Ensemble of Ada Booster with SVM Classifier for Anomaly Intrusion Detection in Wireless Ad Hoc Network

K. Murugan¹* and P. Suresh²

¹Department of Computer Science, Government College for Women, Kolar – 563101, Karnataka, India; mkcsresearch@gmail.com
²Department of Computer Science, Salem Sowdeswari College, Salem – 636010, Tamil Nadu, India; sur_bh0071@rediffmail.com

Abstract

Objectives: An ensemble of Ada Booster with SVM (EAB-SVM) classifier technique is proposed for detecting the network intrusions and monitoring the activities of the node as well as classifying it as either normal or anomalous. Methods/Statistical Analysis: The optimal feature selection method is applied in EAB-SVM to select the relevant features to classify and detect the intrusion in wireless ad-hoc network. After that, an ensemble of Ada booster with SVM (EAB-SVM) classifier is used for classifying the intrusion through updating the weight of samples. Finally, the objective function of the EAB-SVM classifier is used to distinguish the anomalous and normal node behavior accurately. This in turn improves the anomaly intrusion detection accuracy. Findings: The EAB-SVM technique comprises of two model namely optimal feature selection model and intrusion detection model. The EAB-SVM technique employed Optimal Feature Selection to choose the features and to reduce the data space dimension. This in turn assists to increase the packet delivery ratio. After selecting the optimal features, the intrusion detection and classification is performed using AdaBoost with SVM classifier for intrusion detection. The AdaBoost with SVM classifier discover the node behaviors as normal or anomalous and thereby achieves reliable packet delivery in wireless ad-hoc network. The performance of EAB-SVM technique is evaluated in terms of packet delivery ratio, classification time, false positive rate and anomaly intrusion detection accuracy and compared with existing two methods. Application/Improvements: The simulation results shows that the EAB-SVM technique achieved the better performance in terms of packet delivery ratio, classification time, false positive rate and anomaly intrusion detection accuracy compared to state-of-the-art methods.

Keywords: Ada Booster, Anomalous Node, Anomaly-Based Intrusion Detection Features, Normal Node, SVM Classifier, Wireless Ad Hoc Network

1. Introduction

A wireless ad-hoc network comprises group of nodes linked with each other through wireless links without centralized communication. This infrastructure less networks are mostly used in the tactical battlefield, emergency search and rescue operations, as well as civilian ad-hoc circumstances like conferences and classrooms. The wireless ad-hoc networks consists of various aspects from a wired network, the intrusion detection is effective when directly applied to a wireless ad-hoc network.

A node within the network communicates to others directly through wireless links to send their information. Each node in the network functioned both as a router and a host. During transmission in ad-hoc network, the network is more vulnerable to various intrusions due to its characteristics such as communication through wireless links, resource constraints, and dynamic topology. Therefore, recent research is to detect and classify the intrusion in the network.

An efficient ensemble method is used to improve the accuracy of intrusion detection. Ensemble methods are
one of the common approaches to improve the accuracy of classifier and predictor. Ensemble learning is a simple, functional and efficient meta-classification approach using a few base classifiers (or learners). An ensemble method consists of boosting and bagging techniques. Boosting is an ensemble method and it has two way approach, where first employs subsets of the original data to generate a series of normally performing models and then “boosts” their performance by combining them collectively using a majority vote. Bagging also stands for Bootstrap Aggregation (Bagg) is the method that reduces the variance of the prediction by creating an additional data for training from original dataset using combination with duplication to produce multi sets of the similar size as original data. Therefore, the boosting technique provides more accuracy than the bagging method but it also more suitable for training data. The most common implementation of Boosting is an Adaboost to attain improved results. Therefore, the Adaboost technique is selected for anomaly intrusion detection in wireless ad-hoc network.

A SVM-based IDS (SVM-IDS) was introduced for identifying the attacks and removing the malicious nodes from the network with high detection rate and minimum time. However, the outputs of SVM were prone to error, therefore before creating a final response, the performance of SVM needs to be improved.

TermID, a distributed rule based network intrusion detection system was introduced in for wireless networks intrusion detection applications. However, the classification was not improved by the distribution of the tasks in wireless networks.

A New intrusion detection system named Adaptive three Acknowledgments (A3ACKs) was introduced to solve three major problems of Watchdog technique such as receiver collision, restricted transmission power and collaborative attacks. However, it provided higher overhead. An Intrusion detection system used intuitionistic fuzzy logic to identify the malicious behavior of node. But efficient packet delivery ratio and intrusion detection was not attained.

Fuzzy logic technique was developed to detect the malicious node behavior through intrusion detection system. However, an optimal feature selection for classification was not performed effectively. Two algorithms namely Intelligent Agent Weighted Distance Outlier Detection algorithm and an Intelligent Agent-based Enhanced Multiclass Support Vector Machine algorithm were designed to detect the intruders. But, the false positive rate was not significantly reduced.

Multiple classifier techniques were presented to distinguish the malicious behaviors in MANETs. However, an intrusion detection agent was not located in the network. A Fuzzy Inference System (FIS) was introduced with the aim of intrusion detection in MANETs but it failed to reduce the false positive rate. A Trust based mechanism was designed for Ad Hoc Network based intrusion detection system (IDS). But the packet delivery ratio was not improved at a required level. The different classification algorithm was introduced to perform intrusion detection but it unable to provide the more effectiveness for classification.

An incremental particle swarm optimization was introduced to develop the performance of Intrusion Detection System (IDS). But it has more time for classifying the intrusion. The EAB-SVM technique improves the intrusion detection accuracy with minimum classification time. A Finite State Machine (FSM) was designed for denial of service and intrusion detection in MANETs. However, it provided the lower intrusion detection percentage. An ensemble method obtains higher intrusion detection accuracy percentage.

An effective Forward Feature Selection (FFS) algorithms and Enhanced Decision Tree Support Vector Machine (EDTSVM) classifier was introduced but it failed to perform effective feature selection and classification. The proposed ensemble method improves the optimal feature selection and classification. A naïve Bayesian classifier was presented for intrusion detection but it failed to design in line intrusion detection system. Therefore, the proposed EAB-SVM classifier technique improves the intrusion detection accuracy.

Conformal Prediction K-Nearest Neighbor (CP-KNN) classifier was designed for classifying the audit data for anomaly detection. However, the data packet delivery ratio of the network was remained unaddressed. This problem is addressed by using proposed EAB-SVM classifier technique. A Supervised Learning In Quest (SLIQ) classifier was introduced for intrusion detection in ad-hoc network. But it failed to use scalable algorithm in ad-hoc network. An Ensemble of Adaboost with SVM classifier uses the scalable algorithm for detecting the intrusion in wireless ad-hoc network.

A new classifier ensemble based IDS was designed using hybrid method which groups the data level and feature level approach. But the classifier failed to classify the node as either normal or anomalous. An ensemble of Adaboost with SVM classifier effectively classifies the
normal or anomalous behavior of node. A new ensemble construction technique\textsuperscript{14} was introduced for improving the intrusion detection accuracy. But it failed to combine the weak classifier into strong classifiers. This problem is addressed in EAB-SVM classifier technique to improve the analog intrusion detection accuracy.

A complicated classification based on different parameters\textsuperscript{19} was introduced to detect the intrusion detection but an ensemble classifier was not used to improve the intrusion detection accuracy. Therefore, the proposed EAB-SVM classifier used to improve the intrusion detection using ensemble of Ada boost with SVM classifier. A combined algorithm based on Partial Least Square (PLS) and feature extraction and Core Vector Machine (CVM) algorithms\textsuperscript{20} was introduced for anomaly intrusion detection. But the detection capability of CVM was not improved at a required level. The EAB-SVM classifier uses Ensemble of Ada boost with SVM classifier for improving the detection accuracy. Therefore, an Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique is more suitable for Anomaly-based intrusion detection in wireless ad-hoc network.

Based on the reviews related with existing methods, the certain issues are addressed such as lack of classification, reduced packet delivery ratio, failed to select optimal feature for classification and higher false positive ratio as well as overhead. In order to overcome such kind of issues in wireless ad-hoc network, Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique is introduced.

The contribution of the proposed work is described as follows,

- To improve anomaly intrusion detection, Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique is introduced
- To select the optimal feature of the node for classifying the intrusion through the feature selection method
- To classify the node either normal or anomalous, ensemble of Ada Booster with SVM classifier through the objective function is designed

The remaining paper is structured as follows. Section 2 describes the Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique for Anomaly Intrusion Detection with neat diagram. In Section 3 the simulation environment is presented and the results are explained in section 4. Section 5 presents a brief introduction of related works. Finally, the concluding remarks are presented in section 6.

2. Ensemble of Ada Booster with SVM Classifier for Anomaly Intrusion Detection

An efficient Ada Booster with SVM classifier is described in order to detect and classify the anomaly intrusion detection in wireless ad-hoc network. In wireless ad-hoc network, the several nodes are distributed over the rectangular area to perform intrusion detection for efficient routing. The transmission in network contains higher packet delivery ratio, minimum classification time and false positive rate as well as higher anomaly intrusion detection accuracy. With this objective, Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique is designed by starting with a system model, followed by which brief descriptions of the proposed scheme are presented.

2.1 System Model

Let us consider a number of nodes ‘$N_1$, $N_2$, …, $N_n$’ deployed over a given rectangular area of ‘$M*N$’ within the transmission range ‘$R$’. The main aim of the Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique is to detect and classify the anomaly intrusion. The source node ‘$SN$’ sends data packets ‘$DP_1$, $DP_2$, …, $DP_n$’ to destination node ‘$DN$’ through intermediate nodes ‘$IN_1$, $IN_2$, …, $IN_n$’. The following problem is considered to show the performance of proposed EAB-SVM classifier technique.

2.2 Problem Definition

The major issue in wireless ad-hoc network is to detect an intrusion Detection System based on anomalous behavior of neighboring nodes. This helps to degrade the network performance. The major problem is separating the normal behaviors’ node and anomalous node to detect the intrusion with aim of improving the intrusion detection accuracy. An anomalous node presents in network to disturb network action. The SVM-based IDS detects the intrusion but it generates the error during the classification. In addition, the conventional distributed rule based network intrusion detection system improved the classification by the distribution of the tasks in wireless networks. But the classification is not improved through the distribution of task. Therefore, an efficient intrusion detection system (IDSs) is needs to improve the performance of wireless ad-hoc network.
2.3 Design of Ensemble of Ada Booster with SVM Classifier

The major novelty of the research work is to improve the anomaly intrusion detection accuracy in wireless ad-hoc network. An EAB-SVM classifier technique comprises two models. The first model selects optimal features to obtain best performance in intrusion detection. The second model is to accurately differentiate the malicious node behavior from normal. An EAB-SVM classifier uses the Ada Booster with SVM classifiers. It efficiently performs the classification task with minimum time based on the optimal features to distinguish the malicious behavior from the normal accurately.

Figure 1 illustrates the architecture diagram of the Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique to improve analog intrusion detection accuracy in wireless ad-hoc network. As described in Figure 1, the main objective of IDS is the analysis of network data, detecting the behavior of the node. For achieving this objective, an ensemble AdaBoost with SVM classifier is proposed in as shown in Figure 1. The EAB-SVM technique consists of two model such as optimal feature selection model and intrusion detection model. Optimal Feature Selection is applied in EAB-SVM to select the features and reduce the data space dimension. This helps to improve the packet delivery ratio. The intrusion detection model is recognized through the learning feature data. Classification algorithm is used for combining AdaBoost with SVM. Initially, the SVM learn the network with selected optimal feature data, and then intrusion detection approach is attained as base classifiers simultaneously to improve the intrusion detection accuracy. But the intrusion detection accuracy of SVM is not improved for minimum sample. Therefore, ensemble of AdaBoost is introduced which continuously optimizes the SVM base classifier, and improve accuracy. The AdaBoost with SVM classifier is to identify the node behaviors either normal or anomalous for reliable packet delivery in wireless ad-hoc network. The brief description about the proposed EAB-SVM classifier technique is explained in below subsection.

2.3.1 Optimal Feature Selection Model

The first model in the design of the EAB-SVM classifier technique is the optimal feature selection model. In general, the optimal feature selection is the method of choosing relevant features for intrusion detection. The feature selection model is used to make easier for classifying the intrusion. The ensemble learning method used for determining a global optimum features about the nodes in wireless ad-hoc network from the number of features related with the network intrusion detection. Followed by, an efficient intrusion detection and classification is carried out to improve the detection accuracy. Optimal Feature selection is often used in network where several features and relatively selects the few features.

Let us consider, the network consist number of nodes $N_1, N_2, \ldots, N_n$ and the network data consists of several features $F_1, F_2, F_3, \ldots, F_n$. In the wireless ad-hoc network environment, each node receives a network data. Among the multiple features, only a small fraction of features represents the intrusion performance. In order to reduce the irrelevant feature, feature selection is essential for improving the intrusion detection. Therefore, the optimal feature selection function is described as follows,

$$F_n(d) = \left(1 - \frac{1}{L_{ch}^n}\right) \cdot \left(1 + \frac{1}{W_n \cdot tf_d \cdot \log\left(\frac{N_d}{N_k^d} + 0.001\right)}\right)$$

From (1), $F_n(d)$ is the function of feature selection, $W_n$ denotes weight factor of the data packet from the dataset d. $tf_d$ is the frequency that appears in dataset. $N_d$ is the number of data packet and $n_k$ is the frequency that containing the specific approach and $L_{ch}$ is the length of the data packet. Therefore, the packets with larger weight are chosen as the training samples.

Algorithm 1 shows the optimal feature selection algorithm shows the process of determining an optimal
accurately described by a separating hyper plane to classify the intrusion as normal or anomalous. Therefore, an ensemble of AdaBoost with SVM classifier is introduced to detect the intrusion in wireless ad hoc network.

As shown in Figure 2, ensemble of AdaBoost with SVM Classifier is introduced to perform efficient classification. Ada-Boost is a typical ensemble method used in the classifier based on SVM. With the use of SVM base classifiers, training of base classifier based on the results of final strong classifier. SVM base classifiers are iteratively trained by using ensemble learning algorithm as AdaBoost. Therefore, the base classifier SVM is given to inputs of Adaboost algorithm to obtain the strong classifier.

Let us consider \( \{(X_1, Y_1), (X_2, Y_2), \ldots (X_n, Y_n)\} \) is a set of training data i.e. contains the group of nodes in wireless ad-hoc network, where \( X_i \) denotes node and \( Y_i \) is target output where \( Y_i \in \{+1, -1\} \). The strong classifier function yields the output \( Y_i = 1 \) is said to be a normal node, and the output \( Y_i = -1 \) is said to be an anomalous node. The base classifier SVM separates the positive and negative labeled samples using marginal hyper plane from both the upper and the lower side of the margin. Initially, weight of the all the samples are calculated to design the SVM classifier. The weight \( (W_t) \) of the all the training sample is initialized as \((1/N)\).

\[
\sum_{i=1}^{N} W_{ti} = \frac{1}{N}
\]  

(2)

The weight values are measured according to the prediction error of base classifier. Therefore, the error rate is measured as,

\[
E_r = \sum_{t=1}^{N} W_{ti} (e)
\]  

(3)

After that, the weight of the SVM classifier based on the error value \( (\beta) \)

![Figure 2. Ensemble of Ada Boost with SVM Classifier.](image-url)
\[
\beta_t = \frac{1}{2} \ln \left( \frac{1 - E_r}{E_r} \right)
\]  
(4)

From (4), \( \beta_t \) represents adjustment coefficient to ensure the final intrusion detection model. Updating the weight of the each sample in order to achieve the maximum iteration and it is expressed as follows,

\[
w_i(t + 1) = w_i(t) \exp \{ -\beta_t Y_i h_t(X_i(t)) \} / N_f
\]  
(5)

From (5), \( w(t+1) \) denotes the new weight of the sample, \( w(t) \) is the initial weight of the sample and \( h_t \) is the prediction label of the \( t \)th component classifier on the sample, \( Y_i \) is target output, \( N_f \) is the normalization factor. Then the updated Weight value is assigned as 1.

\[
\sum_{i=1}^{n} w_i(t + 1) = 1
\]  
(6)

Based on the above measures, the weight function is compared with specified threshold (\( W_{TH} \)). With the help of threshold value, the design of strong classifier classifies the node either normal or anomalous. In order to improve the classification, the Adaboost algorithm with SVM classifier is used as a final classifier output. Therefore the Adaboost algorithm makes the base classifier into strong classifier. The output of the strong classifier is described as,

\[
Y_t = \text{sign} \left( \sum_{t=1}^{T} \beta_t h_t(X_i) \right)
\]  
(7)

From (7), \( Y_t \) denotes the target strong classifier output. Finally, the improved objective function is anomaly intrusion detection is to consider more concentration to False Positive Ratio (FPR). Due to, high FPR makes the reduction of intrusion classification accuracy. Therefore, the objective function of the ensemble Adaboost algorithm with SVM classifier is to adjust the tradeoff between FPR and anomaly intrusion detection accuracy. Therefore, the strong classifier output is used to classify the node based on the objective function (i.e. weight value) with minimum time.

\[
Y_t = \begin{cases} 
+1 & \text{normal sample} \\
-1 & \text{anomalous sample}
\end{cases}
\]  
(8)

From (8), the target strong output classifier provides two objective functions. If the objective function of Ada boost with SVM classifier is labeled as “+1” as normal sample (i.e. node) whereas ‘-1’ labeled as anomalous sample. Therefore, an ensemble of AdaBoost with SVM classifier is used to make base classifiers and generating the accurate intrusion detection approach by updating the weight of samples until the accuracy of detection model achieves intrusion detection. The algorithmic description of the Ensemble of AdaBoost with SVM classifier is shown in below.

**Input**: \( \{(X_1, Y_1), (X_2, Y_2), \ldots (X_n, Y_n)\} \) is a set of training sample i.e. contains the group of nodes in wireless ad-hoc network,

**Output**: improve analog intrusion detection accuracy with minimum time

- **Step 1**: Begin
- **Step 2**: Initialize the weight of training sample \((1/N)\)
- **Step 3**: for each sample
- **Step 4**: Calculate error to obtain optimal weight using (3)
- **Step 5**: Set the weight of the sample after analyzing the error using (4)
- **Step 6**: update the weight value using (5)
- **Step 7**: if \( w > \delta \) then
- **Step 8**: Train a SVM component classifier for detecting the intrusion
- **Step 11**: if strong classifier uses objective function as \( Y_i = +1 \) then
- **Step 12**: The sample as normal
- **Step 13**: else
- **Step 14**: The sample as anomalous
- **Step 15**: End if
- **Step 16**: End if
- **Step 17**: End for
- **Step 18**: End

**Algorithm 2** Ensemble of AdaBoost with SVM classifier algorithm

As shown in Algorithm 2, algorithm of ensemble of Adaboost with SVM classifier is described to detect the node either normal or anomalous intrusion in wireless ad-hoc network with minimum classification time. For each training sample, weight function is measured based on the error value to train the SVM base classifier by weighted sample. If the weighted sample is greater than the threshold value (\( \delta \)), then SVM classifier makes strong through Ada booster technique. Based on the objective function, the strong classifier output results are classifying it as either normal or anomalous node in
3. Simulation Settings

An Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique is simulated using NS2.3 network simulator for improving the anomaly intrusion detection accuracy in wireless ad-hoc network intrusions. For the simulation settings, KDD cup 1999 dataset is considered for detecting the intrusion. This dataset is taken from UCI repository. The KDD cup 1999 dataset employed for the third International Knowledge Discovery and Data Mining Tools Competition, which was held in combination with KDD-1999 Fifth International Conference on Knowledge Discovery and Data Mining. The task to construct a network intrusion detector, a predictive approach is used to distinguish the “bad” connections, which is called as intrusions or attacks, and “good” as normal connections. Based on this separation, the node which is normal or anomalous is detected in a network environment. The optimal features are selected from the dataset are duration, src_bytes, dst_bytes, number of urgent packets, srv_count, diff_srv_count and so on. Based on the above optimal features, the intruder node is distinguished either normal or anomalous.

In Wireless ad hoc network, totally 500 nodes are deployed over a square area of $A^2$ (1500 m * 1500 m) in a random manner that generates traffic for every 20 m/s. The nodes are distributed using Random Way point mobility model, whereas the link layer provides the link between two nodes. A number of data packets are considered from 10 to 100 and forwards the data packets. The simulation time is set as 1500 sec. The simulation parameter used for experimental works is shown in Table 1.

4. Result and Discussion

An Ensemble of Ada Booster with SVM (EAB-SVM) classifier technique is evaluated with the existing SVM-IDS and TermID. The experimental evaluation is carried out with the different parameters such packet delivery ratio, classification time, false positive rate and intrusion detection accuracy. Simulation analysis is carried out with the help of tables and graph values.

| Parameters         | Values         |
|--------------------|----------------|
| Simulators         | NS 2.34       |
| Network area       | 1500 m * 1500 m |
| Number of nodes    | 50, 100, 150, 200, 250, 300, 350, 400, 450, 500 |
| Number of data packets | 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 |
| Size of data packet | 100 – 512 KB  |
| Range of communication | 30m           |
| Speed of node      | 0 – 20 m/s    |
| Simulation time    | 1500 s        |
| Mobility model     | Random Way Point |
| Traffic type       | Constant bit rate |
| Number of runs     | 10            |

4.1 Impact of Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of numbers of data packets are sent by source nodes to the number of packets correctly received at the destination nodes. The formula for packet delivery ratio is mathematically expressed as,

$$PDR = \frac{\text{No. of DP}_R}{\text{No. of DP}_S} \cdot 100$$  (9)

From (9), packet delivery ratio $PDR$ is number of packet received ($DP_R$) to number of packet sent ($DP_S$). It is measured in terms of percentage (%). While the packet delivery ratio is higher, the method is said to be more efficient.

Figure 3 shows the simulation analysis of packet delivery ratio with respect to number of packets being sent. The number of packet is varied from 10 to 100. From the figure, it is clearly evident that while increasing the number of packets, the packet delivery ratio gets increased in all the methods. But comparatively, the EAB-SVM classifier technique improves the packet delivery ratio than the existing methods. This is because; the optimal feature selection is measured for each feature in dataset. Based on the optimal feature selection function, the data packet transmission is performed to improve the delivery ratio. From the feature selection function, the relevant feature with higher weight is selected to perform transmission and identify the intrusion. The multiple features are presented in KDD cup 1999 dataset. Among the multiple features, the optimal features are selected to perform the intrusion detection. In addition, the ensemble of AdaBoost with
SVM classifier is used to classify the node either normal or anomalous through the strong classifier output. This classification method improves the intrusion detection and increases the classification accuracy. Therefore, the packet delivery ratio is significantly improved by 11% and 23% compared to existing SVM-IDS and TermID respectively.

4.2 Impact of Classification Time
Classification time is measured as the amount of time required for classifying the intrusion either normal or anomalous. The classification time is measured in terms of milliseconds (ms). The formula for classification time is measured as follows,

\[ CT = N \times \text{time (classifying normal or anomalous node)} \] (10)

From (10), Classification time (CT) is measured with number of nodes (N) in the network. While the classification time is lower, the method is said to be more efficient.

Figure 4 depicts the impact of classification time versus numbers of nodes is varied from 50 to 500. From the figure, it is clearly shows that while increasing the number of nodes the classification time gets increased in all the method. But, the figure clearly depicts that the proposed EAB-SVM technique provides minimum time for classifying the normal or anomalous node than the existing methods. This is because; an ensemble of Ada boost with SVM classifier is used for efficient classification. The SVM classifier is trained by AdaBoost to make a strong classifier to classify the intrusion. The AdaBoost technique is used for grouping the weak classifiers into a single strong classifier. Therefore, an ensemble of AdaBoost with SVM classifier is introduced to detect the intrusion through the target objective function in wireless ad-hoc network with minimum time. Therefore, the classification time is significantly reduced by 20% and 29% compared to existing SVM-IDS and TermID respectively.

4.3 Impact of False Positive Rate
False positive rate is measured as the ratio of incorrectly classified the node either anomalous or normal using EAB-SVM technique. The false positive rate is measured during the classification.

\[ FPR = \frac{\text{Incorrectly classified node as anomalous}}{\text{No. of nodes}} \times 100 \] (11)

From (11), FPR denotes false positive rate and it is measured in percentage (%). While the false positive rate is lower, the method is said to be more efficient.

Figure 5 illustrates the simulation performance of false positive ratio with respect to number of nodes in wireless ad-hoc network. In order to improve the nodes in network, false positive ratio gets reduced using EAB-SVM technique than the existing methods. The above simulation analysis of the false positive rate is carried out during the classification of intrusion in network. An ensemble classifier uses an objective function to classify the intrusion. This objective function considers the false positive ratio during the classification. Therefore, the proposed ensemble distinguishes the normal and anomalous node behavior based on the optimal feature selection function. Therefore, an objective function of the ensemble Adaboost with SVM classifier in EAB-SVM technique reduces the FPR. The false positive ratio is considerably reduced by 18% and 27% compared to existing SVM-IDS and TermID respectively.

4.4 Impact of Anomaly Intrusion Detection Accuracy
Anomaly intrusion detection accuracy is measured based on the ratio of the number of nodes correctly detected as anomalous to the total number of nodes in network.
From (12), Anomaly intrusion detection accuracy (AIDA) and it is measured in terms of percentage (%). While the anomaly intrusion detection accuracy is higher, the method is said to be more efficient.

Figure 6 shows the performance analysis of anomaly intrusion detection accuracy using EAB-SVM, SVM-IDS and TermID. From the figure, it is clearly evident that the anomaly intrusion detection accuracy is increased using EAB-SVM technique. This development in EAB-SVM technique is attained by optimal feature selection function based intrusion classification in wireless ad-hoc network. The feature selection function is used to select the optimal feature among the multiple features in dataset to identify the intrusion in network. With the help of optimal feature, Ensemble of Adaboost with SVM classifier is used to calculate the weight of the training samples. Based on the weight value, the EAB-SVM is trained to improve the classification. The Adaboost algorithm is used in EAB-SVM as a final target classifier. In addition, the EAB-SVM classifier reduces the false positive ratio. This also helps to improve the anomaly intrusion detection accuracy. The target objective function output distinguishes the normal and anomalous node behavior. As a result, the EAB-SVM technique improves the anomaly intrusion detection accuracy by 9% and 16% compared to existing SVM-IDS and TermID.

5. Conclusion

An effective Anomaly intrusion detection technique called an Ensemble of Ada Booster with SVM (EAB-SVM) classifier is developed in wireless ad-hoc network. The main objective of the EAB-SVM classifier is to improve the anomaly intrusion detection accuracy with minimum classification time. Initially, optimal feature selection is performed in EAB-SVM classifier to choose the optimal features among the multiple features for efficient intrusion detection. After that, ensemble of Ada Booster with SVM classifier is used in an intrusion detection model with the selected optimal features. In SVM base classifier, the weights of the each sample in hyper planes are calculated. Based on weight calculation, the strong classifier Ada Booster is derived. Finally, the objective function is used in strong classifier to classify the node as either normal or anomalous. The simulation is performed with different metrics such as packet delivery ratio, classification time, false positive rate and anomaly intrusion detection accuracy. The performance result shows that the EAB-SVM technique increases the anomaly intrusion detection accuracy with minimum classification time as well as the packet delivery ratio also increased with minimum false positive rate than the state-of-art methods.

6. References

1. Erfan A, Shams, Rizane A. A novel support vector machine based intrusion detection system for mobile ad hoc networks, Wireless Networks. 2017; 1–9.
2. Constantinos K, Vasilis K, Georgios K. TermID: a distributed swarm intelligence-based approach for wireless intrusion detection. International Journal of Information Security. 2016; 1–16.
3. Abdulsalam B, Tarek S, Elhadi S. Implementation of A3ACKs intrusion detection system under various mobility
speeds. Procedia Computer Science. 2014; 32:571–8. Crossref
4. Anusha K, Jayaleshwari N, Kumar AS, Rajyalakshmi GV. An Efficient and Secure Intrusion Detection Method in Mobile Ad-hoc Network using Intuitionistic Fuzzy. International Journal of Engineering and Technology (IJET). 2013 Jul; 5(3):2575–84.
5. Vishnu B, Priya MK, Gokulnath C, Devi GU. Fuzzy Based Intrusion Detection Systems in MANET. Procedia Computer Science. 2015; 50:109–14. Crossref
6. Ganapathy S, Yogesh P, Kannan A. Intelligent agent based intrusion detection system using enhanced multiclass SVM. Hindawi Publishing Corporation. Computational Intelligence and Neuroscience. 2012; 1–10. Crossref PMid:23056036 PMCid:PMC3465880
7. Sergio P, Aikaterini M, Agustin O, Pedro P. Evaluation of classification algorithms for intrusion detection in MANETs. Knowledge-Based Systems. 2012; 36:217–25. Crossref
8. Vydeki D, Bhuvaneswaran RS. Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks. Journal of Computer Science. 2013; 9(4):521–5. Crossref
9. Dharmesh P, Yask P. Intrusion Detection Systems for Trust based Routing in Ad-Hoc Networks. International Journal of Computer Science and Information Technology & Security (IJCSITS). 2012; 2(6):1160–5.
10. Aikaterini M, Christos D. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. Ad Hoc Networks. 2013 Jan; 11(1):226–37. Crossref
11. Chun-Wei T. Incremental particle swarm optimization for intrusion detection. IET Networks. 2013; 2(3):124–30. Crossref
12. Ahmed MN, Hanan AA, Omprakash K. FSM-F: Finite State Machine Based Framework for Denial of Service and Intrusion Detection in MANET. PLoS ONE journal. 2016; 11(4):1–17. Crossref PMid:27285146 PMCid:PMC4902226
13. Visumathi J, Shunmuganathan KL. An Effective ID for MANET Using Forward Feature Selection and Classification Algorithms. Procedia Engineering. 2012; 38:2816–23. Crossref
14. Jaya S, Deepak X. An Improved Naïve Bayes classifier for Intrusion Detection System. International Journal of Innovations & Advancement in Computer Science (IJIAS). 2016 Jun; 5(6):128–34.
15. Lalli M, Palanisamy V. A novel intrusion detection model for Mobile ad-hoc networks using CP-KNN. International Journal of Computer Networks & Communications (IJCNC). 2014 Sep; 6(5):193–201. Crossref
16. Sreenivasulu P, Reddy R. A Scalable Classifier for Intrusion Detection in Ad-hoc Networks. International Journal of Advanced Engineering and Global Technology. 2014 Apr; 2(4):584–8.
17. Salunkhe, Mali SN. Security Enrichment in Intrusion Detection System Using Classifier Ensemble. Journal of Electrical and Computer Engineering. 2017 Mar; 16.
18. Amin AA, Bin MIR. A novel SVM-kNN PSO ensemble method for intrusion detection system. Applied Soft Computing Journal. 2016; 38:360–72. Crossref
19. Maqbool B. A New Classification Scheme for Intrusion Detection Systems. International Journal of Computer Network and Information Security. 2014; 8:56–70. Crossref
20. Gan X, Duanmu J, Wang J, Cong W. Anomaly intrusion detection based on PLS feature extraction and core vector machine. Knowledge-Based Systems. 2013; 40:1–6. Crossref