International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 5: May 2016, pp 1-8. www.aetsjournal.com ISSN (Online) : 2394-6237

Classification Based Intrusion Detection System

R. Sivagami, D. Sathya

Abstract— Intrusion detection system (IDS) is a software application.The key aspect of IDS is to monitor the system activities for malicious activities or policy violations and produces reports to a management station. Supervised learning technique is a machine learning task of inferring a function from labeled training data and it is consisting of input and desired output value. In supervised learning output datasets are provided which are used to train the machine and get the desired outputs. Classification techniques used for supervised learning algorithm is back propagation network, decision tree, support vector machine and Bayesian classification Normal and abnormal sensor data are trained for the testing data to the supervised learning techniques. In the proposed system supervised learning algorithms are evaluated and compared by monitoring their performance of detecting intrusion and attacks.

Keywords— IDS, Supervised learning, Classification techniques

I. INTRODUCTION

In WSN application scenarios security is a very important concern especially in the applications hostile environments and commercial applications. In fact, security in WSN has a great number of challenges than other types of wireless networks. These challenges are due to many reasons like the broadcast nature of wireless communications, limited resources of the sensor nodes, unattended environment where sensor nodes might be susceptible to physical attacks. Security solutions like authentication, cryptography and key management can enhance the security of WSNs. But these solutions alone cannot prevent all possible attacks. IDS which have been successfully implemented in wired networks can detect the misbehavior of participating nodes and notify other nodes in the network to take appropriate countermeasures. However, an IDS scheme designed for wired networks cannot be applied directly to WSNs because of their specific network characteristics such as limited processing power, memory and battery. Especially, in a wireless sensor network IDS is an important security mechanism against both inside and outside attacks and it focuses on detection of misbehavior or malicious nodes. When IDS detects a sensor node misbehaving, it tries to isolate that malicious node from the network. There are three main approaches that IDS can use to classify the attacks: 1) Misuse detection: The behavior of nodes is compared with well-known attack patterns and these patterns must be defined and given to the system. The disadvantage of this technique is needs to build attack patterns and they are not able to detect novel attacks and have to update the database of attack patterns. These drawbacks significantly reduce the efficiency of system management, as the administrator of the network always has to provide IDS agents with an up-to-date database. In now a days, most of the known attacks are only the results of some assumptions from other classic networks. 2) Anomaly detection: This technique does not search for specific attack patterns, but instead of that it checks whether the behavior of the nodes can be considered as normal or anomalous. This technique has to describe the actual features of a normal behavior first, which are established by using automated training. The wrong decisions made by IDS in terms of false positive and false negative alarms affect the accuracy of detection. The disadvantage of this methodology is that an intrusion that does not exhibit anomalous behavior may not be detected, resulting in false negatives. 3) Specification-based detection: This technique combines the aims of misuse and anomaly detection mechanisms, as it is focused on discovering deviations from normal behaviors that are defined neither by machine learning techniques nor by training data. In fact, the specifications that describe what can be considered as normal behavior are defined manually.

R. Sivagami, Dept. of computer science and engineering , Kumaraguru College of Technology, Coimbatore, India

D. Sathya, Dept. of computer science and engineering, Kumaraguru College of Technology, Coimbatore, India

II. IMPLEMENTATION ON CLASSIFICATION TECHNIQUES

Classification of Australian native forest species using hyperspectral remote sensing and machine learning classification algorithm [1] To classify the species the classification algorithm such as support vector machine, adaboost and random forest were applied. This algorithm significantly improves the results produced by LDA. The machine learning classification results were compared with LDA

classification. The supervised machine-learning method, SVM, based on statistical learning theory, was originally developed to solve the binary classification problem. The SVM classification separates the classes with a decision surface. This decision surface, called hyperplane, maximizes the functional margin between classes, while minimizing the training error. For multiclass problems, SVM is to convert the single multiclass problem into multiple binary classification problems. In addition, kernel functions are commonly used to construct a nonlinear hyperplane. AdaBoost determines classification rules from samples by constructing a "strong" classifier through the combination of many "weak" classifiers. RF classification uses an ensemble classification method which consists of a set of decision tree classifiers, and the improved bootstrap method. The input vectors are randomly sampled for each of the tree classifiers independently, and each tree casts a unit vote for the most popular class to classify the input vector. Specifically, for each of Ntrees iterations, a new bootstrap sample from the training set will be selected to build an un-pruned tree onto the bootstrap. At each internal node, mtry predictors are randomly selected, and used to determine the best split. After all of the iteration steps, RF outputs the majority vote from all individually trained trees. At the leaf level Random Forest classification gives 94.75% of accuracy and at the canopy level Support vector Machine gives accuracy about 84.5% of accuracy and at community level its accuracy is about 75.5%.

ADVANTAGE: In classifying the Australian native forest species SVM achieved the best classification accuracy.

DISADVANTAGE: ADABOOST algorithm is slower for large dataset when compared to SVM and Random forest classification algorithm.

Target tracking using machine learning and kalman filter in wireless sensor networks [2] In this paper described the method combines both machine learning with a Kalman filter to estimate instantaneous positions of a moving target. Radiofingerprints of received signal strength indicators (RSSIs) are first collected over the surveillance area. The obtained database is then used with machine learning algorithms to compute a model that estimates the position of the target using only RSSI information. The kernel-based ridge regression and the vector output regularized least squares are used in the learning process. The Kalman filter is used afterward to combine predictions of the target's positions based on acceleration information with the first estimates, leading to more accurate ones. The method allows accurate tracking, and is proved to be robust in the case of noisy data, whether the noise affects the acceleration information or the RSSI measures.

Combining naive bayesian and support vector machine for intrusion detection system [3] In this paper represents two algorithms for developing the intrusion detection system. Naïve Bayesian (NB) and Support Vector Machine (SVM) are combined to maximize the accuracy, which is the advantage of NB and diminish the wrong alarm rate which is the advantage of SVM. In this paper we proposed hybrid model which give higher detection rate and low false positive rate for IDS. In proposed algorithm using naïve Bayesian the prior $P(Cj)$ and conditional $P(Aij|Cj)$ probabilities in the training data D. For each attribute Ai the number of occurrences of each attribute value Aij can be counted to determine $P(Ai)$. Similarly, the conditional probability $P(Aij|Cj)$ for each attribute values Aij can be estimated by counting how often each attribute value occurs in the class in the training data D. Then the algorithm classifies all the examples in ei with some targeted class the training data D with these prior $P(Cj)$ and conditional $P(Aij|Cj)$ probabilities. Then again the algorithm calculates the prior $P(Cj)$ and conditional $P(Aij|Cj)$ probabilities using updated class values in the training data D, and again classifies all the examples of training data using these probabilities. If any of the training examples is misclassified then the algorithm calculates the information gain for each attributes in the training data D. And after the full training providing using naïve Bayesian Classify the data misclassified data and classified data. Classified data will provided to SVM also provided targeted class.

ADVANTAGE: Hybrid algorithm provides 99% of accuracy.

Network State-Based Algorithm Selection for Power Flow Management Using Machine learning [4] In this paper demonstrates that machine learning can be used to create effective *algorithm selectors* that select between power system control algorithms depending on the state of a network, achieving better performance than always using the same algorithm for every state. Also presented is a novel method for creating algorithm selectors that consider two objectives**.** Novel method for creating network statebased algorithm selectors for PFM. Network state as input and provide an algorithm selection as output. Machine learning technique used for classifier training, and pre-processes training data so that the two objectives of minimizing the number of overloads. Machine learning has been shown to be capable of creating effective network state-based algorithm selectors for power flow management. One disadvantage of a machine learning-based approach is the time taken to create selectors. Applying intrusion detection systems to wireless

sensor networks [5] This approach have general guidelines for applying IDS to static sensor networks and a novel technique to optimally watch over the communications of the sensors' neighborhood based on certain scenarios.IDS agent is divided into local and global agent. Local agent monitor the local activities and the information sent and received by the sensor only when the sensor is active and the sensor only manages its own communications. Local agent detects the attacks against the logical and physical safety of sensor nodes and it can also monitors packet which are addressed directly to the node. Global agents watch over the communications of their neighbors, and can also behave as watchdogs and it analyzing the packets to detect whether a certain node is dropping or modifying packets. There are two architectures hierarchical and flat specify how the sensors route the information over the network and group themselves. In hierarchical configuration sensors are grouped into clusters and one of the members of the cluster behaves as server or cluster head. In flat configurations information is routed sensor by sensor and almost all sensors have the same computational capabilities and constraints. Every agent and node must store information about its surroundings in order to work properly. This information can be divided into knowledge about the security and knowledge about the environment. The spontaneous watchdog technique relies on the broadcast nature of sensor communications .The main goal is to activate only one global agent per packet circulating in the network. Accurate fusion of robot, camera and wireless sensors for surveillance application [6] Camera and laser range finder sensors onboard robots and signal strength of mobile device carried by the person can be used to estimate his position. These entire three sources are combined using data fusion to improve performance. The technique is called data fusion algorithm. The object of interest enters into a new camera the transfer of object should have no overlapping field of view. Learning about relationship between cameras automatically is needed. Modeling the color and Movement of object inter camera used to determine the objects have been previously tracked or new one. Robot camera tracking used for person guiding. The algorithm for these is the combination of person detection and tracking which is based on mean shift technique. By combining these algorithms robot employs the face detector when the tracker is lost to recover the track. Signal strength received by the set of static nodes can be used to find the position of mobile object or person carrying one of the nodes. Algorithm to find the node position is particle filtering. When new message received the weight of the different particle is updated based on RSSI. Finally filter can provide 3D position of the mobile node with 1 meter accuracy. One potential solution is to have a central node that implements a centralized extended kalman filter. In that each node has local information and share with other nodes. Decentralized data fusion used for person tracking.
The rule based intrusion detection and prevention model for biometric system [7] The intrusion detection is an essential supplement of traditional security system. This security system needs the robust automated auditing, intelligent reporting mechanism and robust prevention techniques. . This model contains a scheduler to prepare a schedule to check different logs for possible intrusions and detectors to detect normal or abnormal activity. If activity is normal then alarming and reporting has been executed otherwise the rule engine fires the rule to detect intrusion point and type of intrusion. This model also contains expert system to detect source of intrusion and suggest best possible prevention technique and suitable controls for different intrusions. Backward chaining approach chaining approach is used to detect the source. Rule engine of the system is used to define and store the rules. Intrusion detection and Prevention system is divided into 3 sub systems: 1.Intrusion detection 2.Backtracking of intrusion source 3.Prevention techniques. The malicious activity database is stored for future intrusion detection. Expert system evaluates that data with known malicious activity database and detects the source using backward chaining approach. Rulebased programming is one of the most commonly used techniques for developing expert systems. Rule based analysis relies on sets of predefined rules that can be repeatedly applied to a collection of facts and that are provided by an administrator, automatically created by the system or both. The model also contains an expert system to detect source of intrusion and suggests best possible prevention technique and suitable controls for different intrusions. This model also uses security audit as well as alarming and reporting mechanisms. The malicious activity database is stored for future intrusion detection. To detect the source by tracking, backward chaining approach is used. The rules are defined and are stored in the Rule engine of the system. The intelligent model uses AI and expert system is backbone of this system.
Intrusion detection using PCA based modular neural network [8] Modular neural network for intrusion detection, which apply Principal Component Analysis as preprocessing layer for reducing huge information quantity presented in data set. PCA significantly reduce the high dimensionality of data

set without loss of information. Then this preprocess data in the form of principal component is presented to Batch Backpropagation Neural Network for efficient intrusion detection. Neural networks were proposed to identify the typical characteristics of system users and identify statistically significant variations from the user's established behavior. The advantage of neural network in the detection would be the flexibility and capable of analyzing the data from the network, even if the data is incomplete. The network would possess the ability to conduct an analysis with data in a non- linear fashion. Principal component analysis is a mathematical procedure that transforms a number of correlated variables into a number of uncorrelated variables. PCA is multivariate statistical algorithm to reduce the different representation spaces before applying some machine learning algorithms. Modular neural network consist of five components. Data Collector collects data from audit data record. The functions of preprocessors are Arranging Data in Metrics, Calculate Zero Mean, Calculate Covariance, Formulate Covariance Metrics, Calculate Eigen Vector & Eigen value, Calculate principal component. Neural Net based Analyzer, which analyzes the input given by Preprocessor and detects intrusions and attacks. It uses Batch Back Prorogation Algorithm.

On classification approaches for misbehavior detection in wireless sensor networks [9] Learning algorithms subject to evaluation include bio-inspired approaches such as Artificial Immune Systems and classical such as Decision Trees, Bayes classifier, Support Vector Machines, k-Nearest Neighbors. The more simplistic approaches such as Decision Trees or Bayes classifier offer a reasonable performance. Artificial Immune Systems requires two phases namely learning and detection phase. Learning phase is also called as self set. The detection phase uses the set of detectors in order to detect anomaly. Neural Networks generally consist of input layer, one or more hidden layers and an output layer. By using the back propagation algorithm the weights in the neural network are changed. This procedure is repeated until the correct output. Support Vector Machines use supervised learning methods for classification tasks. SVM with particle and evolutionary optimization uses a binary classifier with a hyperplane to separate class members. Decision tree is a method to classy data based on conjunction features. Every tree node corresponds to an input parameter. K-Nearest Neighbor algorithm classifies input vectors based on a majority vote of its neighbours. Chi-square Automatic Interaction Detectors is a decision algorithm using $\chi 2$ attribute relevance test during the tree building process. The test decides whether two variables are dependent or independent. Naive Bayes is a probabilistic classifier based on the Bayes theorem with naive independence assumptions. Advantage: Naive Bayes classifier is that it requires only a small amount of training data to estimate the parameters necessary for classification. Perimeter-intrusion event classification for on-line detection using multiple instance learning solving temporal ambiguities [10] In this paper describes a novel model for training an event detection system based on object tracking. This model is to training as a multiple instance learning problem, which allows us to train the classifier from annotated events despite temporal ambiguities. This technique is to realize a Perimeter Intrusion Detection (PID) algorithm and employ image-based features to distinguish real objects from moving vegetation and other distractions. An earlier developed tracking system is extended with the proposed technique to create an on-line PID-event detection system. In this paper, we have presented a new formulation of a classifierbased tracking system in order to incorporate and learn specific visual objects-of-interest indicated by the security personnel. The Multiple Instance Learning (MIL) formulation has been used to resolve the ambiguity between the actual event starting time and the decision on the object. The formulation to Perimeter Intrusion Detection (PID) and have shown that it can drastically reduce the number of false positives by a factor 2–3 and improve the F1 detection performance from 0.15 to 0.28 for challenging videos. By considering results, it would be interesting to compare this type of object-level processing with context level processing on userdefined vegetation regions. A Survey of Intrusion Detection Schemes in Wireless Sensor Networks [11] Prevention-based security approaches like cryptography, authentication and key management have been used to protect WSNs from different kinds of attacks but these approaches are not enough to protect the network from insider attacks that may extract sensitive information even in the presence of the prevention-based solution. Detectionbased approaches are then proposed to protect WSNs from insider attacks and act as a second line defense after the failure of the prevention-based approaches. Agent based distributed and collaborative IDSs: For each agent, there is a module to detect anomalies, called the "local detection engine". These modules have two Components, namely features which describes a logical event in the network such as the percentage of the route changes of a node's routing table. Modeling algorithm which uses features as an input to the rule based pattern matching algorithm and then specifies whether the incidence is a normal

or not according to the predefined matching criterion. Clustering (Hierarchical) based IDS: Only the CHs are responsible for the global decision making process and the response. The main reason for this is to reduce the energy consumption. They wanted to conserve the energy of the majority of the nodes, by simply assigning them as subordinates under CHs. Statistical methods require too much data processing in order to sift the information that is valuable for statistics. Therefore, they are not applicable to WSNs. Outsider versus insider attacks based on the node that is launching the attack, if it belonging to the network so it is considered as insider attack; otherwise it is considered as outsider attack. Passive versus active attacks based on the impact that results from an attack. Passive attacks just monitor or eavesdrop on the data packets, whereas the active attacks do modify the data streams or reported false alarms to the base station. Mote-class versus laptopclass attacks based on the capability of the attacker in compromising the network. In mote-class attacks, a few nodes with a similar capability to the network nodes are used as attackers, whereas in laptop-class, an attacker uses powerful devices like laptops with higher transmission range, processing power and energy to compromise the network.
On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks [12] In this paper surveys recently proposed works on Intrusion Detection Systems (IDS) in WSNs, and presents a comprehensive classification of various IDS approaches according to their employed detection techniques. The three main categories explored in this paper are anomaly detection, misuse detection, and specification-based detection protocols. In this paper gives a description of security attacks in WSNs and the corresponding IDS protocols to tackle those attacks. In this paper the Misuse Detection Schemes is Watchdog approach. To check whether a node B forwards packets sent by node A, have to activate watchdogs that reside within the intersection of the radio ranges of A and B. The problem with this approach is that not all packets can be overheard by a global agent, due to the randomness of the selection process. Another drawback of the work is that it does not deal with the collision of packets, which is high likely due to the high density of nodes in various wireless sensor networks applications. Anomaly detection scheme are Statistical Model-Based Approach, Clustering Algorithm Based Approach, Centralized Approach, Artificial Immune System, Isolation table, Machine Learning Based Approaches, and Game Theory-Based Approaches. Specification based detection protocols are Decentralized Approach, Pre-defined Watchdog Approach and Hybrid System Approach. Decentralized approach has three phases: (i) data acquisition, where packets are collected in a promiscuous mode in order to filter out the important data before storing it, (ii) rule application, where the rules are applied to the stored data, and (iii) detection phase, where the number of raised failures are compared with the expected amount of occasional failures that defines whether an intrusion has occurred or not. Drawback is that Simulation results show that the mutual guard method has considerable overhead and it fails to protect nodes when the attacker has a shorter communication range than the sensor nodes. In this paper provided a detailed and comprehensive study on IDSs in wireless sensor networks, classifying them according to their underlying mechanisms. Hybrid intrusion detection system that integrates both anomaly and misuse techniques. The specific goal of this method is to detect routing attacks in WSNs. For energy efficiency, they use hierarchical WSNs. In the misuse detection module, the authors use pre-defined rules such as packet interval rule, integrity rule, packet delay rule, and radio transmission range rule. Drawbacks is unfortunately, there is no proper and full explanation of the anomaly detection techniques used in this paper, that is, how to effectively analyze the collected data and how to make decision on the existence of intrusions.
An Automatically Tuning Intrusion Detection System [13] In this paper, an automatically tuning IDS (ATIDS) will automatically tune the detection model on-the-fly according to the feedback provided by the system operator when false predictions are encountered. Experimental results show that the system achieves up to 35% improvement in terms of misclassification cost when compared with a system lacking the tuning feature. If only 10% false predictions are used to tune the model, the system still achieves about 30% improvement. Moreover, when tuning is not delayed too long, the system can achieve about 20% improvement, with only 1.3% of the false predictions used to tune the model. The results of the experiments show that a practical system can be built based on ATIDS: system operators can focus on verification of predictions with low confidence, as only those predictions determined to be false will be used to tune the detection model. Full and Instant Tuning, Partial But Instant Tuning, Delayed Tuning are the tuning techniques used to examine the performance of ATIDS with respect to how soon tuning is performed to avoid situations where tuning may lead to deterioration of performance. This proposed model is to improve a detection model dynamically after the model is deployed when it is exposed to new data. In this approach the detection performance is fed back

into the detection model, and the model is adaptively tuned. This approach is simple yet effective and its experimental results show that the TMC of ATIDS with full and instant tuning drops about 35% from the cost of the MC-SLIPPER system with a fixed detection model. If only 10% false predictions are used to tune the model, the system still achieves about 30% performance improvement. When tuning is delayed by only a short time, the system achieves 20% improvement when only 1.3% false predictions are used to tune the model. Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems [14] In this paper, propose a novel hybrid model that efficiently selects the optimal set of features in order to detect 802.11-specific intrusions. For feature selection uses the information gain ratio measure as a means to compute the relevance of each feature and the kmeans classifier to select the optimal set of MAC layer features that can improve the accuracy of intrusion detection systems while reducing the learning time of their learning algorithm. Experimental results with three types of neural network architectures clearly show that the optimization of a wireless feature set has a significant impact on the efficiency and accuracy of the intrusion detection system. Experimental results were obtained using NeuroSolutions software. Learning time of the classifiers is reduced to 33 percent with the reduced set of features, while the accuracy of detection is improved by 15 percent. Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation [15] In this paper, multiple models are constructed by comprehensively analyzing the multidomain knowledge of field control layers in industrial process automation, with consideration of two aspects: physics and information and then, a novel multimodel-based anomaly intrusion detection system with embedded intelligence and resilient coordination for the field control system in industrial process automation is designed. In the system, anomaly detection based on multimodel and the corresponding intelligent detection algorithms. A classifier based on an intelligent hidden Markov model, is designed to differentiate the actual attacks from faults. Finally, based on a combination simulation platform using optimized performance network engineering tool, the detection accuracy and the real-time performance of the proposed intrusion detection system are analyzed. Experimental results clearly demonstrate that the system has good performance in terms of high precision and good real-time capability. Multimodel-Based Anomaly Detection is mainly achieved by three components 1) CAD (Communication-Based Anomaly Detection) 2) NAD (Node-Based Anomaly Detection) and 3) AAD (Application-Based Anomaly Detection).The realtime performance of this approach is analyzed by detection time and the effects on the real-time performance of control system. This intelligent intrusion detection system can detect the attack from both spatial and temporal aspects.

III. PROPOSED SYSTEM

Intrusion detection system (IDS) is a software application and its key aspect is to monitor the system activities for malicious activities or policy violations and produces reports to a management station. Supervised learning technique is a machine learning task of inferring a function from labeled training data and it is consisting of input and desired output value and output datasets are used to train the machine and get the desired outputs. Classification techniques which are used for supervised learning algorithm is back propagation network, decision tree, support vector machine and Bayesian classification. Normal and abnormal sensor data are trained for the testing data to the supervised learning techniques. In the proposed system supervised learning algorithms are evaluated and compared by monitoring their performance of detecting intrusion. Abnormaldata

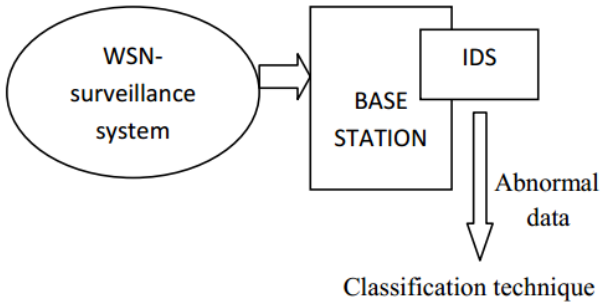


Fig 1.1 Classification based intrusion detection system

CLASSIFICATION TECHNIQUES:

Decision tree: Decision tree learning algorithm is one of the most widely used techniques for classification. The learned classification model is represented as a tree called decision tree. To use the decision tree in testing, traverse the tree top-down according to the attribute values of the given test instance until reaches a leaf node. A decision tree is constructed by partitioning the training data so that the resulting subsets are as pure as possible. The most popular impurity function used for these learning is

information gain and its measure is based on entropy function from information theory.

$$\text{Entropy (D)} = -\sum_{j=1}^{|c|} \Pr(cj) \log_2 \Pr(cj)$$

Where Pr (cj) is the probability of class cj in data set D .

After finding entropy function for the dataset D which is entropy (D) then the entropy function of the attribute in the dataset entropyAi (D).

$$\text{EntropyAi (D)} = \sum_{j=1}^{v} |Dj|/|D| * \text{Entropy (Dj)}$$

The information gain of attribute Ai is computed with

Gain (D, Ai) = Entropy (D) - EntropyAi (D)

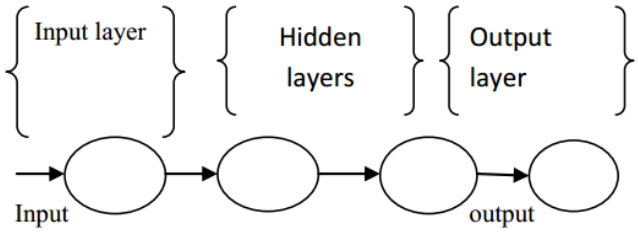
In these proposed system decision tree used to find the attacks in the data and the layer in which the attack is present and the type of attack in that layer. Finally by using the decision tree test data is tested and concluded that it is attacked.

2. SUPPORT VECTOR MACHINE:

Support vector machine is another type of learning system which has many desirable qualities. It performs the classification more accurately than most algorithms in many applications. It finds an optimal solution for finding a separating hyperplane. SVM maximizes the distance between hyperplane and the point close to the decision boundary. Solving SVM is a quadratic programming problem. In general SVM is a linear learning system. To build a classifier it finds the linear function.

$$F(x) = \langle w.x \rangle + b$$

Support vector machine is divided into two types. They are linear SVM and non-linear SVM. Further linear SVM is divided into two categories linearseparable and linear- nonseparable



.

3. Back Propagation Neural Network:

In these proposed system feed forwarded neural network is used. Feed forwarded neural network are arranged in layers. Each unit is linked only in the unit in next layer. No units are linked between the same layer, back to the previous layer or skipping a layer. In these model computations can proceed uniformly from input to the output units. There is no internal state exists. Layer 0 is input nodes. Layers 1 to N-1 are hidden nodes. Layer N is output nodes. All nodes at any layer k are connected to all nodes at layer k+1. There are no cycles between the layers. Input layer Input output

In this system hidden layer gives the result of presence of attacks and layer of attacks presence with the presence of input layer. Output layer gives the output. Output of the output layer is type of attack in that layer.

4. Naïve Bayesian classifier:

Naïve Bayesian classifier is a simple probabilistic classifier based on applying Bayes theorem. It is a classification technique based on Bayes' Theorem with an assumption of independence among predictors. In simple terms, a Naive Bayes classification algorithm assumes that the presence of a particular feature in a class is unrelated to the presence of any other feature. Naive Bayes model is easy to build and particularly useful for very large data sets. Along with simplicity in its classification, Naive Bayes is known to outperform even highly sophisticated classification methods.

$$P(c/x) = p(x/c)\ p(c)\ P(x)$$

Advantage: It is easy and fast to predict class of test data set. It also performs well in multi class prediction. When assumption of independence holds, a Naive Bayes classifier performs better compare to other models like logistic regression and you need less training data. It performs well in case of categorical input variables compared to numerical variables.

Disadvantage: If categorical variable has a category (in test data set), which was not observed in training data set, then model will assign a 0 (zero) probability and will be unable to make a prediction. This is often known as "Zero Frequency". Another limitation of Naive Bayes is the assumption of independent predictors..

IV. CONCLUSION

Intrusion detection is an important method for security protection. In this paper dates' are collected from the surveillance area using sensors. Then that dates' are stored in the base station in which IDS software is implemented. By using classification techniques, layer of attack and the type of attack in that layer is determined and also the accuracy rate is compared with the classification techniques.

REFERENCES

(1) Xiao Shang and Laurie A. Chisholm "Classification of Australian Native Forest Species Using Hyperspectral Remote Sensing and Machine-Learning Classification Algorithms", IEEE

Journal 2013.
(2) Sandy Mahfouz, Farah Mourad-Chehade, Paul Honeine, Joumana Farah, and Hichem Snoussi "Target Tracking Using Machine Learning and Kalman Filter in Wireless Sensor Networks" IEEE SENSORS JOURNAL, VOL. 14, NO. 10, OCTOBER 2014.
(3) Amit D. Sagale, Swati G. Kale "Combining Naive Bayesian and Support Vector Machine for Intrusion Detection System" IJCAT International Journal of Computing and Technology, Volume 1, Issue 3, April 2014.
(4) James E. King, Student Member, IEEE, Samuel C. E. Jupe, and Philip C. Taylor, Senior Member, IEEE "Network State-Based Algorithm Selection for Power Flow Management Using Machine Learning" IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 30, NO. 5, SEPTEMBER 2015.
(5) Maithili Arjunwadkar 1, R.V. Kulkarni 2,"The Rule Based Intrusion Detection and Prevention Model for Biometric System", Journal of Emerging Trends in Computing and Information Sciences[117] April 2014.
(6) Rodrigo Roman, Jianying Zhou, Javier Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks", IEEE Transactions On Parallel and Distributed Systems, vol. 22, no. 9, september 2011.
(7) Khaled Al-Nafjan , Musaed A. Al-Hussein , Abdullah S. Alghamdi, Mohammad Amanul Haque, and Iftikhar Ahmad, "Intrusion Detection Using PCA Based Modular Neural Network", International Journal of Machine Learning and Computing, Vol. 2, No. 5, October 2012.
(8) Matthias Becker, Martin Drozda, Sven Schaust Sebastian, Bohlmann Helena, Szczerbicka, "On Classification Approaches for Misbehavior Detection in Wireless Sensor Networks", Journal of Computers, vol. 4, no. 5.
(9) Andrew Gilbert, John Illingworth and Richard Bowden, "Accurate Fusion of Robot, Camera and Wireless Sensors for Surveillance Applications", IEEE Transactions On Industrial Electronics, vol. 58, no. 3, march 2012.
(10) Julien A. Vijverberg, Roel T.M. Janssen_ Remco de Zwart_ Peter H.N. de, "perimeter-intrusion event classification for on-line detection using multiple instance learning solving temporal ambiguities" 978-1-4799-5751-4/14/$31.00 IEEE 2014.
(11) Murad A. Rassam, M.A. Maarof and Anazida Zainal "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks" American Journal of Applied Sciences 9 (10): 1636-1652, 2012.
(12) Abror Abduvaliyev, Al-Sakib Khan Pathan, Jianying Zhou, Rodrigo Roman and Wai-Choong Wong "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks" IEEE COMMUNICATIONS SURVEYS & TUTORIALS 2013.
(13) Zhenwei Yu, Jeffrey J. P. Tsai, Fellow, IEEE, and Thomas Weigert "An Automatically Tuning Intrusion Detection System" IEEE TRANSACTIONSON SYSTEMS, man, and cybernetics—part b: cybernetics, vol. 37, no. 2, April 2007.
(14) Khalil El-Khatib "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems" IEEE TRANSACTIONS on parallel and distributed systems, VOL. 21, NO. 8, AUGUST 2010.
(15) Chunjie Zhou, Shuang Huang, Naixue Xiong, Senior Member, IEEE, Shuang-Hua Yang, Senior Member, IEEE, Huiyun Li, Yuanqing Qin, and Xuan Li "Design and Analysis of MultimodelBased Anomaly Intrusion Detection Systems in Industrial Process Automation" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 45, NO. 10, OCTOBER 2015.