Intrusion Detection System for Mobile Ad Hoc Networks using Cross Layer and Machine Learning Approach

T. Poongothai
Associate Professor
Department of CSE
K.S.R College of Engineering, Tiruchengode

K. Jayarajan
Assistant Professor
Department of CSE
Selvam College of Technology, Tiruchengode

ABSTRACT
Mobile Ad Hoc Networking (MANET) has become a key technology in recent years because of the increased usage of wireless devices and their ability to provide temporary and instant wireless networking in situations like flooding and defense. In spite of their attractive applications, MANET poses high security problems compared to conventional wired and wireless networks due to its unique characteristics such as lack of central coordination, dynamic topology, temporary network life and wireless nature of communication. It is essential to have effective security system to provide trusted communication in MANET. Intrusion detection plays a major role in the security system of Mobile ad hoc networks. Data collected for intrusion detection system contains redundant and irrelevant features. Inclusion of these features result in poor predictions and high computational overhead. Feature selection process finds the most discriminative features that increase the detection accuracy and efficiency of the IDS. This study aims to select the important features using genetic algorithm and enhance the performance of SVM classifier. The performance of the system is validated using Network Simulator (NS2). The experimental results proved that the detection accuracy of detection with all features is 96.37% and genetic feature selection is 98.22%. The results demonstrate that the proposed IDS effectively detect the anomalies with high detection accuracy.

General Terms
Security, Machine Learning

Keywords
Mobile ad Hoc Networks, Intrusion Detection, Machine Learning, Genetic Algorithm, Cross-Layer design, Support Vector Machines.

1. INTRODUCTION
Wireless networks have gained more importance over wired networks in the recent decades because of their improved technology and reduced costs. Among all the wireless networks, Mobile Ad hoc NETwork (MANET) is the most significant application. In contrary to the conventional wireless network, MANET does not require a fixed infrastructure. All the nodes in the network are free to move randomly. Due to its unique characteristics, this technology has been used to support communications in situation where it may be impossible to deploy infrastructure networks, such as military battlefields, disaster recovery sites and medical emergency situations. In addition, this technology might be used to replace infrastructure networks. Owing to these unique characteristics, MANET is the one of the recent research field and received spectacular consideration among researchers. Network security is of vital importance for such critical applications. Due to the lack of nodes cooperation and physical protection, malicious nodes can easily capture and compromise nodes to achieve attacks. Particularly, the routing protocol of a MANET assumes that every node of a network is trusted and cooperative. Providing effective security for MANET routing become a challenging task.

Preventive techniques like encryption and authentication protect the users from unauthorized activities. But prevention based techniques alone cannot totally eliminate intrusions. Therefore, intrusion detection systems (IDSs), introduced as the second line of defense to protect the network. Based on detection techniques, IDS of MANET can be classified into the following categories.

- Anomaly detection: Here the normal behaviors of users are compared with the collected data, any activity that deviates from the normal behavior is considered as a possible intrusion. Then this information is passed to the system administrator.
- Misuse detection: The system keeps pattern of known attacks and compare these patterns with the collected data. If the data matches with the pattern, the intrusion is identified and the proper response is initiated

Anomaly detection has the advantage over misuse detection that they can detect novel attacks. Although anomaly detection is able to detect new types of intrusions, it is subject to high rate of false alarms.

Traditional intrusion detection system considers the activities of individual layers of network. But most of the attacks simultaneously exploit the vulnerabilities at multiple layer of the network. Intrusion detection system of Mobile ad hoc networks (MANET) proposed in the literature collects data only from single layer and also examines all the features of collected data. The features collected from single layer are not sufficient to detect the suspicious behavior. Some of the collected features may be redundant or contribute little to the detection process causing slow training and testing process. The redundant features increase the resource consumption of IDS and also affect the detection accuracy. The classifier cannot classify correctly irrelevant features. So it is vital to select the important features to improve the performance of classifier. Feature selection is the process selecting subset of features by eliminating irrelevant and uninformative features from original feature set. The advantage of the feature selection process is improving the performance of the learning algorithm and speed up the computation process of the resulting model.

The two main categories of feature selection are filter approach and wrapper approach. In filter approach, the features are selected before applying machine learning algorithm to the data set. In wrapper approach, the features are selected depending on the classifier. Filter approach is computationally efficient than wrapper approach. Wrapper

approach yields better result because of the usage of machine learning algorithm for selecting optimal features. It is essential to collect the features from multiple layers and also to select the important features from collected data to increase the detection accuracy.

In this paper, we propose a novel cross layer intrusion detection method using two machine learning techniques namely Genetic Algorithm (GA) and Support Vector Machines (SVM). Literature shows that the combination of GA and SVM offers excellent detection accuracy for classification. GA is used to preprocess the data and reduce the number of features of collected training data. SVM model is used for learning and classification purpose. This is the first application of Rough Set Theory and Support Vector Machine for Cross Layer Intrusion Detection of MANET.

The rest of the paper is organized as follows. Section 2 overviews the existing intrusion detection methods in MANET. Section 3 explains the introduction of Genetic Algorithm. We introduce the SVM classifier in Section 4. Section 5 presents the architecture of the proposed IDS system. Section 6 discusses the simulation results and analysis. Finally, Section 7 concludes the paper.

2. RELATED WORK

This section discusses the related work on the application of machine learning to IDS , usage of cross layer design for the intrusion detection and the application of feature selection in Intrusion Detection System.

2.1 Machine Learning in IDS of MANET

In the literature few machine learning algorithm used for the IDS of MANET. Nakayama et al., 2009 have proposed an anomaly detection model for detecting malicious behaviors that target the Ad-hoc On-demand Distance Vector (AODV) routing protocol. Their model utilizes machine learning in order to generate and maintain a normal profile and relies on principal component analysis (PCA) for resolving malicious behaviors. Sevil Sen and John A.Clark, 2011 used an evolutionary computation (EC) techniques particularly genetic programming (GP) and grammatical evolution (GE) to evolve intrusion detection programs. Also they analyzed the power consumption of evolved programs. They formed a multi objective evolutionary algorithm to discover optimal tradeoffs between intrusion detection ability and power consumption.EC techniques are proposed to discover the complex properties of MANETs. Farhan Abdel-Fattah, Zulkhairi Md. Dahalin and Shaidah Jusoh., 2010 proposed an intrusion detection method based on the combination of two machine learning techniques namely Conformal Predictor k-nearest neighbor and Distance-based Outlier Detection (CPDOD) algorithm. They devised two different metrics to improve detection ability. They are nonconformity metric and Outlier Factor LDOF metric.

2.2 Cross Layer Design in intrusion detection of MANET

Cross layer design in MANET is a popular research topic in the research community. Y. Liu, Y. Li, and H. Man 2005 proposed a distributed cross-layer based anomaly detection by adapting a rule based data mining technique. In this work, a feature set is collected by correlating the information from the MAC and the network layers. The developed IDS is able to effectively localize attack source within one-hop perimeter. Thamilarasu et al. 2005 proposed a cross-layer based intrusion detection (CIDS) engine to detect DoS attacks at different layers of the protocol stack. The output from different layer is collected and the decision made collectively. By the use of features from MAC and Network layers the accuracy of the Intrusion Detection System (IDS) is increased but the detection module at every layer increases the processing overhead significantly. J. Felix et al., 2011 have proposed an autonomous host IDS engine for detecting sinking attacks in MANETs. The Detection system uses cross layer approach. This method used Optimized Link State Routing (OLSR) routing protocol for defining feature set. The features are collected from network, MAC and physical layer. This IDS uses two machine learning algorithms namely Support Vector Machines (SVM) and Fisher Discriminant Analysis (FDA).

2.3 Feature Selection in IDS

Literature shows the usage of different feature selection techniques. Sung and Mukkamala., 2004 used feature ranking algorithms to reduce the features of DARPA data set. They reduced the number of features from 41 to 6. They used Support Vector Machines (SVMs), Multivariate Adaptive Regression Splines (MARSs), and Linear Genetic Programs (LGPs) for ranking the features. Gary Stein et al., 2005 applied a genetic algorithm to select optimal features for decision tree classifiers for network intrusion detection. The combination of genetic algorithm and decision tree outperforms the decision tree algorithm without feature selection. The work reported by Wang et al., 2005 applied Markov Blanket algorithm combined with bayesian and decision tree classifier. In this approach, Markov Blanket Discovery is used for selecting essential features. Khalil El-Khatib 2010 combines filter and wrapper approach for selecting relevant features. Their model uses information gain ratio to compute the relevance of features and k-means classifier to select the optimal features. Learning time of the classifier is reduced to 33 percent and accuracy of detection is improved by 15 percent. Sevil Sen and Zeynep Dogmus 2012 introduces feature selection technique for the detection of ad hoc flooding attacks. Detection method uses genetic algorithm to select the relevant features. The performance of the support vector machine is improved with the feature selection approach. This method uses network layer features for the detection process and also it consider only the flooding attack.

None of the above works combine the feature selection technique with cross layer IDS of MANET with AODV routing protocol.

3. GENETIC ALGORITHM

Genetic algorithm is presented by Prof. Holland in 1975. It is a stochastic search method which is inspired by Darwinian natural selection and biological reproduction. It is used to find exact or approximate solutions to optimization and search problems. It provides a learning method inspired by evolutionary biology. Genetic algorithms have been successfully applied to a wide variety of scientific and engineering optimization or search problems. It maps the searching space in to genetic space. The searching space is encoded into a chromosome. The chromosome represents the problem to be solved. Each element of a chromosome represents a gene. All of the chromosomes make up a population and is represented by means of binary strings of 0's and 1's. The goodness of a chromosome is measured by using the fitness function which shows how the chromosome solves or comes close to the solution. Initial population of the genetic algorithm is created randomly. GA generates successive populations by using selection, mutation and cross over operations. GA obtains the optimal solution after a series of iterative computations with some termination condition.

The basic algorithm of GA is given below

Algorithm

Input:

Binary String, Number of generations, Population Size,

Crossover Probability, Mutation Probability

Output:

Begin

Initialize population;

Evaluate population members;

While (the stopping criterion is not met)

Begin

Select parents from current population;

Apply genetic operators to selected parents;

Evaluate offspring;

Set offspring equal to current population;

Next generation until stopping criterion

End

End

Initial population is evaluated using fitness function. Based on the fitness values, the parents are selected from current population. Crossover and mutation operator affects the fitness value of a chromosome. Crossover allows the exchanging of genes between two chromosomes using the one point crossover, two point crossover, or uniform crossover. In the process of mutation the genes of chromosome may be altered, i.e. in binary code genes changing genes code from 0 to 1 or vice versa.

Offspring replaces the old population using its goodness value and forms a new population in the next generation. This process operates iteratively until termination conditions satisfy.

GA feature selection uses a wrapper approach. For a data record, each value of the feature is converted into a binary gene value, 0 or 1. We produce initial population randomly where each individual contains approximately the same number of 1's and 0's on the average. The population size is 100 and the number of generation is 100. Fitness value of each individual is calculated and its goodness is evaluated. Based on the goodness value the individuals are selected for mutation and cross over operations.

4. SUPPORT VECTOR MACHINES

The Support Vector Machines was initially proposed by Vapnik (Burges,.C.J.C, 1998). It is a machine learning algorithm that is useful for classification. A classification problem generally involves a variety of information samples, each of which is associated with a category (or label) and some features (or attributes). Given a previously unseen sample, the problem is to predict its class by looking at its features. A support vector machine solves this problem by first building a model from a set of data samples with known classes (i.e., the training set), and use the model to predict classes of data samples that are of unknown classes.

The basic SVM takes a set of input data and predicts, for each given input, which of two possible classes forms the input.SVM construct a hyperplane that separates two classes in the high dimensional space.SVM tries to achieve maximum separation between the classes. Figure 1 shows the hyperplane of SVM

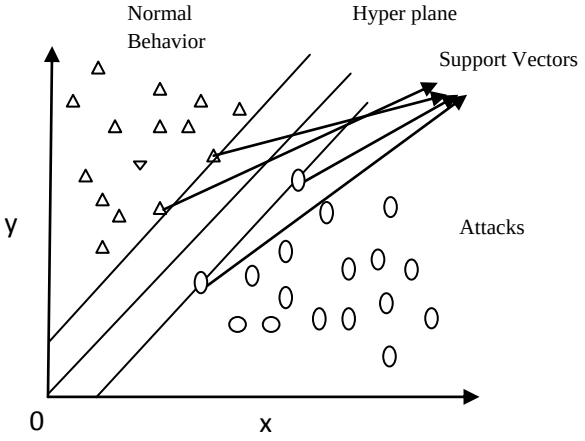

Fig 1: Hyper plane of SVM

The training data is represented as

$(x_i, y_i),\ldots, (x_n ,y_n), x \in R_m ,y \in \{+1,-1\}$

where (xi , yi),…, (x_n ,y_n) are a train data, n is the numbers of samples, m is the input vector, and y fits in to category of +1 or -1 respectively. The hyper plane is

(w. x) + b =0

where w is normal to the hyperplane, |b| / |w| is the perpendicular distance from the hyperplane to the origin.

All the training data satisfy the following constraints

$$w.x + b \geq +1 \text{ for } y_i = +1$$

$$w.x + b \leq -1 \text{ for } y_i = -1$$

The decision function is given in Eq.(1)

$$f(x) = sgn(w.x + b) = sgn(\sum_i^N \alpha_i\ y_i(x_i, x) + b) \qquad (1)$$

The training vectors x_i occur only in the form of a dot product. For each training point, there is a Lagrangian multiplier α_i. The Lagrangian multiplier values α_i reflect the importance of each data point. When the maximal margin hyper-plane is found, only points that lie closest to the hyper-plane will have $\alpha_i > 0$ and these points are called support vectors. All other points will have $\alpha_i = 0$. That means only those points that lie closest to the hyperplane, give the representation of the hypothesis/classifier. These data points serve as support vectors. Their values can be used to give an independent boundary with regard to the reliability of the hypothesis/classifier.

5. PROPOSED IDS ARCHITECTURE

Figure 1 shows the conceptual architecture of proposed IDS. The architecture consists of the following components: Data Collection module, Preprocessing module, Feature Selection module, Training and Classification module.

5.1 Data Collection Module

This module gathers information from medium access control and network layers to identify the normal and malicious behavior of mobile node. The collection module in the IDS architecture monitors the events and packet delivery time,

traffic, and topology statistics and records the feature values. In anomaly detection, we want to select the trace data that bears evidence of normality or anomaly. Normal profile is created using the data collected during the normal scenario. Attack profile is created by simulating the attacks. The feature set includes routing activities and data forwarding behavior at network layer. The proposed system uses the most popular reactive Ad hoc On Demand Distance Vector Routing (AODV) routing protocol for collecting the routing behavior. List of important cross layer features are shown in table 1.

Table 1 List of Cross Layer Features

Layers	**Features**	
MAC Layer	RTS, CTS, DATA, ACK	
Network Layer	Routing Control Packets	RREQ, RREP, RERR and Hello
	Route Table Changes	Number of Neighbors, Added routes, Deleted Routes etc.
	Data Control Packets	Data

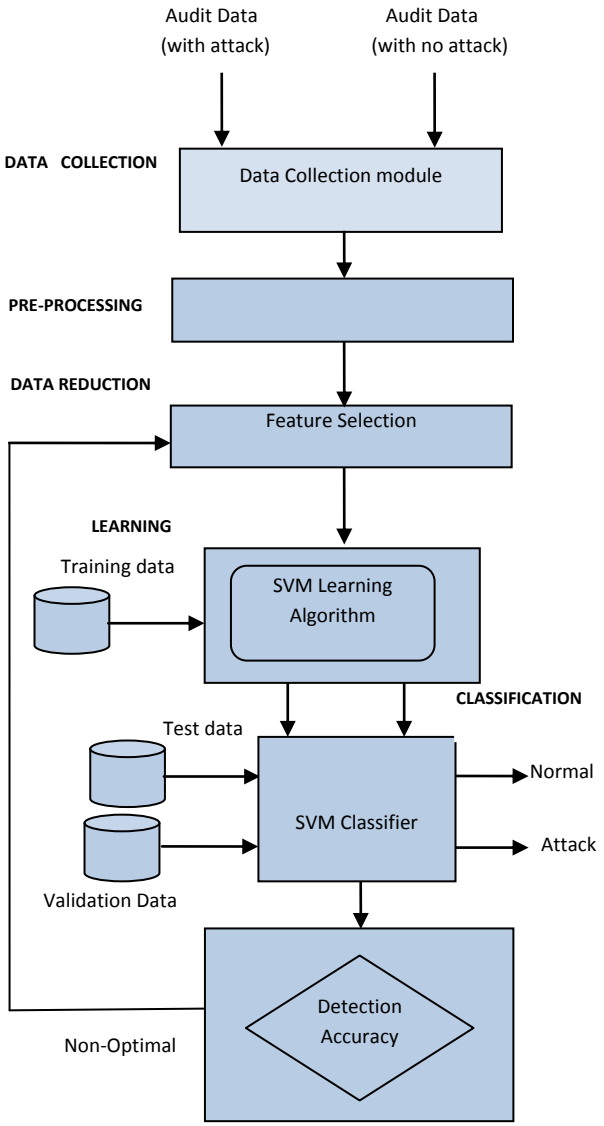

Fig 2: Architecture of proposed IDS

5.2 Preprocessing Module

Collected data are normally incomplete and noisy. Also the values may be missing or it may contain outliers. During preprocessing these issues are handled and also collected data is transformed into appropriate format for the detection process.

5.3 Feature Selection Module

The proposed approach uses wrapper feature selection algorithm for the selecting the important features. Feature selection process consists of two main components: GA and SVM classifier. GA selects the subset of features and then SVM classifier evaluates the subsets during a classification process. The result of the classification is applied for finding the fitness value of GA. The process of feature selection is shown in Fig 3.

Let n be the total number of features of collected data. Random individuals are created for the collected data. Each individual represent the feature sub set. SVM algorithm determines the fitness value for each individual. The fitness value depends on objective function or cost function. Fitness value for each individual is calculated and best individual is selected for next generation given in Eq.(2)

$$Fitness(x) = accuracy(x) \quad (2)$$

Where x is the feature subset. Accuracy(x) is the detection accuracy of SVM on feature subset X. If two feature subsets have the same detection accuracy then feature subset with lowest feature is selected. The GA algorithm applied repeatedly until a defined generation is reached. Finally, it produced the optimal set of features. The reduced feature set is used for training and testing process. The algorithm for feature selection is given below

Input: Data Set

Input for GA: number of chromosomes, total iteration, crossover and mutation rate

Output: selected subset features

Begin

Step 1: Read the total number of features from the collected data.

Step 2: Produce the random initial populations by turning on/off the individual bits.

Step 3: Evaluate each individual.

Step 3.1: Read the feature values.

Step 3.2: chromosome representation in New-GASVM.

Step 3.2.1: Save the values of each feature and store it in array.

Step 3.2.2: Sort the values.

Step 3.2.3: Store the selected features based on the values.

Step 3.3: Evaluate each individual (chromosome) using SVM classifier.

Step 4: GA operates on the population to evolve the best solution.

Step 4.1: Apply the selection strategy and GA operators.

Step 4.2: Repeat Step 3

Step 5: Return the best subset of features.

End

5.4 Training Module

Machine learning is used for the training purpose of proposed IDS. The learning model is essentially a Support Vector Machines (SVM). This model is trained by SVM algorithm using the reduced training set. By using set of training examples, the SVM training algorithm constructs a model that determine the category of new example.

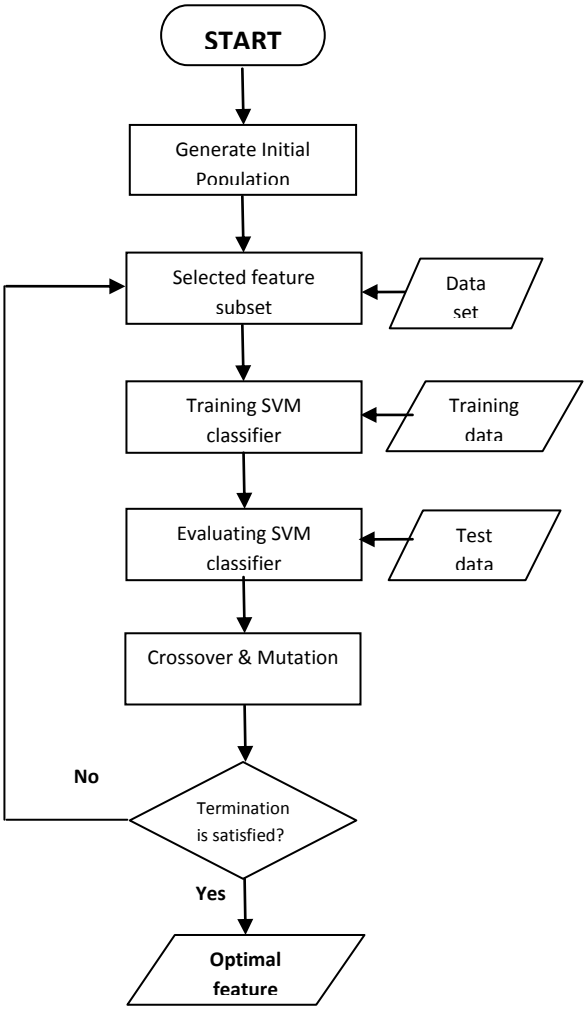

Fig 3: GA based feature selection

An SVM maps linear algorithms into non-linear space. It uses a feature called, kernel function, for this mapping. Kernel function is used to divide the feature space by constructing a hyperplane. The kernel functions can be used at the time of training of the classifiers which selects support vectors along the surface of this function.

5.5 Classification

The trained SVM model can be used for the detection of malicious behavior. For many problems it is not easy to find hyper planes to classify the data. The SVM has several kernel functions that users can apply to solving different problems. Selecting the appropriate kernel function can solve the problem of linear inseparability. Another important capability of the SVM is that it can deal with linear inseparable problems. Internal product operations affect the classification function. A suitable inner product function $K(x_i,x)$ can solve certain linear inseparable problems without increasing the complexity of the calculation. There are four kernel function namely, linear function, polynomial function, radial basis function (RBF), and sigmoid function.

The decision function for non linear SVM is given in Eq.(3)

$$f(x) = sgn(\sum_{i}^{N_S} \alpha_i y_i k(x_i, x) + b) \quad (3)$$

Ns is the total number of support vectors. The sign of the decision function determine the category of unknown behavior x. $K(x_i,x)$ is the kernel function. The proposed IDS use RBF as the kernel function.

6. PERFORMANCE EVALUATION

6.1 Simulation Environment

To validate the efficiency of the proposed IDS model attacks are simulated with varying network conditions under Linux environment using Network Simulator (ns-2) [12]. Table 2 lists the different values of experiment parameters. The three network conditions mobility, traffic density and number of malicious nodes are varied for analysis. Intrusion detection system is evaluated under different mobility conditions, traffic density and number of malicious nodes. Traffic density represents the number of nodes involved in the transmission. Mobility is varied by varying the pause time of the mobile nodes.

Table. 2. Ns-2 Attack Simulation setup with varying network conditions

Sno.	Parameter	Value
1	Routing protocol	AODV
2	Simulation duration	1000 sec
3	Topology	1000m x 500 m
4	Number of mobile nodes	50
5	Transmission range	250 m
6	Mobility model	Random waypoint model
7	Traffic type	CBR/UDP
8	Data payload	512 bytes
9	Number of connections	5,10,15 and 20
10	Maximum speed	10 m/s
11	Number of malicious nodes	5,10,15 and 20
12	Pause time	0,20,40,60 and 80
13	Attack duration	2 – 50 sec

6.2 Attacks Simulated

In this work one of the most popular reactive routing protocol of a MANET, Ad hoc On Demand Distance Vector (AODV) is used. AODV (Perkins, C., Belding-Royer, E. and Das, S.,2003) is designed such that all the nodes must participate in the routing process. This protocol assumes that the network is trusted and the nodes are cooperative. But AODV is vulnerable to wide variety of attacks like Route Disruption, Route Invasion, Node Isolation and Resource Consumption

(P.Ning and K.Sun, 2003). The trace files are generated by simulating the attacks with different mobility of a node. The features are collected by each node periodically by analyzing the data from the trace log using awk scripts. All these features are only local to the nodes.

6.3 Results and Analysis

The node mobility is varied and the performance of detection rate is studied. The detection rate of IDS also analyzed with varied traffic density and number of malicious nodes. LIBSVM tool [5] is used for the SVM operations. For each scenario, five individual runs with different network conditions are performed.

To evaluate the performance of IDS, there are three parameters used namely, detection accuracy, false positive rate and false negative rate. Detection accuracy (DA) is defined as the ratio of the number of events being predicted correctly to the total number of events. False positive rate (FPR) is defined as the ratio of the number of attack-free events falsely being identified as anomalies to the total number of normal events. False negative rate (FNR) is defined as the ratio of the number of anomalies falsely predicted as attack-free events to the total number of anomalies. These metrics are measured as the average of five runs of ns2 simulation with varying network conditions.

The results of IDS are compared between SVM aided by Rough Set and SVM without Rough set for the Route Disruption Attack. All these features are not relevant to the detection process every instance. Only some of the features contribute more. In order to select the essential features, the most popular feature selection method Rough set is used.

6.3.1 Effect of mobility

These three parameters are affected by mobility. To see this consequence performance metrics are measured with five mobility levels, i.e. pause time is set to 0, 20, 40, 60 and 80. It shows false positive rate, false negative rate increases and detection accuracy increases as mobility decreases (or pause time increases). Figure 3 depicts the relationship between detection accuracy and pause time. If the pause time is 0, the nodes are moving in the network all the time. Due to the mobility, the detection accuracy is reduced. If the pause time is increased, then the nodes are closer to static position. Therefore the detection accuracy is better if the pause time is increased.

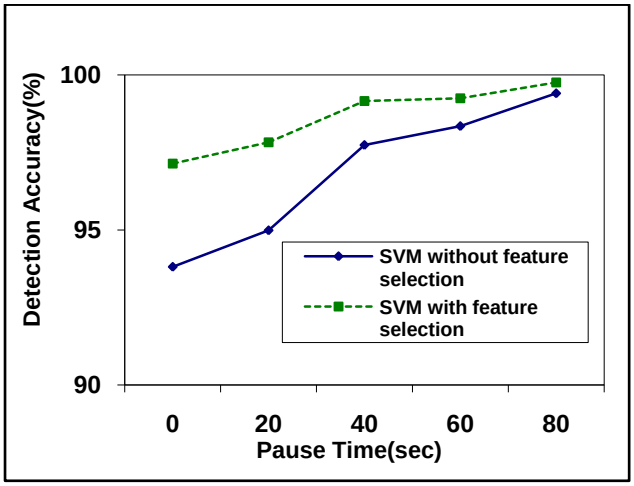

Fig 3: Pause Time vs. Detection Accuracy

Figure 4 and 5 depicts the relationship between incorrect predictions (false positive rate and false negative rate) and pause time. From that we infer that, if the nodes are not moving the activities of the network can be easily predicted.

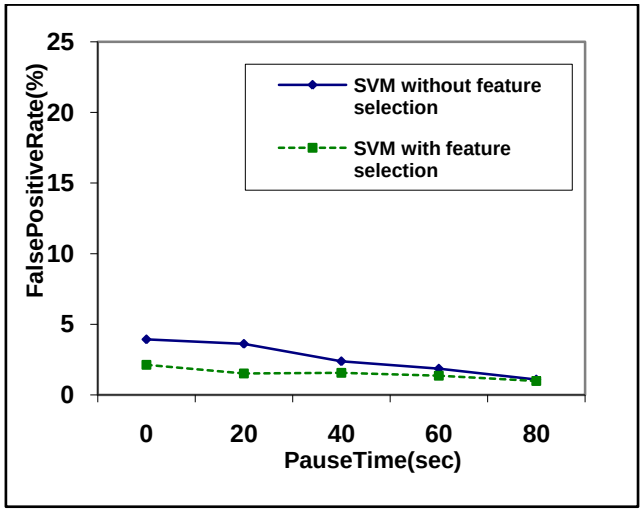

Fig 4: False Positive Rate vs. Pause Time

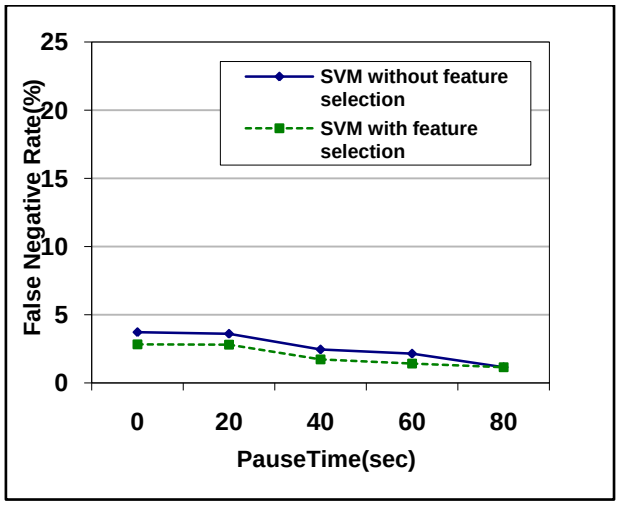

Fig 5: False Negative Rate vs. Pause Time

6.3.2 Effect of Traffic Density

Figure 6 illustrates the effect of network traffic against detection accuracy. Metrics are measured with different traffic levels such as 5, 10, 15, and 20 data sources. Here the experiments are done with the pause time of 40 seconds and number of malicious nodes with 5. Observation shows that the number of connections increases then there is slight performance degradation. If the traffic increases, all malicious nodes are trying to send bogus routing control packets to every source. So the system has to take care of different anomalous activities. Due to this reason the detection accuracy is reduced by one percentage at each traffic level.

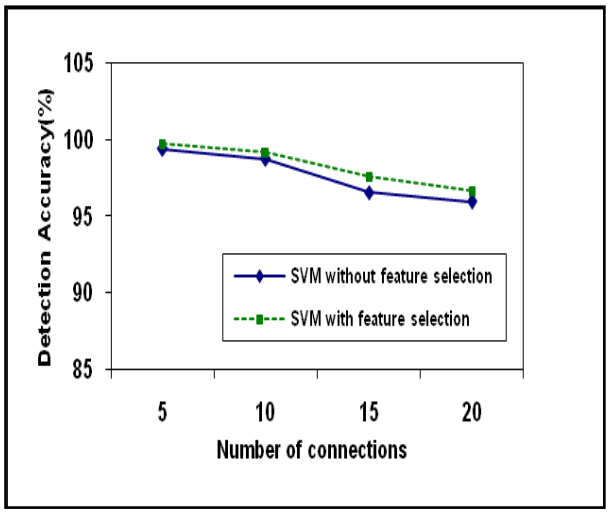

Fig 6: Number of connections vs. detection accuracy

6.3.3 Effect of Number of Malicious Nodes

Figure 7 illustrates the effect of different number of malicious nodes with detection accuracy. Metrics are measured with different attack levels such as 5, 10, 15, and 20 malicious nodes. Experiments were done with the pause time of 40 seconds and number of connections with 20. Here also there is a slight degradation in detection accuracy. If the number of malicious nodes is less, then they cannot send bogus messages to normal nodes all the times because of the communication range. If it increases the attacker can easily achieve its objective. Because of these characteristics the detection accuracy is decreased by the rate of 1%. Table 3 compares the performance of the cross layer IDS with all features and the cross layer IDS with rough set feature selection for the simulated attacks.

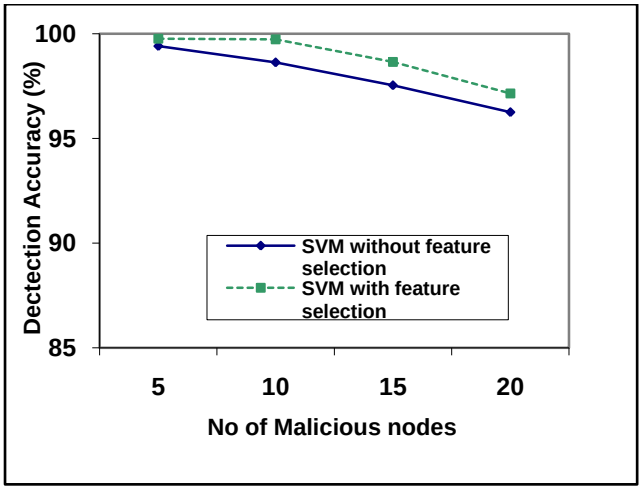

Fig 7: Number of malicious nodes vs. detection accuracy

Table 3. Detection Accuracy of the Proposed IDS

Attack type	Results with all features (%)	Results with genetic selection (%)
Route Disruption	96.86	98.63
Route Invasion	96.23	98.39
Node Isolation	96.36	98.41
Resource Consumption	96.03	97.45

7. CONCLUSION

In this work, cross-layer based anomaly detection system has been presented for detecting misbehaviors. This approach is based on feature selection method and it applies genetic algorithm to choose relevant features. Genetic algorithm shows that it is not necessary to use all the features for classification. This approach reduces the computation overhead and increases the detection accuracy. The efficiency is of the IDS is analyzed with varying network conditions by simulating routing attacks. The detection accuracy of IDS with all features is 96.37% and genetic feature selection is 98.22%. Experimental studies shown that IDS with selected features increases the detection accuracy and minimizes the false alarm rate. The observation states that the performance of cross IDS with genetic feature selection is improved.

8. REFERENCES

[1] Chih-Fong Tsai, Yu-Feng Hsu , Chia-Ying Lin and Wei-Yang Lin, 2009. Intrusion detection by machine learning: A review *Expert Systems with Applications*, 36(10),pp.11994-12000.

[2] Farhan Abdel-Fattah, Zulkhairi Md. Dahalin and Shaidah Jusoh, 2010. Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm *IJCA Special Issue on MANETs*, no .1,pp. 22-29.

[3] Geethapriya Thamilarasu, Aruna Balasubramanian, Sumita Mishra and Ramalingam Sridhar ,2005.A Cross-Layer Based Intrusion Detection Approach for Wireless Ad Hoc Networks, *Proc. IEEE Int'l Conf.Mobile Adhoc and Sensor Systems 2005*.

[4] Joseph, J.F.C., Bu-Sung Lee, Das,A. and Boon-Chong Seet,2011. Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA *IEEE Transactions on Dependable and Secure Computing*, vol.8, no.2, pp.233-245.

[5] LIBSVM -- A Library for Support Vector Machines:www.csie.ntu.edu.tw/~cjlin/libsvm/.

[6] Liu, Y., Li, Y., and Man, H.,2005. Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks *Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks 2005 (SecureComm '05).*

[7] Mishra, A., Nadkarni, K. and Patcha, A., 2004. Intrusion detection in wireless ad hoc networks *IEEE Transactions on Wireless Communication*s, vol. 11, no.1, pp. 48–60.

[8] Nakayama, H., Kurosawa, S., Jamalipour, A., Nemoto, Y. and Kato, N., 2009. A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks *IEEE Transactions on Vehicular Technology*, vol.58, no.5, pp.2471-2481.

[9] Ning,.P and Sun,.K,2003. How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols, *In Proceedings of 4th Annual. IEEE Information Assurance Workshop*, pp. 60–67.

[10] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya ,2011. Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET *IEEE*

Transactions on Dependable and Secure Computing, vol 8, no 1 pp.89-103.

[11] Ns-2: The Network Simulator, 2010. http://isi.edu/nsnam/ns/.

[12] Perkins, C., Belding-Royer, E. and Das, S.,2003. Ad hoc On-Demand Distance Vector (AODV) Routing, *IETF RFC 3561*.

[13] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han, 2010. A Novel Cross Layer Intrusion Detection System in MANET, *24th IEEE International Conference on Advanced Information Networking and Applications*, pp.647 – 654.

[14] Sevil Sen, John A. Clark, 2011. Evolutionary computation techniques for intrusion detection in mobile ad hoc networks, *Computer Networks*, Vol 55, Issue 15, pp. 3441-3457.

[15] Sergio Pastrana, Aikaterini Mitrokotsa, Agustin Orfila ,Pedro Peris-Lopez, 2012. Evaluation of classification algorithms for intrusion detection in MANETs *Knowledge-Based Systems* Vol.36,pp.217-225.

[16] Shengrong Bu, Richard Yu F., Xiaoping P. Liu, Peter Mason and Helen Tang,2011. Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks *IEEE Transactions on Vehicular Technology*, vol 60 no.3 pp. 1025–1036.

[17] 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.

[18] Burges,.C.J.C, 1998, A Tutorial on Support Vector Machines for Pattern Recognition *Data Mining and Knowledge Discovery*, vol. 2, no. 2,pp. 121-167.

[19] X. Wang, T. L. Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network, Technical Report, Computer Science, Iowa State University, USA, 2005.

[20] G. Stein, B. Chen, A.S. Wu, and K.A. Hua, "Decision Tree Classifier for Network Intrusion Detection with GA-Based Feature Selection," Proc. 43rd ACM Southeast Regional Conf.—Volume 2, Mar. 2005.

[21] A.H. Sung and S. Mukkamala, The Feature Selection and Intrusion Detection Problems, Proc. Ninth Asian Computing Science Conf., 2004.

[22] Sevil Sen, Zeynep Dogmus, Feature Selection for Detection of Ad Hoc Flooding Attacks, *Advances in Intelligent and Soft Computing*, *Springer* 2012, Volume 176, pp 507-513.