The proposed IDS uses a cross-layer approach to make best use of detection accuracy. To further maximize the detection accuracy SVM is used for training the detection model. However, SVM is computationally expensive for resource-limited ad hoc network nodes. Hence, the proposed IDS preprocess the training data for reducing the computational overhead incurred by SVM. Number of features in the training data is reduced using predefined association functions. In [18], the review on strategies that are used to improve the classification performance in terms of accuracy of SVMs and perform some experimentation to study the influence of features and hyper-parameters in the optimization process, using kernels function. Huang et al provide a study on the joint optimization of C and g parameters (using the RBF kernel), and feature selection using Grid search and genetic algorithms[6].

In [19] proposed an SVM-based intrusion detection system, which used a hierarchical clustering algorithm, leave one out, and the SVM technique. The hierarchical clustering algorithm provided the SVM with fewer, abstracted, and higher-qualified training instances that are derived from the KDD Cup 1999 training set. It was able to significantly minimize the training time, and improve the performance of SVM. The simple feature selection procedure (leave one out) was applied to eliminate unimportant features from the training set so they obtained SVM model could classify the network traffic data more accurately.

3 TRAIL BASED SUPPORT VECTOR FOR INTRUSION DECTECION MACHANISM (TSVID)

3.1 System Structure

In the case of a Network Intrusion Detection System (NIDS), the source of the data can be the raw frames from the network or information from upper protocol layers such as the IP or UDP. In case of host based system, source of data are the assessment logs maintained by the OS. The Feature Generator module is responsible for extracting a set of selected features from the data acquired by the acquisition module. Features can be classified as low-level and high-level features. A feature can be directly extracted from captured data while some deductions are required to be performed to extract the top features. Considering the example of a network based IDS, the source IP and destination IP of network packets would be the low level features whereas information such as number of failed login attempts would be classified as high level features. Sometimes features are categorized based on the source of data as well [20][21]. The Incident Detector is the core of IDS. This is the module that processes the data generated by the Feature Generator and identifies intrusions. Intrusion detection methodologies are generally classified as misuse detection and anomaly detection. Misuse detection systems have definitions of attacks and they match the input data against those definitions. Upon a successful match, the activity is classified as intrusion. Anomaly detection systems are based on a definition of normal behavior of a system. Any deviations from this normal problem lead to the classification of the corresponding activity as suspicious. Irrespective of the detection methodology, upon detection of an intrusion, an alert is generated and sent to the Response Management module. Traffic model Generator module contains the reference data with which the Incident Detector compares the data acquired by the acquisition modules and processed by the feature generator. The source of data of the Traffic Model Generator could be non-automated (coming from human knowledge) or automated (coming from automated knowledge gathering process). Response upon in receipt of an alert from the incident detector, initiates actions in response to a possible intrusion. A block diagram of the architecture of a Network Intrusion Detection is presented in. The architecture for a Host Based Intrusion Detection System would be similar. The steps are shown in figure 1. The following are the steps to be performed while executing TSVM. At first the training dataset is selected from KDD Cup'99 dataset. The TSVM training is performed for the training data and as a result structures of fields are produced. Then the structures are obtained and the trained data is loaded for testing. The TSVM data classification is performed based on the trained structure using the structured fields. Finally, classified results are obtained that contains the detected attacks for the protocols [22].

3.2TSVID Classification

Let {(*x* , *y* } Where xi represents the input vector and the TSVID regression function is,

$$f(x) = w.x + b \quad (1)$$

Where x Denotes the high-dimensional feature space, w represents the weight vector and b indicates the bias term. The coefficients w and b are calculated accordingly. In accordance with the Karush–Kuhn–Tucker's (KKT) conditions of solving quadratic programming difficulty, the equivalent data points are support vectors, which are engaged in determining the decision function. TSVID built by using Radial Basis Function (RBF) has excellent nonlinear forecasting performance and less free parameters that require determination. TSVID which is an extension of conventional SVM has a set of supervised learning methods used for classification and regression. Non-negative matrix factorization is an Unsupervised Learning method that is being used in TSVID. The Supervised Machine Learning is a method in which the algorithm uses forecaster and intention attribute value in order to discover the predictor and target value relation. Kernelized Iterative Support Vector Machine is a supervised learning technique for creating a decision function with a training dataset.

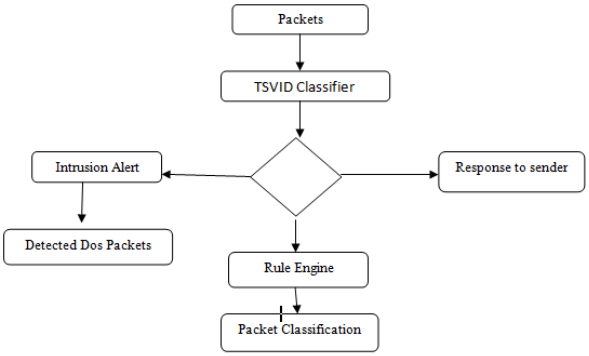

Fig.2TSVID Classification

The training data consist of pairs of predictor and target values. Each predictor value is tagged with a target value. If the algorithm predicts a categorical value for a target attribute, it is called classification function. Class is an example of a categorical variable. Positive and negative can be two values of the categorical variable class. Categorical values do not have partial ordering. If the algorithm can predict a numerical value then it is called regression. Numerical values have partial ordering. TSVID maps linear algorithms into non-linear space. It uses a feature called, kernel function, for this mapping. Kernel functions like polynomial, radial basis function are used to divide the feature space by constructing a hyper plane. The kernel functions used at the time of training the classifiers which selects support vectors alongside the surface of the function. TSVID classifies the data by using these support vectors that outline the hyper plane in the feature space. The two classes are then separated by an optimum hyper plane, illustrated in Figure 4, minimizing the distance between the closest +1 and -1 points, which are known as support vectors. The right hand side of the separating hyper plane represents the +1 class and the left hand side represents the -1 class Then, ÷ The determination of the parameters plays a significant role in the performance of TSVID One of the important features of TSVID is the transformation that are not required to be implemented to decide the separating hyper plane in the probably very elevated dimensional feature space, a kernel depiction can be exploited for influential the separating hyper plane, in which the solution evaluated at the Kernelized support vectors is written as a weighted sum of the values of certain kernel function.

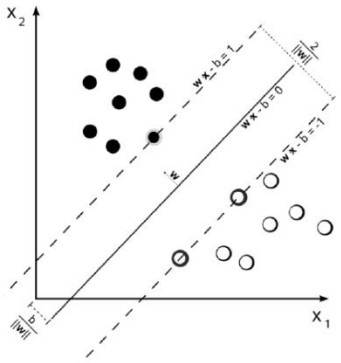

Fig.3 Optimal margin Clarifier

By introducing the kernel, TSVIDs gain flexibility within the selection of the form of the threshold separating solvent from insolvent companies, which wants nonlinear and even need not have an equivalent functional form for all data, since its perform is non-parametric and operates locally. As a consequence, TSVIDs can work with financial ratios, which show a non-monotone relevancy score and to the probability of default, or that are non-linearly dependent and this without having any specific work one very non-monotone variable. Since the kernel perfectly contains a non-linear transformation, no assumptions regarding the functional kind of the transformation makes the data linearly divisible, for its importance. The transformation pertaining to a strong theoretical basis and human experience judgment earlier is not required. TSVIDs offer straight out-of-sample generalization, if the parameters C and r (in the case of a Gaussian kernel) are suitably chosen. This implies that, by selecting an applicable generalization grade, TSVIDs may be robust, once the training sample has some bias. TSVIDs deliver solution, since the optimality problem is turned in. This can be an advantage compared to Neural Networks, that have multiple solutions related to local minima and for this reason might not be robust over totally different samples. With the choice of a suitable kernel, the values of its ratios are compared with those support vectors of the training sample which is then classified according to the group depend on the best similarity.

3.3Reaction Engine

The output of the TSVID is sent from the detection module to the response module for the final decision. The final response is then generated after analyzing the inputs and the necessary actions are taken accordingly. To reach the best conclusion before responding to the output of the Detection module, two important cases need to be accounted; the precision of the detection module and the possible patterns of the future DoS attacks. The precision of the detection module is degraded by the false positive and false negative output of the TSVID. Therefore, decisions based on a single TSVID output are prone to error, so before generating the final response, the performance of the response module needs to be improved. To be able to advance the functionality of the response module by minimizing false positive/negative decisions, a mechanism based on an alert-

threshold is developed and integrated into the system. The alert-threshold is based on the output of the detection module and is the maximum threshold at which the response module would trigger an intrusion alarm. It is initially set to zero, and needs to reach the predefined peak to set out an alarm; e.g. if the alert-threshold is set to three, it takes at least three seconds or more depending on negative alarms—to trigger the alert if any malicious nodes are present in the network. This is also necessary for the alert-threshold to degenerate over time to prevent false alarm in the long run. However, an intruder can plan the attack similar to Gray hole attack and act randomly, attacking for a random amount of time and then pausing the attack [18]. Therefore, the detection module should be designed such that the negative alarms from detection module have lower weight compared to positive alarms.This will invalidate such behaviors to a degree and ensure the gradual degradation in false alert-threshold. Upon reaching the maximum threshold the response module selects the misbehaving node according to the Statistics from the data gathering module, and sends a message to the system and neighbor nodes to remove the attacker from their routing tables. After removing a malicious node from the system, the response module resets the threshold to give the system time to recover before identifying the next possible attacker. The threshold is chosen based on series of experiments with different amounts tofind the most efficient response time.

4. RESULTS AND DISCUSSION

The KDD Cup 1999 Dataset was used for the purpose of this simulation.In 1998 MIT Lincoln Labs had prepared a data set under the DARPA Intrusion Detection Evaluation Program. The Third International Knowledge Discovery and Data Mining Tools Contest, which was held along with the Fifth International Conference on Knowledge Discovery and Data Mining, used a version of the DARPA Intrusion Detection Data Set. The simulation was run with various sizes of the labeled and unlabeled set, where the maximum ratio between the labeled and unlabeled set was maintained to be 1:10. It was observed that the minimum size of labeled training set required for effective Self-Training was around five hundred records. The overall accuracy of detection either did not change or in some cases it got reduced from its original value. This may be explained by considering the fact that in case of limited labeled points in the original case, the decision boundary obtained may not be accurate and upon use of the model on the unlabeled set, the points belonging to the set may be classified incorrectly. This may further lead to a reduction in the overall accuracy of detection. Results obtained for a labeled set of five hundred records with an unlabeled set of five thousand records is presented in figure 4. It can be inferred from the results that Self-Training process as given in flow diagram converges and for the given examples, it converges pretty quickly. The level of enhancement in the detection accuracy with the iterations of the Self-Training algorithm depends on the size of the labeled and unlabeled training set. This result can be inferred from the fact that after 5 iterations, the change in the detection accuracy for the simulation with labeled records set is almost double that of the simulation with labeled records set. This observation is also rearmed by the fact that for very small labeled training sets, there was virtually no positive improvement in the detection accuracy. The results also show that the overall accuracy is most sensitive to the size of the labeled set. In case of the simulation with 30 nodes, the final detection accuracy was around 91% whereas for the simulation with 10 nodes, it was found to be around 96%.

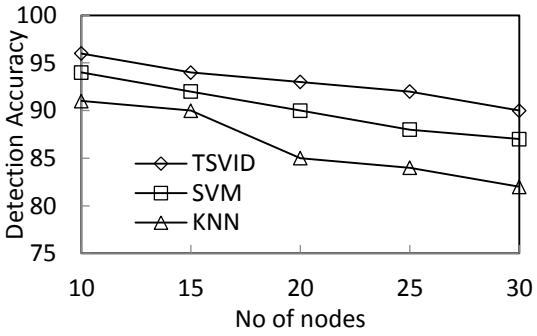

Fig.4 Detection Accuracy

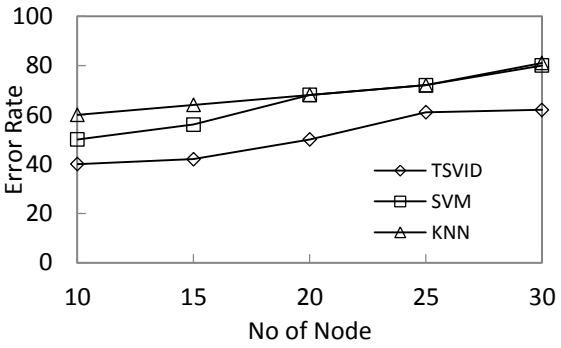

Fig.5 Error Rate

Finally the results validate the error rate shown in figure 5, that Self-Training can be used for reduction of the labeled training set size in the domain of Intrusion Detection as well. Error rate of the model when we use 10 node is 40 where as model with 30 node the error rate is around 50%. A comparison of the performance of Standard SVM, KNN and TSVID as shown in Figure 5.

5. CONCLUSION

Detecting malicious exercises in MANETs is a complex task because of the inherent features of these networks, such as the mobility of the nodes, the lack of a architecture as well as the resource constraints. There is an imperative need to defend these communication networks and to recommendwell-organized mechanisms in order to sense malicious behavior. In this article we offer a evaluation of the effectiveness of different classifiers that can be working as intrusion detection algorithms in MANETs. Consequences show that TSVID may be a good model to utilize when the objective is just to notice an intruder, even if if the objective is to point to which is the particular attack launched then it is improved to use a SVM classifier. The assessment of the classifiers is performed consider that the intrusion detection procedure is totally distributed and each node of the network hosts an self-governing intrusion detection agent.

Reference

[1] Di Pietro, R., Guarino, S., Verde, N. V., & Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks—A survey. Computer Communications, 51, 1–20. doi:10.1016/j.comcom.2014.
06.003

[2] Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. IEEE Communications Surveys & Tutorials, 15(4), 2027–2045.
[3] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, 14(5), 85–91.
[4] Amudhavel, J., Brindha, V., Anantharaj, B., Karthikeyan, P., Bhuvaneswari, B., Vasanthi, M., et al. (2016). A survey on intrusion detection system: State of the art review. Indian Journal of Science and Technology, 9(11), 1–9. doi:10.17485/ijst/2016/ v9i11/89264.
[5] Schweitzer, N., Stulman, A., Shabtai, A., & Margalit, R. D. (2016). Mitigating denial of service attacks in OLSR protocol using fictitious nodes. IEEE Transactions on Mobile Computing, 15(1), 163–172.
[6] Ahmed, M. N., Abdullah, A. H., & Kaiwartya, O. (2016). FSM-F: Finite state machine based framework for denial of service and intrusion detection in MANET. PLoS ONE, 11(6), 0156885. doi:10.1371/journal.pone.015688.
[7] Poongodi, M., & Bose, S. (2015). A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET. Arabian Journal for Science and Engineering, 40(12), 3583–3594. doi:10.1007/s13369-015-1822-7.
[8] Chhabra, M., & Gupta, B. B. (2014). An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET). Research Journal of Applied Sciences, Engineering and Technology, 7(10), 2033–2039.

[9] Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials, 16(1), 266–282.
[10] Kumar, S., & Dutta, K. (2016). Intrusion detection in mobile ad hoc networks: Techniques, systems, and future challenges. Security and Communication Networks, 9(14), 2484–2556. doi:10. 1002/sec.1484.
[11] Akilarasu, G., & Shalinie, S. M. (2016). Wormhole-free routing and DoS attack defense in wireless mesh networks. Wireless Networks. doi:10.1007/s11276-016-1240-0.
[12] Suresh, KC& Prakash, S 2012, 'MAC and Routing Layer Supports for QoS in MANET: A Survey', International Journal of Computer Applications, Vol.60, No.8, December 2012, pp.41-46
[13] Gagandeep, Aashima, Pawan Kumar,"Analysis of DifferentSecurity Attacks in MANETs on Protocol Stack A-Review",International Journal of Engineering and AdvancedTechnology (IJEAT), Vol. 1, Issue 5, June 2012.
[14] KC Suresh, S Prakash, AE Priya, A Kathirvel, Primary path reservation using enhanced slot assignment in TDMA for session admission". The Scientific World Journal **2015**, 1–11 (2015)
[15] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh KantUpadhyay,"Different Types of Attacks on IntegratedMANET" International Journal of Computer Science andSecurity (IJCSS) Vol. 4, Issue 3, Dec 2010.
[16] Li, Y, J Wei.," Guidelines on Selecting Intrusion DetectionMethods in MANET", In the Proceedings of the InformationSystems Education Conference 2004, v 21 (Newport):§3233.
[17] Satria Mandala, Md. Asri Ngadi, A. Hanan Abdullah, "ASurvey on MANET Intrusion Detection", InternationalJournal of Computer Science and Security, Vol. 2, Iss
[18] Christos Xenakis, Christoforos Panos, Ioannis Stavrakakis,"A comparative evaluation of intrusion detection architecturesfor mobile ad hoc networks, Computers & Security", Vol.30, Issue 1, pp. 63-80, January 2011.
[19] Nadeem, A.; Howarth, M.P., "A Survey of MANET IntrusionDetection & Prevention Approaches for Network LayerAttacks," Communications Surveys & Tutorials, IEEE, Vol.15, No. 4, pp. 2027-2045, Fourth Quarter 2013.
[20] Nadeem, Adnan, Michael Howarth,"Protection of MANETsfrom a range of attacks using an intrusion detection andprevention system."Telecommunication Systems 52.4(2013): pp. 2047-2058.
[21] Adnan Nadeem, Michael P. Howarth, An intrusion detection& adaptive response mechanism for MANETs, Ad HocNetworks, Vol. 13, Part B, February 2014, pp. 368-380.
[22] Aikaterini Mitrokotsa, Christos Dimitrakakis, Intrusiondetection in MANET using classification algorithms: Theeffects of cost and model selection, Ad Hoc Networks, Vol.11, Issue 1, January 2013, pp. 226-237.