

Trust Aware Svm Based Ids For Mitigating The Malicious Nodes In Manet

A.R.Rajeswari, K.Kulothungan, S.Ganapathy, A.Kannan

Abstract: MANET is dynamic in nature, openness, infrastureless and no centralized monitoring and controlling unit. Due to these unique characteristic features, MANET is subjected to various security threats caused by the malicious nodes. A system that observes the unwanted attacks caused by the malicious nodes is defined as Intrusion Detection System. The major responsibility of IDS is to detect attacks from the network. In this paper, we propose a Trust Aware SVM based Intrusion Detection System (TASVM-IDS) with an objective to detect and isolate the malicious nodes. The proposed system consists of the following modules, namely feature extraction module, trust estimation module, classification module and decision making model. In this paper, a novel feature extraction algorithm, namely Linear Correlation Coefficient Based Feature Extraction (LCCBFE) algorithm is proposed with an aim to minimize the training time and to enhance the lifetime of the system. The trust level node is estimated by utilizing the behavior analysis and residual energy level of nodes. Thus, we have proposed a new Behavior Analysis Based Trust Algorithm (BABT) algorithm to compute the trust level of nodes in the network. Finally, SVM based classifier is used to classify the nodes into a trustworthy, untrustworthy or malicious node based upon the measured trust level of the nodes. Simulation results proves that the proposed TASVM-IDS can successfully mitigate malicious node and gives better results when compared to SVM and ELM.

Keywords: Intrusion Detection System; Data preprocessing; SVM; ELM; Trust; MANET.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a dynamic and self-composed network comprised of different mobile wireless nodes[1]. The mobile nodes within radio range of each other, can directly communicate whereas the others, seeks the support of the intermediate node to transmit their packets. MANET aims to provide wireless network services without depending on any centralized architecture[2]. In MANET each node behaves as a router, thus nodes exhibit the responsibility of the router by routing packets between neighbors to reach an intended destination. MANETs can be applied to different fields of applications, including battlefield communications, emergency relief scenarios, public meeting, virtual classroom and other security-delicate environments[3]. Despite tremendous applications and numerous advantages security issues in MANET is a key challenging issue due to the openness nature of the network environment. MANET is vulnerable to attacks caused by the malicious node. Thus, research in MANET has been developed since in 1990 on wider areas such as Security, Quality of Service, Routing, IP addressing and Management of MANETs.

Revised Manuscript Received on June 05, 2019

A.R.Rajeswari, Department of Computer Science and Engineering, Sethu Institute of Technology, kariapatti, India

K.Kulothungan, Department of Information Science and Technology, CEG Campus, Anna University, Chennai, India

S.Ganapathy, School of Computing Science and Engineering, VIT University-Chennai Campus, Chennai, India

A.Kannan, Department of Information Science and Technology, CEG Campus, Anna University, Chennai, India

The security issue for MANET has been considered as major challenging issue, thus a significant number of researches have been carried in this area. Key management schemes and authentication techniques are two primary security mechanisms but not supported much in case of enhancing the security concern of MANET and hence IDS based security mechanisms act as the solution to address the security issues faced by MANETs. Dynamic nature of Ad hoc network has a great effect on the secure routing performance evaluation of the network. An IDS is a vital research area with numerous important applications. The main focus in the designing of IDS for MANET is distributed architecture. The malicious nodes affects the network by violating the network policy of MANETs. Thus, mitigating these nodes is a specific challenge for developing IDS in MANETs. MANET faces many security challenges due to the absence of any central monitoring system to monitor the behaviour of the nodes in the network. Thus, many research works are carried out to address the security issues and in turn to enhance the secure routing in MANET. In MANETs, IDS is defined as a system that identifies the attacks caused by the malicious nodes. Thus, IDS has a primary role to detect the attacks. Normally the IDS consist of the following process such as feature extraction and intrusion detection. Devolving an IDS for MANETs are complex and challenging issue due to the lack of limited computational ability of the nodes. Constructing an IDS for MANET holds the following challenges:

- Lack of centralized controlling for the process of monitoring functionality.
- In MANET, each node act as a router that leads as a cause for many routing attacks.

The data collected from the network trace file are considerable enormous in size that act as major issue in developing IDSs to enhance the security level of the network. These huge data brings down the detection procedure and hence cause degradation in the classification accuracy. Classifying data set as such without the process of feature extraction normally includes more computational complexity. The feature extraction is defined as a process of fetching out the necessary and relevant features for the set of available data set source. Thus, it act as primary step during the designing of the IDS to extract the important and required features, those are necessary for identifying the attacks caused by the malicious nodes are extracted from the network trace data set. Therefore, the major objective of this phase is to improve the detection rate and the training time of the system. In general filter and wrapper methods are two common types of methods for feature selection[4]. In case of Filtering method certain factors as information, distance and consistency are taken into consideration for the process of measuring the relation among the features. Moreover in case of wrapper method learning algorithms are employed to extract the features. Therefore, the wrapper methods are

expensive in terms of computational cost when compared to the filter method particularly when the data set are huge in size. The classification phase is the next step after feature selection process and the extracted features are given as input to the classifier training phase and the testing phase will classify a test instance as normal or attacks. The classification techniques can be classified as one class and multi-class classification techniques. Due to the self-organised and distributed nature, nodes in MANET can act as the major source of malicious nodes. Thus, trusting such type of nodes during routing and other network functions may lead to several drawbacks such as vulnerabilities to attacks and degradation in the network performance. Therefore a novel trust management system is necessary to estimate the trust relationship between one node to another node and to enhance the security standard of the network. The trust is termed as the measure of belief about the behaviour of a node. Trust Management system can be employed to improve network security and to improve the network lifetime. Sensing and event monitoring are considered as two major deployment goals of MANET. Thus, in order to achieve the goals trustworthy collaborations and genuine information sharing among the nodes are measured as mandatory criteria. Moreover MANETs is uncontrollable in nature due to the absence of centralized controlling unit to control the nodes behaviour. Therefore, the probability of attacks caused by malicious and selfish nodes are more. Thus, the estimation of trust of nodes acts as a vital source for the security issues of MANETs.

However, the trust estimation process is considered as challenging issue in MANET due to the following reasons:

1. The nodes are dynamic in nature and hence therefore it becomes difficult task to estimate the trust level between one node by another node.
2. Due to the absence of any centralized controlling unit it becomes difficult to absence the behaviour of nodes. Thus the complexity during the trust estimation process increases non-linearly in the absence of centralized controlling unit. Moreover, the worst case complexity for trust estimation is $O(N^2)$ [5] for a network with N nodes. Thus, to address the security issues in MANET, in this work we have proposed a new intrusion detection system based on trust mechanism. The proposed system consists of the five modules. The first module act as gathering module to collect the network data. The second module is responsible for the feature extraction process. Moreover, a novel algorithm Linear Correlation Coefficient Based Feature Extraction (LCCBFE) algorithm for enhancing the feature extraction process is proposed. The third module is responsible for trust computation process. Moreover, a new algorithm Behavior Analysis Based Trust Algorithm (BABT) algorithm is proposed for the purpose of trust computation process. Moreover, by using the fourth module that utilize the Support Vector Machine (SVM) based Classifier malicious nodes are identified. The final module is the decision module that deals about decision regarding the classified nodes in the network.

The remainder of this paper is organized as follows section 2 describes the related works existing in IDS for MANET.

Section 3 presents the system architecture and functionality of the proposed work. Section 4, discuss on the simulation results and finally, we concluded the paper in section 5.

II. RELATED WORKS

A numerous amount of research has been proposed and carried on to build an Intrusion Detection System (IDS) for MANET, with an aim to enhance the security level. Anderson in 1980's was the first researcher to handle the research area related to IDS[6]. A survey of MANET intrusion detection and prevention approaches for network attacks was published[7]. A novel framework was developed for vulnerability analysis in wireless ad hoc networks by using the probabilistic model[8]. A decision tree based SVM algorithm was used to build multiclass IDS that integrates SVM and decision tree. The primary goal of this classifier is to solve the multiclass problem. Moreover, the classifier improved the training time, testing time, accuracy of IDS and high detection accuracy[9]. An IDS based on information theory and statistical methods for feature selection and SVM based classification techniques for classification has been proposed and the performance of the algorithm is compared to a mutual information based feature selection method. The experimental results show high accuracy in detecting the attacks such as R2L & U2R attacks[10]. An improved multi-class SVM based on binary tree structure was developed for effective classification process[11]. The feature selection process can be used to provide better accuracy for detecting the DoS attacks[12]. A powerful and useful survey has been reviewed that narrates about application of data mining techniques for cyber security field. Anomaly detection techniques could be used to detect unusual pattern and behavior [13]. An IDS model to analyze the data set was proposed and unsupervised clustering algorithm was developed to mitigate the known and unknown attacks[14]. A Feature selection algorithm was developed based on the wrapper approach using neural network[15]. A constructive approach involving correlation information in selecting features and determining NN was used in developing this algorithm. Thus, it reduces the redundancy information caused due to the compact NN architecture. Four different approaches have been developed for the process of attribute normalization to pre-processes the data for anomaly IDS[16]. The evaluation results of these approaches show that the process of attribute normalization will improve the detection performance of the IDS. The enhanced v-FSVM has been reformulated to analyze the performance of the proposed work it has been subjected to IDS[17]. The importance of supervised classification algorithms in intrusion detection was examined and analyzed[18]. A hierarchical architecture of generalized intrusion detection and prevention system was developed by using the concept of clustering mechanism[19]. An intrusion detection system was developed by using the concept of trust and agent scheme[20]. An optimal solution was developed for security problems in MANET by employing the user authentication and intrusion detection system. A powerful survey [21] that discusses about various intelligent techniques for feature selection and classification for intrusion detection in MANET. An ID consists of two process namely pre-



processing and intrusion detection stages. An intrusion detection scheme was developed by using the ELM classifier[22]. An Intrusion Detection system has been proposed using the ELM based single classifier hidden layer feed forward neural network[23]. An Active Rule Approach was developed for Network Intrusion Detection with Enhanced C4.5 Algorithm[24]. A novel feature selection algorithm based on the rule based approach has been proposed by extending the Multiclass Support Vector Machine (MSVM) algorithm. The main advantages with this work are improved detection rate and reduced false alarm rate when compared to the existing work. A simplified decision table was employed in the process of feature reduction. The experimental results proved about the correctness and effectiveness of their feature selection scheme[25]. Recently a number of search work has been proposed on various trust management techniques for MANET[26]. Trust factor can be utilized as a major design factor during the development of IDS for MANET. Moreover, IDS enables the process of isolating the malicious node from the network by means of estimating the trust value of one node by another nodes. TRUNCMAN, has been developed with an aim to form a trust based routing mechanism to remove the non-cooperative nodes in the path discovery process[27]. Hierarchical trust management protocol has been developed by employing the probability model with primary goal to enhance secure routing by isolating malicious node[28]. A leader follower cluster based direct trust estimation algorithm was proposed to support the context-aware trust model. In this algorithm, the similarity metrics is used for selecting the recommendation from the neighbors. A dynamic trust prediction model has been proposed to estimate the trust of node.

III. SYSTEM ARCHITECTURE OF THE PROPOSED WORK

The system architecture of the proposed Trust Aware SVM based IDS (TASVM –IDS) is shown in Figures .1 The proposed work consist following modules such as Network Trace Data, Data Gathering Module, Data Pre-Processing Module, Trust Computation Module, SVM based Classifier Module and Decision Making Module. In a MANET environment each node acts as a router. Thus, in this paper,

we have utilized data set collected from the network trace as a dataset source. The data gathering module collects the necessary data from the network trace data set. The data pre-processing module is responsible reducing the features. The main role of trust computation module is to compute the trust of the node based upon the behavior analysis in term of the following metrics namely Packet Delivery Ratio (PDR), Packet Modification Ratio (PMR) and Packet False injection ratio (PFIR), Packet Altering Ratio (PAR) and Residual Energy Level(REL) of the nodes. The SVM based classifier module is responsible for classifying the node as trustworthy, medium trustworthy and malicious node (or) untrustworthy node. Finally, the major responsibility of decision making module is to keep track of the proposed system and to assign the penalty in terms of blocking of the malicious nodes either permanently or temporarily. In the forthcoming subsections detailed discussion about the modules in the proposed system is explained.

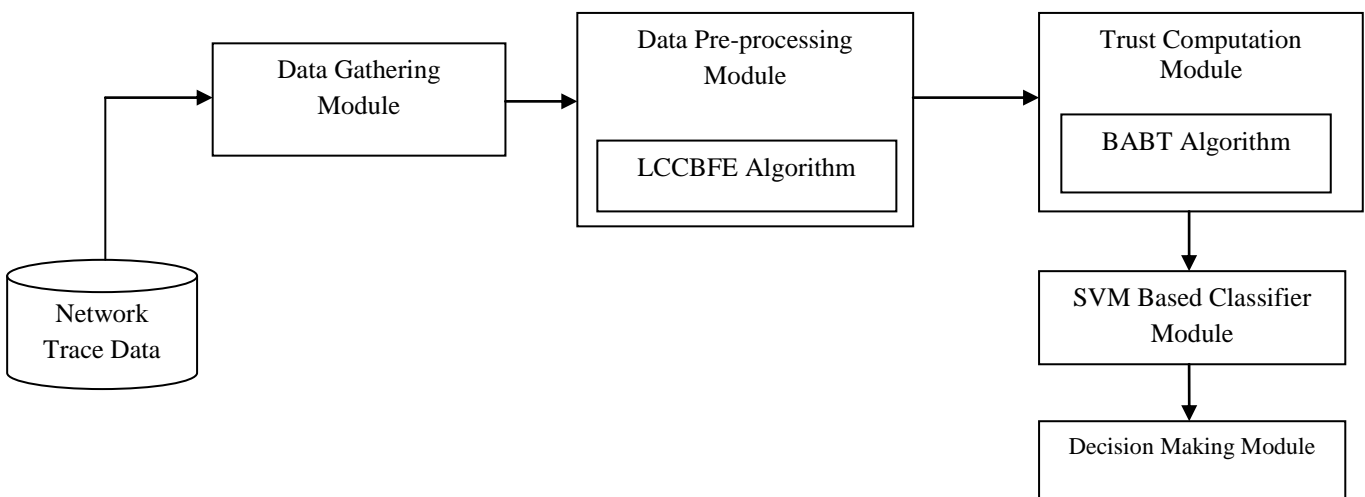


Figure 1 Architecture of Trust aware SVM based IDS (TASVM –IDS)

3.1 Data Set

The experiments are carried out by utilizing the data set collected from the network trace data. The features are classified into two groups, namely mobility based and packet based features. Features relevant to the mobility of the node are described in the mobility based features set. Information about the routing information such as Route_Request, Route_Reply and Route_Error are shown in the packet based feature set. The dataset fetched from a medium mobility traffic node is utilized to train the proposed work. The features are gathered from each node in MANET environment. Table 1 illustrate about the list of 47 features collected from the network trace data set.

Table 1 List of Features Collected from the trace data set

| S. No | Feature Name |
|-------|----------------------------|
| 1 | neighbors |
| 2 | added neighbors |
| 3 | removed neighbors |
| 4 | active path |
| 5 | repaired path |
| 6 | invalidated path |
| 7 | added routes disc |
| 8 | added routes notice |
| 9 | updated path |
| 10 | added routes repaired |
| 11 | invalid routes timeout |
| 12 | invalid routes other |
| 13 | recvr rreq |
| 14 | recvf rreq |
| 15 | send rreq |
| 16 | frw rreq |
| 17 | recv rrep |
| 18 | recvf rrep |
| 19 | send rrep |
| 20 | frw rrep |
| 21 | recvB rerrPs |
| 22 | send rerr |
| 23 | recv aadv |
| 24 | recvf aadv |
| 25 | send aadv |
| 26 | frw aadv |
| 27 | recvf data |
| 28 | send data |
| 29 | avg_num_hops |
| 30 | num_routes |
| 31 | num_req_initd |
| 32 | num_req_receivd |
| 33 | num_req_receivd_as Dest |
| 34 | num_rep_initd_as Dest |
| 35 | num_rep_initd_as Intermede |

| | |
|----|------------------------|
| 36 | num_rep_fwrd |
| 37 | Num_rep_receivd |
| 38 | Num_rep_receivd_as Src |
| 39 | num_err_initd |
| 40 | num_err_fwrd |
| 41 | num_err_receivd |
| 42 | num_dataPks_Initd |
| 43 | num_dataPks_fwrd |
| 44 | num_dataPks_receivd |
| 45 | num_brknLinks |
| 46 | consumed_battery |
| 47 | dropped_datapkts |

3.2 Data Gathering Module

The data gathering module is responsible for collecting the necessary information for the proposed system. The nodes in the network are monitored for a specific period of time and data are collected. The features are gathered based upon the following categories such as mobility based features and packet based features. Thus the gathered features may act as a signature to identify a specific attack caused by the malicious node such as to identify the sleep deprivation attack caused by the malicious node the unusual drop in the consumed power by a node may act as a sign. Data collected by this module is passed as input to pre-processing module of the proposed system.

3.3 Data Pre-Processing Module

The data pre-processing module is an important and necessary module in constructing an IDS for MANET, because in this modules features that are relevant to the system are extracted and unwanted features are eliminated. The main aim of this module is to extract the subset of features that act as an input in developing the system with better performance and enhanced accuracy. Through the features extraction process the redundant and incomplete data are removed from the dataset. In this paper, a novel Linear Correlation Coefficient Based Feature Extraction (LCCBFE) algorithm with the primary objective of the feature extraction is to reduce the number of features and in turn the classification time is also reduced. The Main flow of the algorithm is shown in Algorithm 1.

Linear Correlation Coefficient (LCC) is the popular dependency measure that is employed in evaluating the relationship between two random variables. The main features about LCC are very fast and accurate. By using LCC it is possible to estimate between random linear dependent variables in a fast and accurate manner. The correlation coefficient with respect to x and y can be measured by the following equation (1).



$$Corr(x; y) = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \sum_{i=1}^n (y_i - \bar{y})^2}}$$

(1)

The value of corr(X;Y) lies in the interval of [-1,1] . Depending on the value of corr(X;Y) the relationship between the two random variables X and Y can be classified. The relationship between x and y is defined to be a strong relationship if the value falls either to -1 or 1, else if the value lies close to 0 indicates that the relationship between X and Y is weak. The primary aim of the proposed LCCBFE algorithm is to select features those are required to identify the malicious nodes and to discard the unwanted and redundant features. The LCCBFE algorithm has extracted totally 19 features as shown in the Table 1. The equation 2 shows the feature selection equation.

$$F_{corr} = \text{Max}(corr(class; fs)) - \frac{1}{|FS|} \sum_{fs \in EFS} \frac{corr(fs;f)}{corr(Class;fs)} \quad (2)$$

where F_{corr} is Feature correlation
fs is Feature Set,
EFS is Extracted Feature Subset

The Following are the properties of the F_{corr} :

Step 1: If $F_{corr} = 0$, indicates that the candidate features $fs_i \in fs$ is unwanted (or) irreverent the class CL. Thus, the fs_i is discarded.

Step 2: If $F_{corr} < 0$, indicates that the calculated features is redundant to the class CL. thus the feature fs_i is discarded.

Step 3: If $F_{corr} > 0$, indicated that the candidate feature is relevant and provides information about the output class CL. Hence, the feature fs_i is added into the EFS.

Algorithm 1: LCCBFE Algorithm

Input: Feature Set(fs)= { fs_i } $i = 1..n$ // n number of features

Output: Extracted Feature Set EFS

Step 1: Initialize EFS to 0

Step 2: Measure F_{corr} using the equation 2

Step 3: if ($F_{corr} > 0$) then

EFS = EFS U {FSi}

End if

Step 4: Return EFS.

Table 2 List of 19 selected features

| S.No | Name of the selected features |
|------|--|
| 1. | Average number hops |
| 2. | Numnber of routes |
| 3. | Number of request initiated |
| 4. | Number of request receivd |
| 5. | Number of request as destination |
| 6. | Number of reply initiated as Destination |
| 7. | Number of reply initiated as Intermdiate |
| 8. | Number of reply forward |
| 9. | Number of reply received |
| 10. | Number of reply received as Source |
| 11. | Number of error initiated |
| 12. | Number of error forwarded |
| 13. | Number of error received |
| 14. | Number of data packets initiated |
| 15. | Number of data packets forward |
| 16. | Number of data packets received |
| 17. | Number of broken links |
| 18. | Consumed energy level |
| 19. | Number of dropped packets. |

3.4 Trust Computation Module

In this module, the trust value of a node is estimated based upon the behavior analysis and REL of nodes. For instance, a node say ‘A’ estimates the trust value of another node ‘B’ based on the behaviour analysis of a node A on node B as well as REL of B. In this work, we have utilized the following parameters as a trust factor to measure the trust of a node and to detect the malicious node from the network. Moreover, a novel Behavior Analysis Based Trust Algorithm (BABT) algorithm is proposed with the primary objective to compute the trust of the node. The trust factors are as follows:

1. Packet Dropping Ratio (PDR): PDR measures



the percentage of packet dropped.

$$PDR = \frac{\text{Number of packets transmitted by the node}}{\text{Number of packets received by the node}} \quad (3)$$

2. Packet Misrouting Ratio (PMR): PMR measures percentage of packets misrouted.

$$PMR = \frac{\text{Number of packets misrouted by the node}}{\text{Total Number of incoming packets}} \quad (4)$$

3. Packet Falsely Injected Ratio (PFIR): PFIR measures percentage of packets falsely injected.

$$PFIR = \frac{\text{Number of packets Falsely injected by the node}}{\text{Total Number of incoming packets}} \quad (5)$$

4. Packet Altering Ratio (PAR): PAR measures percentage of packets altered.

$$PAR = \frac{\text{Number of packets Altered by the node}}{\text{Total Number of incoming packets}} \quad (6)$$

Table3 Illustrate about the maximum and minimum value for each of the trust factors

| Trust Factor | Minimum Value | Maximum Value |
|--------------|---|---|
| PDR | $d_{min} = \sum_{i=1}^n \frac{(PDR_i)}{n}$ | $d_{max} = \sum_{i=1}^n \frac{(PDR_i)}{n}$ |
| PMR | $m_{min} = \sum_{i=1}^n \frac{(PMR_i)}{n}$ | $m_{max} = \sum_{i=1}^n \frac{(PMR_i)}{n}$ |
| PFIR | $f_{min} = \sum_{i=1}^n \frac{(PFIR_i)}{n}$ | $f_{max} = \sum_{i=1}^n \frac{(PFIR_i)}{n}$ |
| PAR | $a_{min} = \sum_{i=1}^n \frac{(PAR_i)}{n}$ | $a_{max} = \sum_{i=1}^n \frac{(PAR_i)}{n}$ |

3.4.1 Residual Energy Level

The energy of a node is measured by using the following Equation (7) and (8).

$$REL = \frac{E_{curr}}{E_{initial}} \quad (7)$$

where REL represented as the ratio of currently available energy of a node to its initial energy.

$$E_{Threshold} = \frac{\sum_{i=1}^n REL(n)}{n} \quad (8)$$

where $E_{Threshold}$ is the threshold energy level.

n represents number of nodes in the network.

Algorithm 2 Behaviour Analysis Based Trust Algorithm (BABT)

Input: Set of nodes n

Output: Set of trustworthy nodes

For each $i \in N$

Step 1: calculate the PDR by using the equation (3)

Step 2: calculate the PMR by using the equation (4)

Step 3: calculate the PFIR by using the equation (5)

Step 4: calculate the PAR by using the equation (6).

Step 5: calculate the REL and $E_{Threshold}$ by using the equation (7) and (8).

Step 6: if ($PDR < d_{min}$) and ($PMR < m_{min}$) and ($PFIR < f_{min}$) and ($PAR < a_{min}$) and ($REL < E_{Threshold}$) then

Node i is labelled as highly trusted node

Else

Step 6: if ($d_{min} \leq PDR \leq d_{max}$) and ($m_{min} \leq PMR \leq m_{max}$) and ($f_{min} \leq PFIR \leq f_{max}$) and ($a_{min} \leq PAR \leq a_{max}$) and ($E_{Threshold} > REL < E_{Threshold}$) then

Node i is labelled as medium trusted node

Else

Step 7: if ($PDR > d_{max}$) and ($PMR > m_{max}$) and ($PFIR > f_{max}$) and ($PAR > a_{max}$) and

($REL > E_{Threshold}$) then

Node is labelled as malicious node

Node i is isolated from the network

End if

End if



End if

End for

3.5 CLASSIFICATION MODULE

SVM based classifier is used as classifier in this proposed work to classify the nodes as a normal or malicious node. The malicious node may act as a source for many attacks. In this proposed work by employing the trust factor and REL of a node following attack such as DoS and sleep deprivation attack are mitigated from the network. Initially, the SVM is trained with extracted set of features along with the trust factors namely PDR,PMR,PFIR,PAR and REL of a node. In the testing phase, the nodes are classified based upon trust factors and REL. The attacks are classified as DoS or Sleep Deprivation attack with respect to trust factors. The following equation (8) is used for classification.

$$DIFF = (\sum_{i=1}^n |X_i - Y_i|^p) \tag{8}$$

where X_i and Y_i indicates the feature sets of node X and Y.

Diff represents the difference in value between nodes of classes. The nodes are classified as either trustworthy or malicious node.

3.6 DECISION MAKING MODULE

In this module, the decision authority frames the decision regarding whether to give penalty to a node or node depending upon the estimated trust value. The decision making table that describes about the node status is shown in Table 4.

Table 4 Decision Table about the node status

| S. No | Node Status | Penalty |
|-------|-------------|------------|
| 1 | Trustworthy | No Penalty |

| | | |
|---|-----------------------------------|---------|
| 2 | Middle Trustworthy | Block |
| 3 | UnTrustworthy (or) Malicious Node | Isolate |

For temporarily blocking penalty, the nodes are included to the block list, then the behaviour of the blocked node is analyzed if it is satisfactory then, the blocked node is added into the network's functionality else it is isolated from the network.

IV. SIMULATION AND RESULTS

The proposed work has been evaluated using NS2. For experiments, 100 nodes are deployed over an area of (500x500) m² and the initial energy for each node is assumed as 1J. The Simulation parameters are shown in the table 5.

Table 5 Simulation Parameters

| Parameter | Value |
|------------------|------------------------|
| Network area | 500X500 m ² |
| Number of nodes | 100 |
| Mobility Pattern | Random waypoint |
| Speed | 0-10m/s |
| Simulation time | 1000s |

In Figure 2, the detection accuracy rate of the TASVM –IDS with and without LCCBFE, the feature extraction algorithm is presented. The detection accuracy rate of the proposed work with LCCBFE algorithm ranges from 90% to 96%, whereas the detection accuracy rate in the absence of the LCCBFE algorithm falls between 88 % and 94%. Thus, it is clear that TASVM –IDS with feature extraction shows better performance in terms of detecting the malicious nodes more accurately when compared to the TASVM –IDS without feature extraction. This is due to the fact, that in our proposed work the features required for detecting the malicious nodes are extracted by the LCCBFE algorithm. This results in better detection accuracy rate of the proposed system with feature extraction algorithm than without the algorithm.

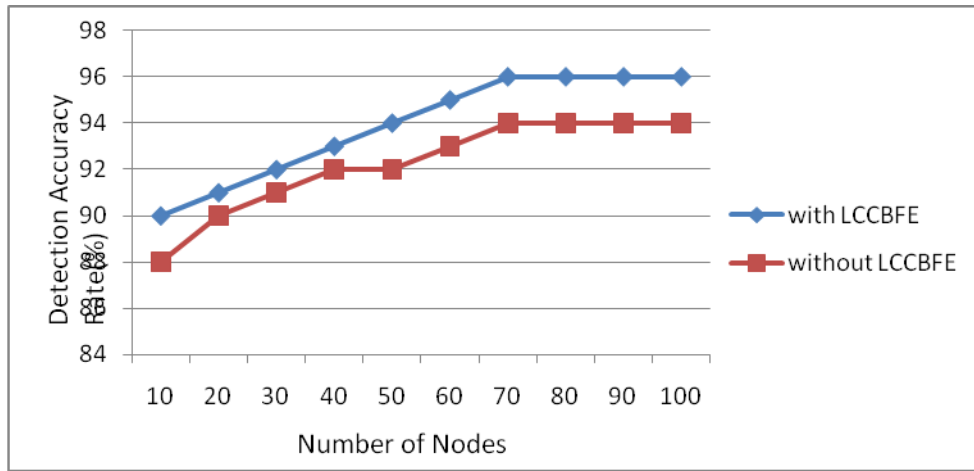


Figure 2 Detection Accuracy

In Figure 3 the comparison of the classification rate of the TASVM –IDS with and without LCCBFE is shown. From the results it is observed that the classification rate of the proposed work TASVM –IDS with LCCBFE ranges from 8% to 2%, on the other hand without the LCCBFE is in the

range from 9% to 3%. So it is clear that the classification rate of the TASVM –IDS system with LCCBFE was low when compared to the TASVM –IDS without LCCBFE as compared to the system without the feature extraction.

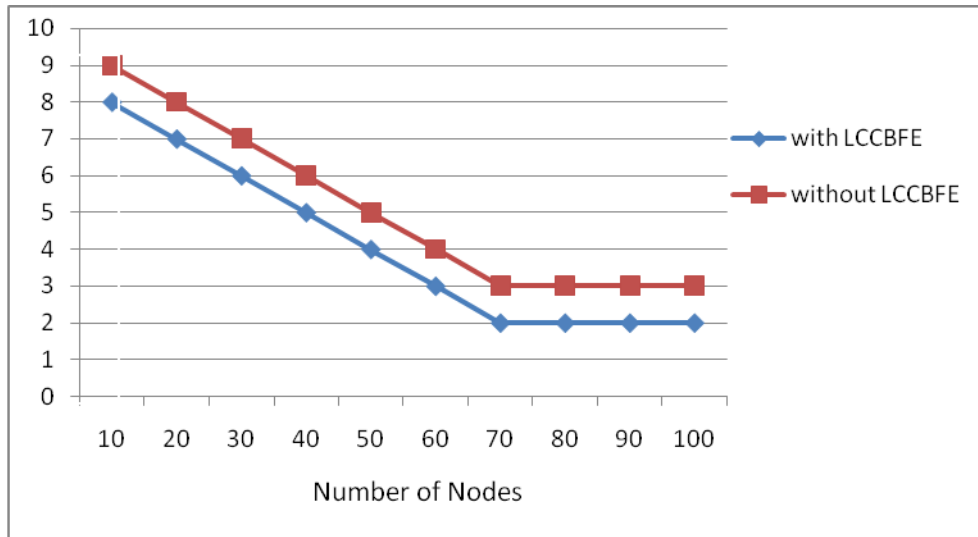


Figure 3 Misclassification Rate

Figure 4 depicts the detection time of the system in comparison with and without feature extraction. From the results it is observed that it takes 0.1 to 1.4 sec to detect the malicious node from the system with feature extraction, whereas the system without feature extraction needs 0.2 to 2

secs. Thus the proposed system takes less time with feature extraction when compared to the system without the feature extraction. This is because in the proposed work, the features are reduced by utilizing the LCCBFE algorithm which in turn will enhance the detection time of the system.

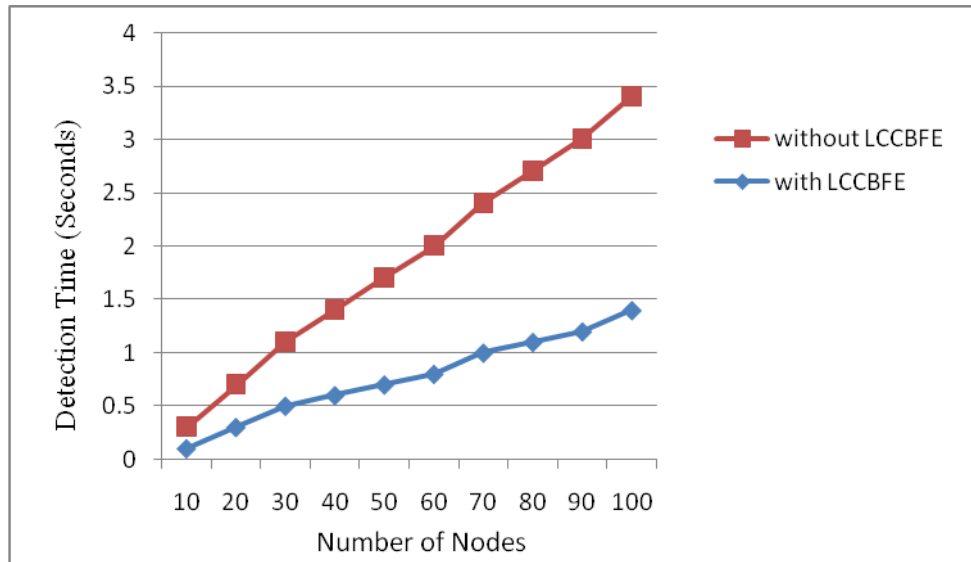


Figure 4 Detection Time

In Figure 5, the detection accuracy rate of the proposed system with respect to the trust level is shown. From the results, it is observed that system with trust shows the detection accuracy rate between 92% and 98.5% where as for the system without trust the detection accuracy rate ranges from 91% to 97.5%. Thus it is clearly proven from

the figure the proposed system with BABT, trust estimation algorithm detects the malicious node better when compared to the system without trust. The reason is that in our proposed work the trust level of the nodes are estimated by using both the behaviour analysis and REL of the nodes.

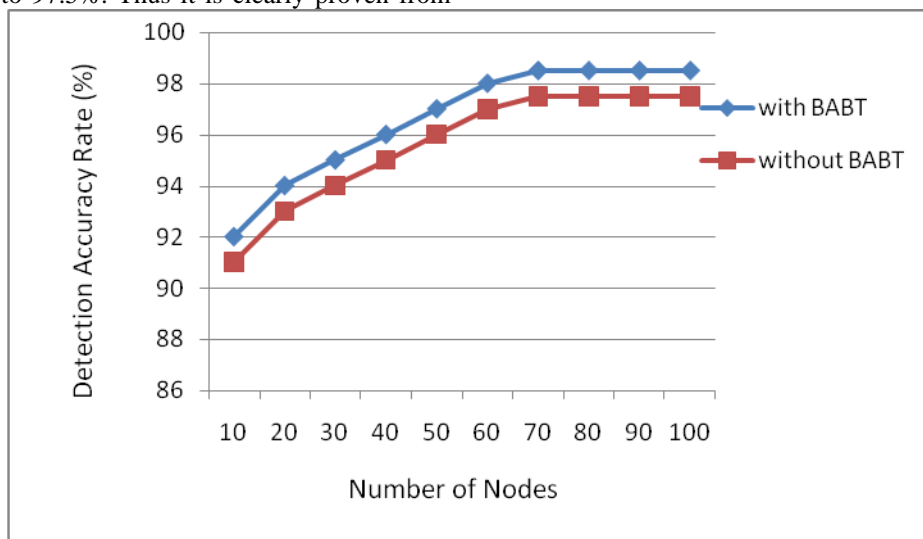


Figure 5 Detection Accuracy

In Figure 6, the comparative analysis of the detection time of the system with and without BABT algorithm is given. From the results, it is clear that the detection time of the proposed system with trust factor ranges from 0.1 to 1.4 sec.

On other hand for the system without the trust level is lies between 0.2 to 1.7 sec. Thus, the system with BABT algorithm consumes less time to detect the malicious node when compared to the system without trust factor.

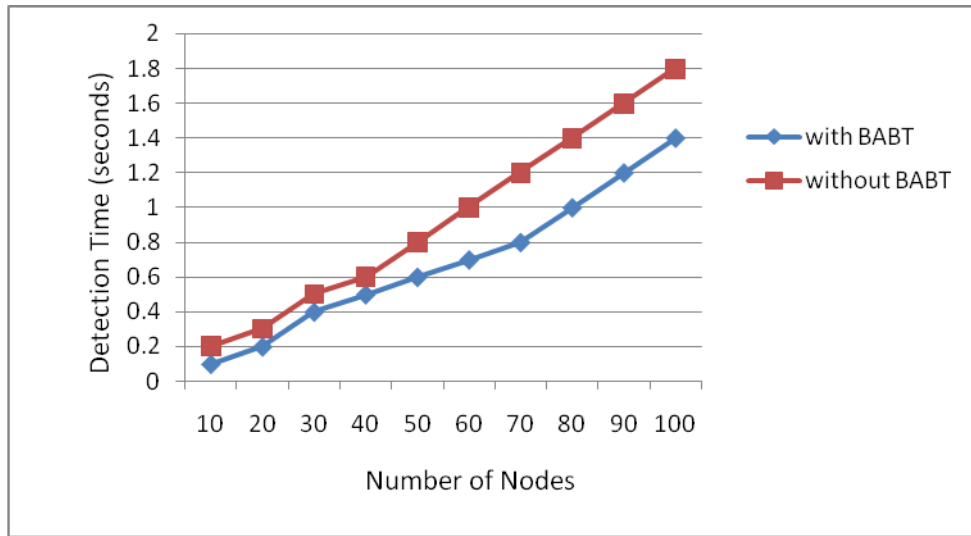


Figure 6 Detection Time

The comparative analysis of the detection accuracy rate for TASVM –IDS, SVM and ELM is presented in Figure 7. From the results it is observed that the detection accuracy rate of the proposed work ranges from 93.3% to 99.8%, for SVM lies between 93% and 99%, for ELM between 90%

and 95.4%. Thus, it is clear from the results that the proposed work achieves higher detection accuracy rate. This is because TASVM –IDS the detection accuracy is improved by both LCCBFE, the feature extraction algorithm and BABT, the trust estimation algorithm.

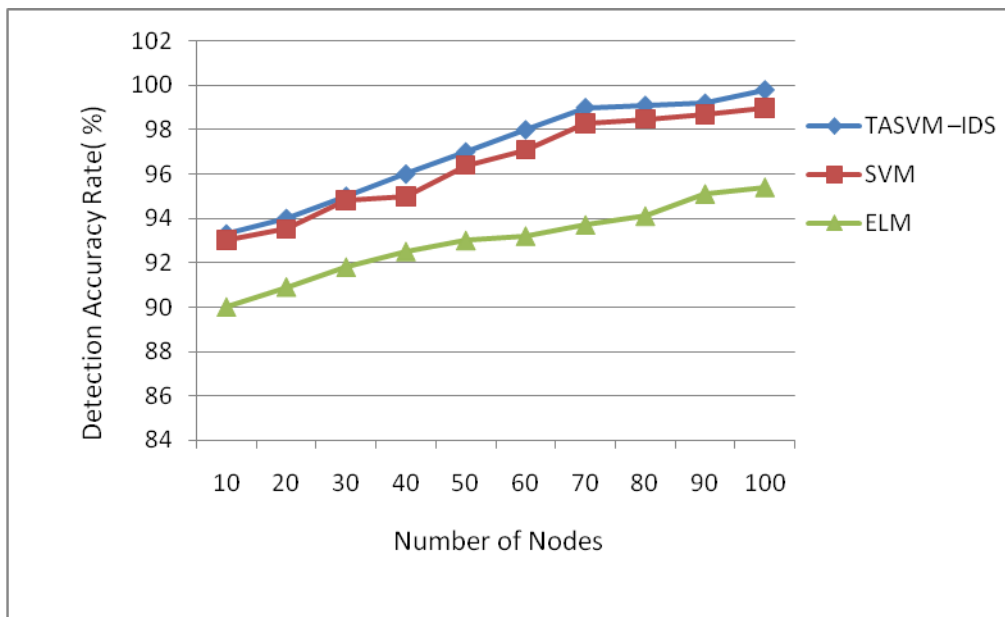


Figure 7 Detection Accuracy Rate

The comparison of misclassification rate between the proposed work, SVM and ELM is shown in the Figure 8. From the results it is observed that the misclassification rate of the proposed work varies from 7 to 0.5, in case of the SVM the misclassification rate ranges from 7.4 to 0.8

and for ELM the misclassification rate falls between 9.9 and 4.9. Therefore, it is clear that the proposed work has the lowest misclassification rate when compared to other existing works.

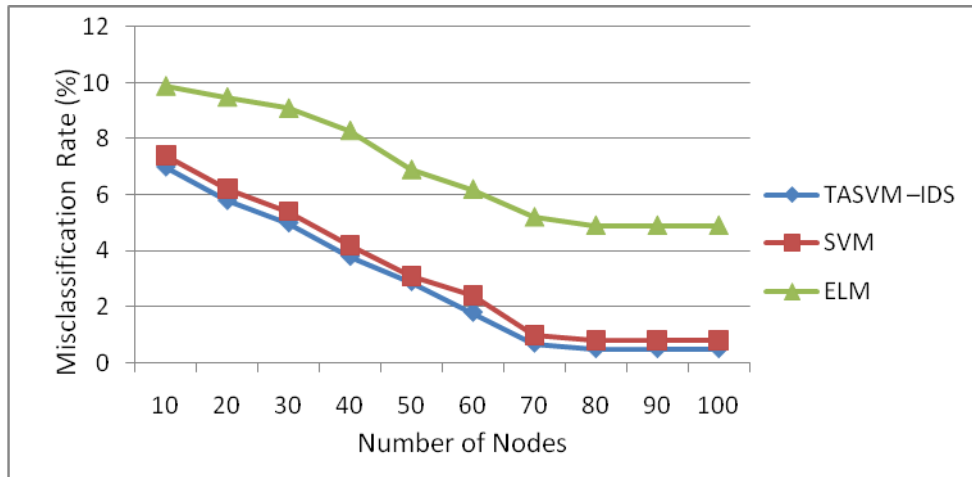


Figure 8 Misclassification Rate

In Figure 9, the comparison of detection time analysis between the proposed work SVM, ELM and MLP is presented. From the results the following observation are carried on for the proposed work the detection time varies from 0.1 to 0.95 , in case of the SVM the detection time ranges from 0.11 to 1.5 and for ELM the detection time falls

between 0.8 and 3. Therefore it is clear that the proposed work has the lowest detection time when compared to some of the already existing classifier. The reason is, in the proposed TASVM-IDS, detection time is enhanced by utilizing feature extraction process along with the trust estimation algorithm.

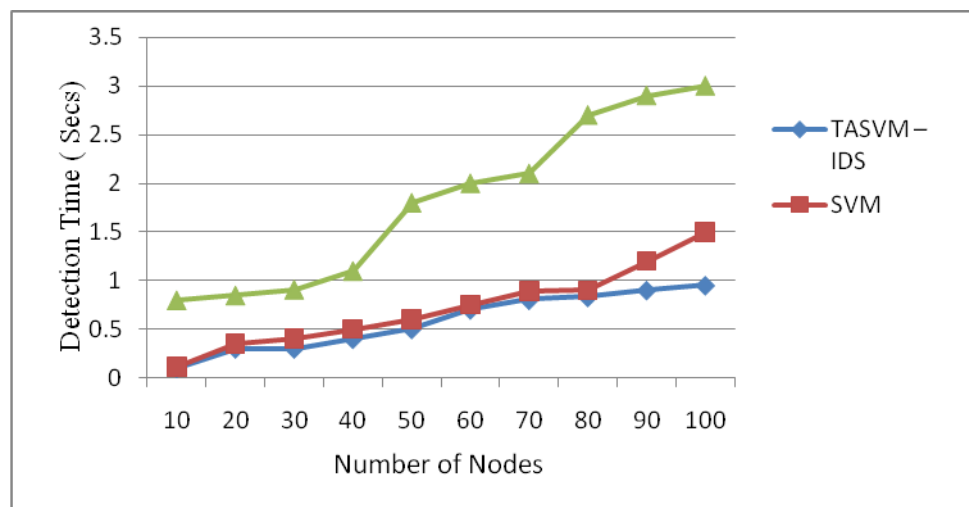


Figure 9 Detection Time Analysis

Table 6 illustrates the results of detection accuracy obtained from proposed work, SVM and ELM. From this experimental result it has been observed that the detection accuracy for DoS and Sleep deprivation are improved in the proposed when it is compared with the existing SVM and ELM algorithm. This is due to the fact that in the proposed work the malicious node those acts as a source for causing the attacks are detected more accurately by using the trust evaluation factor. Thus the detection accuracy in enhanced in this proposed work in comparison with the existing work.

Table 6 Detection Accuracy Analysis

| Experiment Number | SVM | | ELM | | TASVM-IDS | |
|-------------------|-------|----------------------|-------|----------------------|-----------|----------------------|
| | DoS | Sleep Deprive attack | DoS | Sleep Deprive attack | DoS | Sleep Deprive attack |
| 1 | 92.28 | 91.52 | 98.00 | 95.19 | 99.56 | 99.62 |

| | | | | | | |
|---|-------|-------|-------|-------|-------|-------|
| 2 | 91.35 | 90.72 | 97.22 | 95.42 | 99.40 | 99.25 |
| 3 | 91.65 | 90.62 | 97.23 | 95.92 | 99.52 | 99.42 |
| 4 | 91.58 | 91.27 | 97.28 | 96.21 | 99.27 | 99.28 |
| 5 | 91.88 | 91.20 | 97.82 | 95.48 | 99.15 | 99.18 |

Table 7 illustrate about the performance of TASVM-IDS in detecting the attacks. From this table it is clearly evident that training time and testing time are greatly reduced for both sleep deprivation attack and DoS attack. In this proposed work, only the features that contribute to attack decision process alone are considered. Hence, the classification accuracy is improved.

Table 7 Performance analysis of the proposed work in terms of training time, testing time and classification accuracy

| | Training Time | Testing Time | Accuracy |
|-------------------------------------|---------------|--------------|----------|
| Sleep deprivation Attack | 0.41 | 0.20 | 99.75 |
| DoS Attack (Packet Dropping Attack) | 1.72 | 0.83 | 99.86 |

5 CONCLUSION

In MANET design, developing an Intrusion Detection System to mitigate the attack caused by the malicious node is a major issue. In this paper, a novel Trust aware SVM based IDS TASVM-IDS has been proposed with the objective to mitigate the malicious nodes from the network and enhance the network lifetime. Moreover in this work the feature extraction process was carried out by the proposed Linear Correlation Coefficient Based Feature Extraction (LCCBFE) algorithm. Moreover, in this work a new Behavior Analysis Based Trust (BABT) algorithm has been developed to estimate the trust level of nodes based upon the behavior and residual energy level of nodes. From the simulation results the performance of the proposed system is analyzed with SVM and ELM. The results show that the proposed system gives better performance in terms of detection rate, detection accuracy and classification accuracy.

REFERENCES

1. Chlamtac, M. Conti, J.J.N.Liu. Mobile ad hoc networking: Imperatives and challenges. *Ad Hoc Networks*, 1(1);(2003);pp.13–64.

2. J.N. Al-Karaki, A.E. Kamal. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, 11(6); (2004);6–28.

3. S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.

4. F. Amiri, M. RezaeiYousefi, C. Lucas, A. Shakeri, and N. Yazdani, "Mutual information-based feature selection for intrusion detection systems," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1184–1199, 2011.

5. P. B. Velloso, R. P. Laufer, D. O. Cunha, O. C. M. B. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Trans. Netw. Serv. Manage.*, vol. 7, no. 3, pp. 172–185, Sep. 2010.

6. J. Anderson "Computer Security, Threat monitoring and surveillance", Fort Washington PA, James P, Anderson & Co, 1980.

7. Adnan Nadeem and Michael P. Howarth, "A survey of MANET Intrusion Detection & Prevention Approaches for Network layer Attacks," *IEEE Communication Surveys & Tutorials*, pp.1-19, 2012.

8. V. Karyotis, S. Papavassiliou, M. Grammatikou, and V. Maglaris, "A Novel Framework for Mobile Attack Strategy Modelling and Vulnerability Analysis in Wireless Ad Hoc Networks," *International Journal of Security and Networks*, Vol. 1, Nos.3/4, pp. 255 - 265, 2006.

9. S. Tilak , N.B. Abu-Ghazaleh , W.Heinzelman . A taxonomy of wireless micro-sensor network models. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(2); (2002);pp.28–36.

10. S.A. Mulay, P.R.Devale, & G.V. Garje, Intrusion Detection System using Support Vector Machine and Decision Tree, *International Journal of Computer Applications*, 3(3);(2010); pp.0975-8887.

11. C. Liu, Y. Yang and C. Tang. An Improved Method for Multiclass Support Vector Machines, *ACM International Conference on Measuring Technology and Mechatronics Automation*, Vol. 3;(2010);pp. 504-508.

12. K.Gupta, R.Kotagiri, B. Nath , Conditional Random Fields for Intrusion Detection, *Proceedings of International Conference of Advanced Information Networking and Applications Workshops*, Niagara Falls, (2007); pp.203-208.

13. B. Thuraisingham, L. Khan, M.M. Masud and K.W. Hamlen, Data Mining for Security Applications, *Web Intelligence and International Conference on Intelligent Agent Technology Workshops*, Milan, Italy, (2008); Vol.2;pp.585-589.

14. C.Zhang, G. Zhang and S. Sun, A Mixed Unsupervised Clustering-Based Intrusion Detection Model, In *Proceedings of International Conference on Genetic and Evolutionary Computing*, USA, (2009); pp. 426 - 428.

15. D.M.Farid, J. Dormont, N. Harbi, N.H. Hoa & M.Z.Rahman, Adaptive Network Intrusion Detection Learning: Attribute Selection and Classification, In *Proceeding of world academy of science, engineering and technology*,(2010); pp.154-158.

16. W.Wang, Z.Xiangliang ,S. Gombault and S. J. Knapkog, "Attribute Normalization in Network Intrusion Detection, *Proceedings of International Symposium of pervasive systems algorithms and networks*. Taiwan,(2009);pp.448-453.

17. D.Hongle, T. Shaohua, Z. Qingfang, Intrusion detection Based on Fuzzy support vector machines, *International Conference on Networks Security. Wireless Communications and Trusted Computing*.(2009); pp. 639-642.

18. Mitrokotsa, C. Dimitrakakis. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. *Ad Hoc Networks*. 11(1);(2013); pp.226–237.

19. Nadeem, M. Howarth. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. *Telecommunication Systems*. 52(4);2011;pp. 2047–2058.

20. J.Tweedale, A. Quteishat, C.P. Lim, L.C. Jain,. A neural network based multi-agent classifier system. *Neuro computing*. 72(7–9); (2009);pp.1639–1647.

21. S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh, A. Kannan, Intelligent feature selection and classification techniques for intrusion detection in networks: a survey. *EURASIP Journal of Wireless Communication Networks*. 271(1);(2013);pp. 1–16.

22. G.B.Huang,H. Zhou,X. Ding,R. Zhang, Extreme learning machine for regression and multiclass classification. *IEEE Transactions on Systems, Man, Cybernetics Part B Cybernetics*. 42(2); (2012);pp.513–529.





23. L.Prem,A. Kannan , An Active Rule Approach for Network Intrusion Detection with Enhanced C4.5 Algorithm. *The*



Journal of Communications, Network and System Sciences, 1(4);2008; pp. 314-321.

24. Yang, C, Ge, H, Yao, G & Ma, L 2009, 'Quick Complete Attribute Reduction Algorithm;', In: IEEE Sixth International Conference on Fuzzy Systems and Knowledge Discovery, vol. 4, pp. 576-580.
25. J. Cho, A. Swami, and I. Chen. 2011. A Survey on Trust Management for Mobile Ad Hoc Networks. IEEE Communications Surveys Tutorials, vol.13, no.4 , pp.562-583.2011.
26. K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communication Surveys and Tutorial*, vol. 14, no. 2, pp. 279-298, 2012.
27. Thanigaivel, G, Kumar, NA &Yogesh, P 2012, 'TRUNCMAN: Trust based routing mechanism using non-cooperative movement in mobile ad-hoc network', in Digital Information and Communication Technology and it's Applications (DICTAP), Second International Conference, pp. 261-266.
28. Bao, F, Chen, R, Chang, M & JH Cho 2012, 'Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection', Network and Service Management, IEEE Transactions, vol. 9, pp. 169-183, 2012.

AUTHORS BIOGRAPHY

| | |
|---|--|
|  | <p>A.R.Rajeswari, is currently working as Associate Professor in the Department of Computer Science and Engineering, Sethu Institute of Technology, Kariapatti, India. She has completed her M.E. and Ph.D degrees from Anna University, Chennai. She has published more than 10 papers in journals and conferences. Her area of interest include Computer Networks, Wireless Sensor Networks, Mobile Ad-hoc Networks and Security.</p> |
|  | <p>K.Kulothungan, is currently working as Associate Professor in the Department of Information Science and Technology, College of Engineering Guindy Campus, Anna University, Chennai. He received his M.E and Ph. D degrees from Sathyabama University and Anna University, Chennai respectively. He has published more than 40 articles in journals and conferences. His area of interest includes Computer Networks, Soft Computing, Cloud Computing and Security.</p> |
|  | <p>Sannasi Ganapathy, is currently working as Assistant Professor (Sr. Gr) in VIT University, Chennai. He received his M.E and Ph. D degrees from Anna University, Chennai. He has published 50 articles in journals and conferences. His area of interest includes Computer Networks, Soft Computing, Cloud Computing and Security.</p> |
|  | <p>A. Kannan is a Retired Professor of Anna University. He has received his M.E and Ph.D degrees in Computer Science & Engineering from Anna University, Chennai. He has published more than 350 articles in journals and conferences. His area of interest includes Databases, Artificial Intelligence and Security.</p> |