Asian Journal of Information Technology 12 (8): 242-249, 2013
ISSN: 1682-3915

Effective Cross Layer Intrusion Detection in Mobile Ad Hoc Networks Using Rough Set Theory and Support Vector Machines

[1]T. Poongothai and [2]K. Duraiswamy
[1]IT Department, K.S.R. College of Engineering, 637215 Tiruchengode, Tamil Nadu, India
[2]CSE Department, K.S. Rangasamy College of Technology,
637215 Tiruchengode, Tamil Nadu, India

Abstract: Intrusion detection on Mobile Ad Hoc Networks (MANET) is a challenging task due to its unique characteristics such as open medium, dynamic topology, lack of centralized management and highly resource constrained nodes. Conventional Intrusion Detection System developed for wired networks cannot be directly applied to MANET. It needs to be redesigned to suit the ad hoc technology. Proposed IDS uses cross layer features instead of using single layer features to improve the performance. Also, the proposed system maximizes the detection accuracy by using two machine learning techniques. Support Vector Machines (SVM) and rough set theory are used together to take the advantage of better accuracy of SVM and faster speed of rough set. The performance of the system is validated using Network Simulator (NS2). The simulation results demonstrate that the proposed IDS effectively detect the anomalies with high detection accuracy.

Key words: Mobile ad hoc networks, intrusion detection, machine learning, rough set theory, cross-layer design, support vector machine

INTRODUCTION

In recent years, Mobile Ad Hoc Networks (MANET) are one of the fastest growing areas of research and more popular technology in wireless network because of the increased usage of wireless devices. Unlike conventional networks, they do not have fixed infrastructure and centralized management. Each node in the network needs to act as a router as well as a host. Therefore, node cooperation is very much important for the network functioning.

This creates a lot of security vulnerabilities called attacks in MANET. Attack prevention measures such as authentication and encryption are used to handle outside attacks but they cannot detect inside attacks. The intrusion detection system acts as a second line of defense to detect the inside intruders. Existing Intrusion Detection technique developed for wired networks cannot be applied directly to MANET. The use of IDS developed for wired networks to safeguard the MANET is neither direct nor easy to perform. It needs to be restructured to suit the characteristics of MANET. The main function of the IDS is to identify the intrusion from audit data collected from network. Based on detection techniques, IDS of MANET can be classified into the following categories (Mishra *et al*., 2004).

Anomaly detection: Here the normal behaviors of users are compared with the captured data, anyactivity that deviates from the baseline 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 captured data. Any matched pattern is treated as an intrusion. Then, 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, most of these anomaly-based IDSs suffer from a 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 features of collected data may be redundant or contribute little to the detection process. Use of all features increases the computational complexity and degrades the performance of the detection

Correspondong Author: T. Poongothai, IT Department, K.S.R. College of Engineering, 637215 Tiruchengode, Tamil Nadu, India

system. 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 study, researchers propose a novel cross layer intrusion detection method using two machine learning techniques namely Rough Set Theory (RST) and Support Vector Machines (SVM). Literature shows that the combination of RST and SVM offers excellent detection accuracy for classification (Chen *et al*., 2009; Shrivastava and Jain, 2011; Pastrana *et al*., 2012). RST 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. The combinations of rough set theory and support vector machines algorithms has been applied to IDS of wired networks but have not been applied to mobile ad hoc network intrusion detection. This is the first application of rough set theory and support vector machine for intrusion detection of MANET.

Literature review: This study reviews related research on intrusion detection in MANET, the application of machine learning to IDS and the usage of cross layer design for the intrusion detection.

Intrusion Detection Systems in MANET: The intrusion detection system for MANET is a challenging task compared with wired networks. Many solutions have been developed to detect the intrusions. Mohammed *et al*. (2011) proposed a mechanism design based model for secure leader election in the presence of selfish nodes. To balance the resource consumption of the nodes in the network, nodes with the most remaining resources should be elected as the leaders. This model proposed a two leader election algorithms namely Cluster Dependent Leader Election (CDLE) and Cluster Independent Leader Election (CILE). The former does not require any pre-clustering whereas CDLE requires nodes to be clustered before running the election mechanism. This study mainly focuses the leader election process instead of detecting the malicious behavior. Bu *et al*. (2011) proposed a fully distributed scheme of combining intrusion detection and continuous authentication in MANETs. They used Dempster-Shafer theory for data fusion. The main drawback of this approach is high computational complexity.

Machine learening 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 learening in order to generate and maintain a normal profile and relies on Principal Component Analysis (PCA) for resolving malicious behaviors.

Abdel-Fattah *et al*. (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. Sen and 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.

Cross leayer design in intrusion detection of MANET: Cross layer design in MANET is a popular research topic in the research community. Liu *et al*. (2005) recently proposed a distributed cross-layer based anomaly detection by adapting a rule based data mining technique. In this research, 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 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. Joseph *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). To the best of the knowledge the combination of SVM and rough set theory with cross layer IDS has not introduced for MANET.

MATERIALS AND METHODS

Machine learning: Machine Learning (ML) is a branch of artificial intelligence. It programs the computer to be able to learn from examples. This system tries to eliminate the

need for human intuition in data analysis. Machine learning algorithms can be used for classification and clustering. Intrusion Detection System of MANET is a typical classification problem. Various machine learning algorithms are fuzzy logic, artificial neural networks, Support Vector Machines (SVM), Genetic algorithm, K-nearest neighbor, decision trees, Rough Set Theory (RST) and Bayesian classifiers. Among all the algorithms support vector machines offers excellent detection accuracy compared to other algorithms (Tsai *et al*., 2009). If the size of the data set is large, SVM suffers from high computational overhead. Therefore, the size of the data set is reduced using feature selection technique. Rough set theory has proven popular feature selection method (Parthalain, 2009) and has attracted much interest from researchers. This data reduction process increases the performance of SVM.

Rough set theory: Rough Set Theory (RST) is an extension of classical set theory that supports approximations in decision making. This concept was introduced by Pawlak (1998) in the early 1980's. RST proposes a new mathematical approach to imperfect knowledge. It is an approximation of a vague concept by a pair of precise concepts, called lower and upper approximations which are a classification of the domain of interest into disjoint categories. The lower approximation is a description of the domain objects which are known with certainty to belong to the subset of interest whereas the upper approximation is a description of the objects which possibly belong to the subset. The approximations are constructed with regard to a particular subset of attributes or features. RST is a mathematical tool for approximate reasoning for decision support and is particularly well suited for classification of objects. It can also be used for feature selection and feature extraction. In rough set theory the data is represented as a table, called decision table. Rows of the decision table correspond to objects and columns correspond to attributes. The class label is known as the decision attribute and the rest of the attributes known as the condition attributes. The basic concept of the RST is the notion of approximation space which is an ordered pair:

$$A = (U, R)$$

Where:

U = Nonempty set of objects, called universe

R = Equivalence relation on U called indiscernibility relation. If x, y$\in$U and xRy then x and y are indistinguishable in A

Let X be a subset of U, i.e., X$\subseteq$U. R(x) denote the equivalence class of R determined by element x. The lower approximation of a set X with respect to R and denoted by $R_*(X)$:

$$R_*(X) = \{x: R(x) \subseteq X\}$$

The upper approximation of a set X with respect to R and denoted by $R^*(X)$:

$$R^*(X) = \{x: R(x) \cap X \neq \phi\}$$

The set of all objects which can be decisively classified neither as members of X nor as members of -X with respect to R is called the boundary region of a set X with respect to R and denoted by $RN_R(X)$:

$$RN_R(X) = R^*(X)\text{-}R^*(X)$$

The lower approximation of a set is union of all granules which are entirely included in the set; the upper approximation is union of all granules which have non-empty intersection with the set; the boundary region of a set is the difference between the upper and the lower approximation of the set. The following are the four basic classes of rough sets:

- A set X is roughly R-definable, iff $R_*(X) \neq \phi$ and $R^*(X) \neq U$
- A set X is internally R-undefinable, iff $R_*(X) = \phi$ and $R^*(X) \neq U$
- A set X is externally R-undefinable, iff $R_*(X) \neq \phi$ and $R^*(X) = U$
- A set X is totally R-undefinable, iff $R_*(X) = \phi$ and $R^*(X) = U$

RST classifies all the attributes into three categories: core attributes, reduct attributes and dispensable attributes. Core attributes have the essential information to make correct classification for the data set and should be retained in the data set; dispensable attributes are the redundant ones in the data set and should be eliminated and reduct attributes are in the middle between. Depending on the combination of the attributes in some cases, a reduct attribute is not necessary while in other situations it is essential.

RST can be used to combine the similar attributes and to reduce the number of attributes. So, it can increase the processing speed and raises the detection rate.

Support vector machines: The support vector machines was initially proposed by Burges (1998). SVMs are a set of related supervised learning methods used for classification. 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. The training data is represented as:

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

Where:

$(x_i, y_i),\ldots, (x_n, y_n)$ = A train data
n = The numbers of samples
m = The input vector
y = Fits into the category of +1 or -1

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 written as:

$$f(x) = \text{sgn}(w.x+b) = \text{sgn}\left(\sum_i^N \mu_i y_i (x_i,x)+b\right)$$

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 $\alpha_i = 0$.

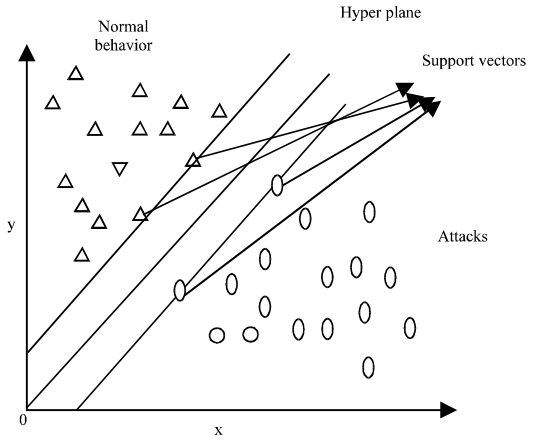

Fig. 1: Hyper plane of SVM

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.

Proposed IDS architecture: Figure 2 shows the conceptual architecture of proposed IDS. The architecture consists of the following components: data collection module, data reduction module, training and classification module.

Data collection module: The data collection module collects the audit data from MAC and network layers to profile 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, researchers want to select the trace data that bears evidence of normality or anomaly. Normal profile is

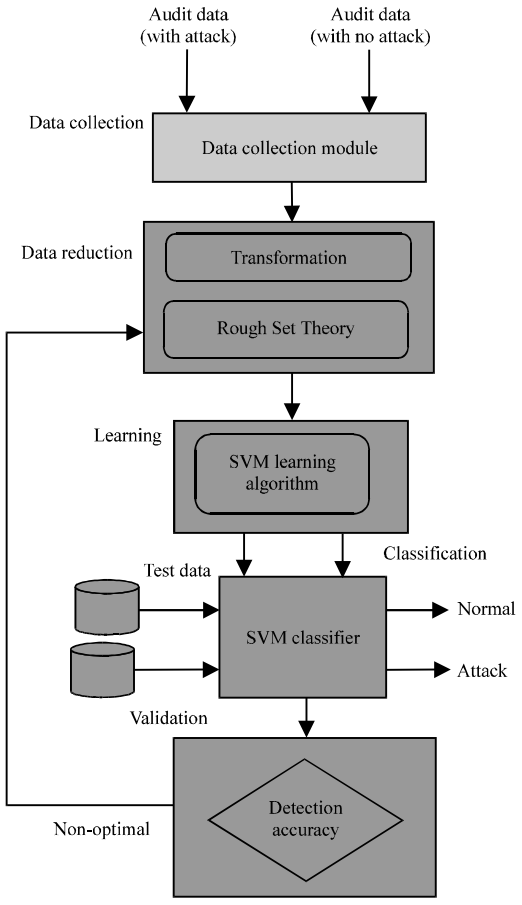

Fig. 2: Architecture of proposed IDS

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 (AODV) routing protocol for collecting the routing behavior. List of important cross layer features are shown in Table 1.

Data reduction module: In data reduction module there are two processes namely transformation and feature selection. Transformation converts the audit data into packet data. The collected audit data is large in size and difficult to understand. Some of the collected features are redundant and uninformative. Selecting the correct set of features is an important step in the classification process. Therefore, the essential features are selected and redundant information is eliminated by applying rough set theory.

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. Given a set of training examples a SVM training algorithm builds a model that predicts whether a new example falls into one category or the other. 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.

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:

$$f(x) = \text{sgn}\left(\sum_{0}^{Ns} \alpha_i y_i K(x_i, x)\right) + b$$

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.

Table 1: List of cross layer features

Layers	Features
MAC	RTS, CTS, DATA and ACK
Network	Routing control packets (RREQ, RREP, RERR and Hello)
	Route table changes (Number of neighbors, Added routes, Deleted routes, etc.)
	Data control packets (data)

RESULTS AND DISCUSSION

To validate the efficiency of the proposed IDS Model attacks are simulated with varying network conditions under Linux environment using Network Simulator (NS-2). 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. There are 13 different scenarios: five in varying mobility conditions, four in varying traffic density and four in varying 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.

In this research one of the most popular reactive routing protocol of a MANET, Ad hoc On Demand Distance Vector (AODV) is used. AODV (Perkins *et al*., 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 (Ning and 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.

Table 2: NS-2 Attack simulation setup with varying network conditions

Parameters	Values
Routing protocol	AODV
Simulation duration	1000 sec
Topology	1000×500 m
Number of mobile nodes	50
Transmission range	250 m
Mobility model	Random waypoint model
Traffic type	CBR/UDP
Data payload	512 bytes
Number of connections	5, 10, 15 and 20
Maximum speed	10 m sec^{-1}
Number of malicious nodes	5, 10, 15 and 20
Pause time	0, 20, 40, 60 and 80
Attack duration	2-50 sec

The size of audit data is reduced using rough set theory. Implementing rough set operations ROSETTA a data mining tool, invented by Ohrn and Komorowski (1997) is used. The algorithm used by ROSETTA library supports two categories of discernibility:

- Full: in this category of discernibility, reducts are selected relative to the system as a whole
- Objects: in this category of discrenibility, reducts are selected relative to a single object. There are four algorithms, namely Johnson's, Genetic, Holte's and Manual reducer. The proposed IDS interested in Genetic Algorithm, it gives less number of reducts as compared to other algorithms

The node mobility is varied and how mobility affects the detection rate is studied. Similarly, by varying the traffic density and number of malicious nodes is experimented and the effect of these conditions over detection efficiency is studied. LIBSVM tool is used for the SVM operations. For each scenario, five individual runs with different network conditions are performed. To measure the performance there are three metrics used in the evaluation 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.

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.

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 that false positive rate, false negative rate decreases 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.

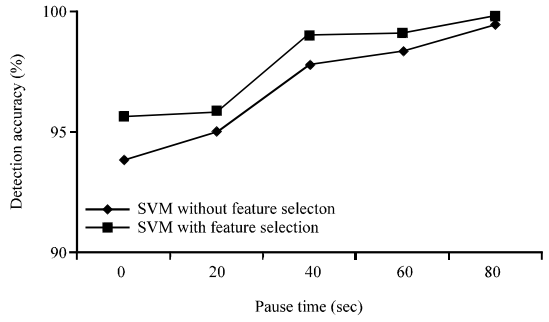

Fig. 3: Pause time vs. detection accuracy

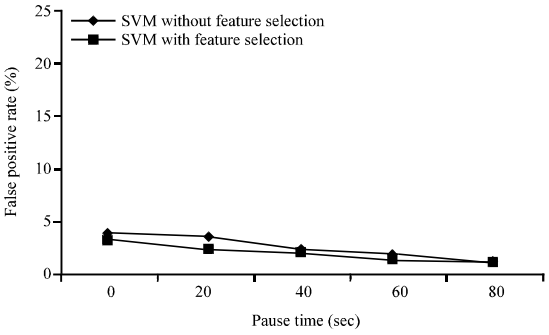

Fig. 4: Pause time vs. false positive rate

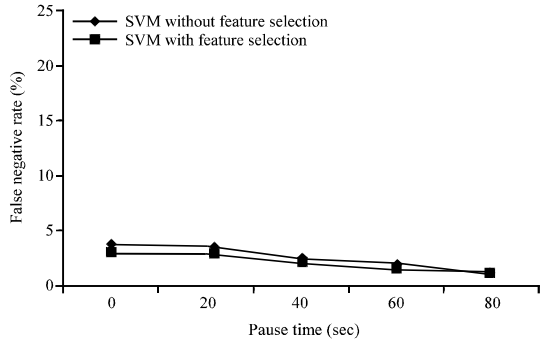

Fig. 5: Pause time vs. false negative rate

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

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 sec 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

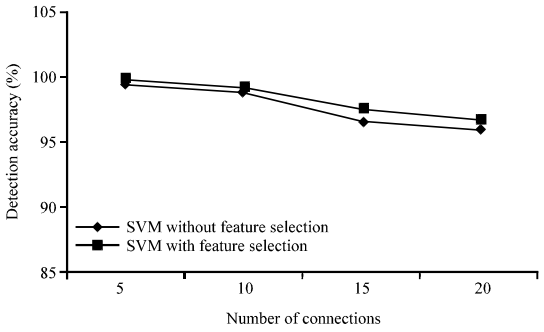

Fig. 6: Number of connections vs. detection accuracy

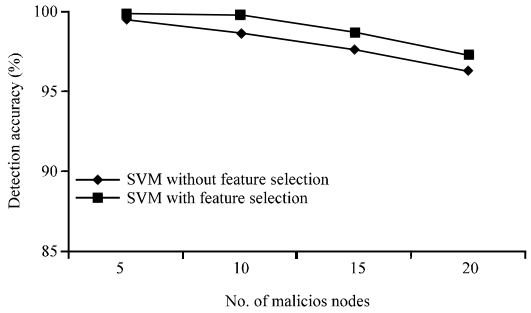

Fig. 7: Number of malicious nodes vs. detection accuracy

Table 3: Detection accuracy of the proposed IDS

Attack types	Results with all features (%)	Results with rough set feature selection (%)
Route disruption	96.86	97.84
Route invasion	96.23	97.27
Node isolation	96.36	97.33
Resource	96.03	96.90

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.

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 sec 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 detection accuracy of the cross layer IDS with all features and the cross layer IDS with rough set feature selection for the simulated attacks.

Results indicates that the performance of feature selection achieve better accuracy. Considering all the scenarios, it is clear that the proposed IDS Model achieves better accuracy.

CONCLUSION

In this research, researchers have presented an effective cross-layer based anomaly detection system which trains a normal profile from features collected from both MAC layer and network layer. Two machine learning algorithms support vector machines and rough set are used for profile training and intrusion detection. The efficiency is analyzed with varying network conditions by simulating four attacks. In this research, rough set reduces the size of feature that reduces the complexity of SVM. Experimental result shows that the detection accuracy of IDS with selected features increased by 1%.

RECOMMENDATIONS

The proposed IDS Method is limited to local system. To extend this research, in future, researchers would examine optimal solution to deploy such intrusion detection to provide a Distributed and Cooperative Intrusion Detection System. Also, researchers will investigate the feasibility of implementing this technique in real time test bed with all prominent attacks of mobile ad hoc networks.

REFERENCES

Abdel-Fattah, F., Z.M. Dahalin and S. Jusoh, 2010. Dynamic intrusion detection method for mobile ad hoc network using CPDOD algorithm. IJCA Special Issue MANETs, 1: 22-29.

Bu, S., F.R. Yu, X.P. Liu, P. Mason and H. Tang, 2011. Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. IEEE Trans. Veh. Technol., 60: 1025-1036.

Burges, C.J.C., 1998. A tutorial on support vector machines for pattern recognition. Data Mining Knowl. Discov., 2: 121-167.

Chen, R.C., K.F. Cheng and C.F. Hsieh, 2009. Using rough set and support vector machine for network intrusion detection. Proceedings of the 1st Asian Conference on Intelligent Information and Database Systems, April 1-3, 2009, Dong Hoi, pp: 465-470.

Joseph, J.F.C., B.S. Lee, A. Das and B.C. Seet, 2011. Cross-layer detection of sinking behavior in wireless ad hoc networks using SVM and FDA. IEEE Trans. Dependable Secure Comput., 8: 233-245.

Liu, Y., Y. Li and H. Man, 2005. Short paper: A distributed cross-layer intrusion detection system for ad hoc networks. Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, September 5-9, 2005, Baltimore, Maryland, pp: 418-420.

Mishra, A., K. Nadkarni and A. Patcha, 2004. Intrusion detection in wireless ad hoc networks. IEEE Wireless Communicat., 11: 48-60.

Mohammed, N., H. Otrok, L. Wang, M. Debbabi and P. Bhattacharya, 2011. Mechanism design-based secure leader election model for intrusion detection in MANET. IEEE Trans. Dependable Secure Comput., 8: 89-103.

Nakayama, H., S. Kurosawa, A. Jamalipour, Y. Nemoto and N. Kato, 2009. A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. IEEE Trans. Vehicular Technol., 58: 2471-2481.

Ning, P. and K. Sun, 2003. How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols. Proceedings of the Systems, Man and Cybernetics Society on Information Assurance Workshop, June 18-20, 2003, IEEE Computer Society, USA., pp: 60-67.

Ohrn, A. and J. Komorowski, 1997. A rough set toolkit for analysis of data. Proceedings of the 3rd Joint Conference on Information Sciences, Volume 3, March 11-14, 1997, Burlingame, CA., pp: 403-407.

Parthalain, N.S.M., 2009. Rough set extensions for feature selection. Ph.D. Thesis, Department of Computer Science, Aberystwyth University, Aberystwyth, United Kingdom.

Pastrana, S., A. Mitrokotsa, A. Orfila and P. Peris-Lopez, 2012. Evaluation of classification algorithms for intrusion detection in manets. Knowl. Based Syst., 36: 217-225.

Pawlak, Z., 1998. Some Issues on Rough Sets. In: Transactions on Rough Sets I, Peters, J.F. and A. Skowron (Eds.). Springer, New York, pp: 1-58.

Perkins, C., E. Belding-Royer and S. Das, 2003. Ad hoc On-Demand Distance Vector (AODV) routing. Network Working Group, Request for Comments: 3561 July 2003. http://www.ietf.org/rfc/rfc3561.txt.

Sen, S. and J.A. Clark, 2011. Evolutionary computation techniques for intrusion detection in mobile ad hoc networks. Comput. Networks, 55: 3441-3457.

Shrivastava, K.S. and P. Jain, 2011. Effective anomaly based intrusion detection using rough set theory and support vector machine. Int. J. Comput. Appl., 8: 35-41.

Tsai, C.F., Y.F. Hsu, C.Y. Lin and W.Y. Lin, 2009. Intrusion detection by machine learning: A review. Exp. Syst. Appl., 36: 11994-12000.