International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 28811-28827

http://www.ripublication.com

GA Trained Classification For Behavior Based Anomaly Detection in the MANETS

S.R .SEENIVASAN

ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER APPLICATIONS (MCA)
K.L.N. COLLEGE OF INFORMATION TECHNOLOGY
POTTAPALAYAM - 630612
SIVAGANGAI DISTRICT
TAMILNADU
INDIA

DR. M. GANAGA DURGA

ASSISTANT PROFESSOR
GOVERNMENT COLLEGE OF ARTS AND SCIENCE FOR WOMEN
SIVAGANGAI
TAMAILNADU
INDIA

Abstract

Anomalous behavior detection is an important measure to counter act the security breaches in the MANETS. This paper proposes an approach which uses the evolutionary algorithm to train the classifier to detect the anomaly. The environment is simulated using the GloMoSim simulator to depict the MANET environment. The dataset is created for three attacks. Then this dataset is analyzed using the proposed approach. The experimental analysis shows that the proposed approach is performing better than the benchmark algorithm. The results are discussed. The future work must be concentrated on tweaking the classifier for improving the results.

Keywords: MANET, Intrusion detection, Classification, Genetic Algorithm, etc.

Introduction

Mobile phone applications are widespread in the day to day life. Many of the users are highly depended on the mobile phone applications. The backbone of the mobile phone applications are the mobile network. The mobile network is highly ad hoc in nature. This nature of the mobile network is highly vulnerable to the security issues. Mobile security is a thrust area where numerous works are going on.

The topology of the mobile network frequently changes because of their mobility nature. Security breaches are highly expected in the mobile ad hoc networks. Because of this inherent property of the mobile networks security measures should be give due interest. Standard information security measures such as encryption and authentication do not provide complete protection, and, therefore, intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs [1].

The flexibility of the network in turn gives a major flow for the security in the network. The proactive mechanism should be employed for the security breaches. Intrusion detection is used in the networks by comparing the set of baselines of the system with the present behavior of the system [2]. Intrusion detection is one of key techniques behind protecting a network against intruders. An Intrusion Detection System tries to detect and alert on attempted intrusions into a system or network, where an intrusion is considered to be any unauthorized or unwanted activity on that system or network [3]. There are two major analytical techniques in intrusion detection, namely misuse detection and anomaly detection. Misuse detection uses the "signatures" of known attacks [4].

In this paper we have used a behavior based anomaly detection using the evolutionary tuned classification. The evolutionary algorithm employed in this paper for the training of the classification purpose is the Genetic Algorithm (GA). GA is good for searching in the large space. Here GA is made to identify the sequences which are used to identify any anomalies. Further ID3 classification algorithm is employed for the classification for the intrusion detection.

In this paper next section is employed for the background study required for this paper. Section 3 talks about various methodologies proposed by other researchers in this research area. Section 4 deals with the problem that has been formulated in this paper. Section 5 clearly describes the proposed algorithm in this paper. Section 6 discuss about the experimental set up details under which the research analyzed in this paper. Section 7 shows the results obtained out of the experiment carried out and the discussions on the results. Section 8 gives the conclusion about this paper.

Background Study

This paper deploys a model for the anomaly detection for the Mobile ad-hoc networks. In this paper we have used the evolutionary trained classification algorithm for the anomaly detection in the mobile ad-hoc network. In this section we will discuss about the Mobile adhoc networks, Anomaly detection, classification, Genetic algorithms.

Mobile Ad-Hoc Networks

Opposed to infra structure wireless networks, where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET, does not rely on a fixed infrastructure for its operation [5]. The characteristics of the MANETS are listed below

- Autonomous and infrastructure less
- Multi-hop routing
- Dynamic network topology
- Device heterogeneity
- Energy constrained operation
- Bandwidth constrained variable capacity links
- Limited physical security
- Network scalability
- Self-creation, self-organization and self-administration

Securing wireless ad hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Ad hoc networks have to cope with the same kinds of vulnerabilities as their wired counterparts, as well as with new vulnerabilities specific to the ad hoc context The complexity and diversity of the field (different applications have different security constraints) led to a multitude of proposals that cannot be all surveyed in this article. Detailed analyses of ad hoc networking security issues and solutions can be found in. Below we summarize only the main directions of security in ad hoc networks. Active attacks involve actions such as the replication, modification and deletion of exchanged data. Certain active attacks can be easily performed against an ad hoc network. These attacks can be grouped in: Impersonation, Denial of service, and Disclosure attack [6].

Anomaly Detection

Anomaly Detection is an important alternative detection methodology that has the advantage of defending against new threats not detectable by signature based systems. In general, anomaly detectors build a description of normal activity, by training a model of a system under typical operation, and compare the normal model at run time to detect deviations of interest. Anomaly Detectors may be used over any audit source to both train and test for deviations from the norm [7]. The goal of the anomaly detection is to find all objects that are different to other objects. Anomaly detection finds extensive use in a wide variety of applications such as fraud detection for credit cards, insurance or health care, intrusion detection for cyber-security, fault detection in safety critical systems, and military surveillance for enemy activities [8].

Classification

Classification is used to learn a model (classifier) from a set of labeled data instances (training) and then, classify a test instance into one of the classes using the learnt model (testing). Classification based anomaly detection techniques operate in a similar two-phase fashion. The training phase learns a classifier using the available

labeled training data. The testing phase classifies a test instance as normal or anomalous using the classifier [9].

The basic idea to use classification algorithms for the intrusion detection is that a classifier is used to distinguish between the normal and anomalous behavior classes in the given dataset. The classifier is trained and the task could be done by the detection of the abnormality which is defined in the training set.

The advantages of classification based techniques are as follows [10] :

- Classification based techniques, especially the multi-class techniques, can make use of powerful algorithms that can distinguish between instances belonging to different classes.
- The testing phase of classification based techniques is fast since each test instance needs to be compared against the pre-computed model.

The disadvantages of classification based techniques are as follows:

- Multi-class classification based techniques rely on availability of accurate labels for various normal classes, which is often not possible.
- Classification based techniques assign a label to each test instance, which can also become a disadvantage when a meaningful anomaly score is desired for the test instances. Some classification techniques that obtain a probabilistic prediction score from the output of a classifier, can be used to address this issue

Genetic Algorithms

Genetic algorithms (GAs), a form of inductive learning strategy, are adaptive search techniques which have demonstrated substantial improvement over a variety of random and local search methods [11]. This is accomplished by their ability to exploit accumulating information about an initially unknown search space in order to bias subsequent search into promising subspaces. Since GAs are basically a domain independent search technique, they are ideal for applications where domain knowledge and theory is difficult or impossible to provide [12].

Other Methodologies Involved

Hall et al. [13] propose Anomaly Based Intrusion Detection (ABID), a semi-supervised IDS that uses a machine learning technique (Instance Based Learning) and is based on mobility profiles. The authors point out an IDS based on mobility is particularly effective against node capture attacks because the thief will likely have a different movement pattern than the owner. Two controls parameterize their system: precision level (PL) enlarges or constrains the granularity of the location data (digits of precision used from latitude/longitude), and sequence length (SL) extends or reduces the size of tracks under analysis. ABID classifies test data that is too similar to the training data as anomalous in order to counter a profile replay attack. The con of this study is the extremely long training phase: up to six months. The authors focus on replay and node capture attacks.

Li et al. [14] propose a cross layer behavior based IDS using neural networks called Host based Multi-level Behaviour Profiling Mobile IDS (HMBPM). They

prosecute application layer features such as URL visited, network layer features such as packets transmitted and machine layer features such as microprocessor load. Li et al. establish three Radial Basis Function neural nets for analysis:

one each for call details, device usage and Bluetooth activity; the Multi-Level Behaviour Selector changes the neural net feature set over time as the behavior pattern changes. The con of this study was the error rate which is as high as 36.4%. The authors focus on spoofing and node capture attacks.

Samfat and Molva [15] propose a multitrust IDS called Intrusion Detection Architecture for Mobile Networks (IDAMN) that runs in real-time (it can detect an intruder while a call is in progress) and distributes computation hierarchically. The authors minimize the amount of profile data which enhances privacy and prevents profile replay attacks. IDAMN uses three techniques to detect intrusions: studying user velocity to detect clones, looking for disparity between switch/base station activity and user density and comparing user behavior with user profile. IDAMN user profiles For the call details component of the user profile, IDAMN weights recent data more heavily than older data. For the mobility component of the user profile, IDAMN weights frequent itineraries more heavily than rare itineraries. The pro of this study is the false positive rate which ranges from 1 to 7%. The con of this study is the detection rate which is as low as 60%. These results are counterintuitive: generally, anomaly detection techniques have weak false positive rates and excellent detection rates. The authors focus on spoofing and node capture attacks.

Problem Formulation

There is a definite need for Intrusion detection systems that will improve security and use fewer resources on the mobile phone. The existing approaches suffer from the factors like, it is designed for the wired network and doesn't take the considerations of the mobile networks. The mobile networks vary in the ease of hackers to intrude in to the network. The device itself has the security threat of the misplacement or explicit steeling. Thus the security in this concern is a thrust area for research. The research scope is to design the intrusion detection mechanism for the mobile network.

The intrusion detection technique is basically depends on the data received from monitoring the network and the nodes participating in it. The data could be from the host based or the network based. Intrusion detection system is a passive method. It just monitors the information over network or hosts and raises alarms when any intrusion happens. But data mining based ids can identify these data when it arrives and forecast it on its own, thus by gaining the function of active approach [16]. In [17] the intrusion detection technique for the network security is proposed by the supervised learning mechanism. Here the supervised learner classifiers learns the collected historical and log data then builds a predictive model in order to identify the intruders. The algorithm proposed in [16] reduces the space occupied by the dataset, which would be useful for the network administrator/manager to avoid the delay between the arrival and detection time of the attacks respectively.

The mobile network security could be implemented by the using the supervised learning and then the predictive framework is built. This framework further predicts and detects the attackers and hackers. The knowledge about these attacks is acquired from the huge volume of network data with data mining tools. This knowledge

facilitates the security system to identify the attackers or hackers based on their behavior in a network. The behavior of the attackers and hackers are studied and identified by two types of learning strategies namely supervised and unsupervised learning.

Proposed Approach

The proposed approach is clearly illustrated with the framework shown below. The dataset is built for the system using the simulation which is described in section 6. The GA is employed as the searching technique for the feature extraction, which could facilitate in classification problem to overcome the disadvantages of the classifications mentioned in section 2.3.

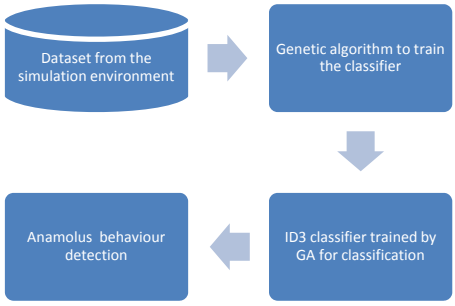

Figure 1: Frame work of the proposed approach

The algorithm employed in this paper is described in the following section. The algorithm consists of two phases where, in the first phase GA is used for sequence extraction and in the next phase the classifier is described.

Proposed Algorithm

Input: Dataset for consideration

Phase I: Genetic algorithm for the sequence extraction to train the classifier

a. Initialize the chromosomes with the subsequences
b. Selection from the population in a random manner for reproduction
c. Crossover the chromosomes selected
d. Apply mutation based on the probability
e. Evaluate the off springs for the feature selection from the subsequences

Phase II: Multi class classifier trained by genetic algorithm

/* ID3 algorithm to build the decision tree trained by Genetic algorithm

Step 2(a) Tree construction

a. choose one attribute as the root with highest information gain and put all its values as branches

b. choose recursively internal nodes (attributes) with their proper values as branches.
c. Stop when
    - all the samples (records) are of the same class, then the node becomes the leaf labeled with that class
    - or there is no more samples left
    - or there is no more new attributes to be put as the nodes. In this case we apply MAJORITY VOTING to classify the node.

Step 2(b) Tree pruning

- Identify and remove branches that reflect noise or outliers

Output: Multi Class classified dataset for anomaly detection

The algorithm provides the clear detail of the working of the proposed approach. The algorithm is tested on various dataset and the results are tabulated in section 7. The experimental details are described in the next section.

Experimental Details

GloMoSim simulator [18] provides a scalable simulation environment for large wireless and wireline communication networks. Its scalable architecture supports up to thousand nodes linked by a heterogeneous communications capability that includes multi-hop wireless communications using ad-hoc networking.

The incorporation of misbehavior into the network is the same as done in [19]. We reiterate for clarity. The nodes can be set to misbehave as a Boolean parameter. It can be set or reset. Using this implementation capability we could have different numbers of misbehavior set up (In our experiments, 5 10 and 20 were involved). The structured GA as employed in [20] is used for the detection. Tables 1 and 2 define the parameters for the simulation environment.

Table 1: Parameters of The Simulation System

System parameters	**Values in the simulation system**
Routing protocol	DSR
Simulation area in meters	800x1000
Number of nodes	40
Radio range	380 m
Mobility model	Random way point
Mobility speed (number of pauses)	1m/s
Misbehaving nodes	5,10,20
Traffic type	Telnet, CBR
Payload size	512 bytes
Frequency/rate	0.2-1s
Radio-Bandwidth/link speed	2 Mbps

Table 2: Parameters of The Intrusion Detection In The Simulation System

System parameters	**Values in the simulation system**
Upper limit for Events sequence sets of a Monitored Node for learning	500
Number of subsequences in a sequence set	4
Upper limit for the number of events in a sequence set	40
Upper limit time for a sequence set collection	10 s
Misbehavior probability	0.8
Learning data threshold	0.001 - 0.1
Threshold for detection (% of Detection rate or true positive)	0.25
Mutation probability	0.05-0.1
Crossover probability	0.6
Normalized space range	[0.0, 1.0]
Number of dimensions	4, 2

Dataset Description

In this experiment dataset based on three attacks are produced. The three attacks considered are

Black Hole Attack

A black hole problem means that one malicious node utilizes the routing protocol toclaim itself of being the shortest path to the destination node, but drops the routing pack-ets but does not forward packets to its neighbors [21]. A single black hole attack is easilyhappened in the mobile ad hoc networks [22]. These nodes use their resource and aims to weaken other nodes or whole network by trying to participate in all established routes thereby forcing other nodes to use a malicious route which is under their control.

Selfish Dropping of Packets Attack

Nodestake participation in the route discovery and route maintenance phases but refuses to forward data packets to save its resources [23]. This node produces the selfish dropping of packets attack.

Modification of Routes Attack

In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called „wormhole link“ . They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network [24].

The dataset have been generated based on the following table description. The number of misbehaving nodes varies from 5, 10, 15. The learning rate is differed as 0.001, 0.002, 0.005, 0.01.

Table 3: Black Hole Dataset Description

Name of the Dataset	Type of Attack	Number of Misbehavior nodes	Learning Rate
BH1	Black hole	5	0.001
BH2	Black hole	5	0.002
BH3	Black hole	5	0.005
BH4	Black hole	5	0.01
BH5	Black hole	10	0.001
BH6	Black hole	10	0.002
BH7	Black hole	10	0.005
BH8	Black hole	10	0.01
BH9	Black hole	15	0.001
BH10	Black hole	15	0.002
BH11	Black hole	15	0.005
BH12	Black hole	15	0.01

Table 4: Dropping of packets Dataset description

Name of the Dataset	Type of Attack	Number of Misbehavior nodes	Learning Rate
DP1	Dropping of Packet	5	0.001
DP2	Dropping of Packet	5	0.002
DP3	Dropping of Packet	5	0.005
DP4	Dropping of Packet	5	0.01
DP5	Dropping of Packet	10	0.001
DP6	Dropping of Packet	10	0.002
DP7	Dropping of Packet	10	0.005
DP8	Dropping of Packet	10	0.01
DP9	Dropping of Packet	15	0.001
DP10	Dropping of Packet	15	0.002
DP11	Dropping of Packet	15	0.005
DP12	Dropping of Packet	15	0.01

Table 5: Modification of routes Dataset description

Name of the Dataset	Type of Attack	Number of Misbehavior nodes	Learning Rate
MR1	Modification of routes	5	0.001
MR2	Modification of routes	5	0.002
MR3	Modification of routes	5	0.005
MR4	Modification of routes	5	0.01
MR5	Modification of routes	10	0.001
MR6	Modification of routes	10	0.002
MR7	Modification of routes	10	0.005
MR8	Modification of routes	10	0.01
MR9	Modification of routes	15	0.001
MR10	Modification of routes	15	0.002
MR11	Modification of routes	15	0.005
MR12	Modification of routes	15	0.01

Performance Metrics

The performance metrics used for comparison is listed as below

TPR (Total positive Rate)

The true-positive rate is also known as sensitivity. Itis the proportion of positive cases that were correctly identified. It is defined by the following equation

$$TPR = \frac{TP}{TP + FN}$$

FPR (False Positive Rate)

It is the proportion of negatives cases that were incorrectly classified as positive, as calculated using the equation.

$$FPR = \frac{FP}{FP + TN}$$

Accuracy

It is the proportion of the total number of predictions that were correct. It is determined using the equation

$$Accuracy = \frac{TP + TN}{(TP + FN) + (FP + FN)}$$

Where

TP = True positive = correctly identified

FP = False positive = incorrectly identified

TN = True negative = correctly rejected

FN = False negative = incorrectly rejected

Results and Discussions

The results obtained by conducting the experiment is shown in the following tables and graphs

Table 6: Results obtained from ID3 for Black hole dataset

ID3 classification Algorithm			
Dataset	TPR	FPR	Accuracy
BH1	0.732	0.354	0.745
BH2	0.764	0.362	0.758
BH3	0.756	0.386	0.725
BH4	0.784	0.327	0.765
BH5	0.768	0.314	0.784
BH6	0.759	0.362	0.765
BH7	0.791	0.385	0.786
BH8	0.762	0.365	0.758
BH9	0.754	0.326	0.727
BH10	0.769	0.341	0.783
BH11	0.788	0.328	0.746
BH12	0.792	0.366	0.735

Table 7: Results obtained from Proposed for Black hole dataset

Proposed Algorithm			
Dataset	TPR	FPR	Accuracy
BH1	0.751	0.347	0.756
BH2	0.782	0.356	0.789
BH3	0.765	0.374	0.769
BH4	0.795	0.331	0.798
BH5	0.774	0.308	0.776
BH6	0.762	0.358	0.768
BH7	0.796	0.376	0.801
BH8	0.768	0.358	0.775
BH9	0.763	0.319	0.768
BH10	0.781	0.335	0.789
BH11	0.794	0.321	0.799
BH12	0.796	0.357	0.802

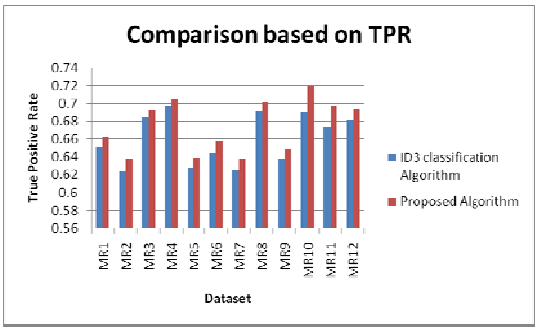

Figure 2: Comparison based on TPR for Black hole dataset

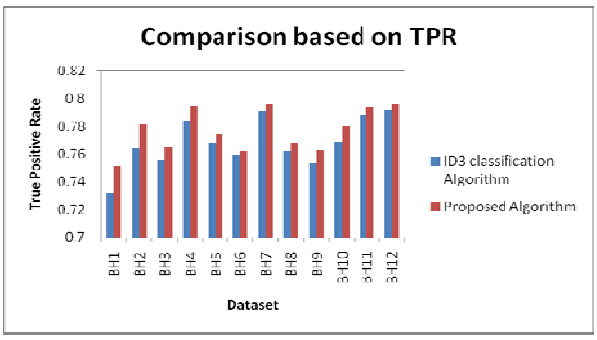

Figure 3: Comparison based on TPR for Black hole dataset

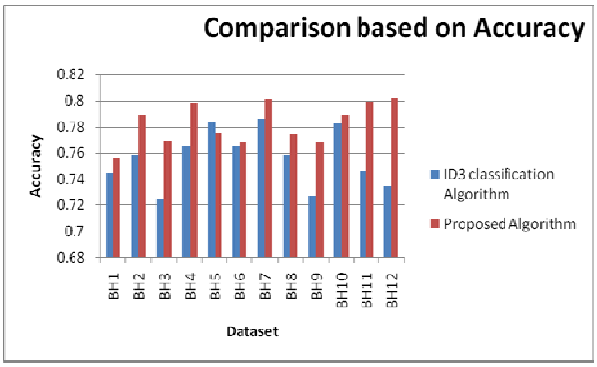

Figure 4: Comparison based on Accuracy for Black hole dataset

Table 8: Results obtained from ID3 for Selfish packet dropping dataset

ID3 classification Algorithm			
Dataset	TPR	FPR	Accuracy
DP1	0.765	0.362	0.77
DP2	0.787	0.374	0.791
DP3	0.75	0.382	0.781
DP4	0.758	0.329	0.761
DP5	0.789	0.346	0.794
DP6	0.756	0.329	0.763
DP7	0.785	0.368	0.796
DP8	0.752	0.361	0.768
DP9	0.749	0.395	0.756
DP10	0.781	0.328	0.794
DP11	0.732	0.384	0.741
DP12	0.794	0.354	0.805

Table 9: Results obtained from Proposed algorithm for Selfish packet dropping dataset

Proposed Algorithm			
Dataset	TPR	FPR	Accuracy
DP1	0.771	0.354	0.79
DP2	0.786	0.362	0.806
DP3	0.786	0.376	0.792
DP4	0.762	0.318	0.775
DP5	0.779	0.336	0.786
DP6	0.764	0.314	0.772
DP7	0.789	0.358	0.797
DP8	0.765	0.354	0.779
DP9	0.754	0.335	0.768
DP10	0.795	0.319	0.806
DP11	0.748	0.376	0.756
DP12	0.802	0.349	0.813

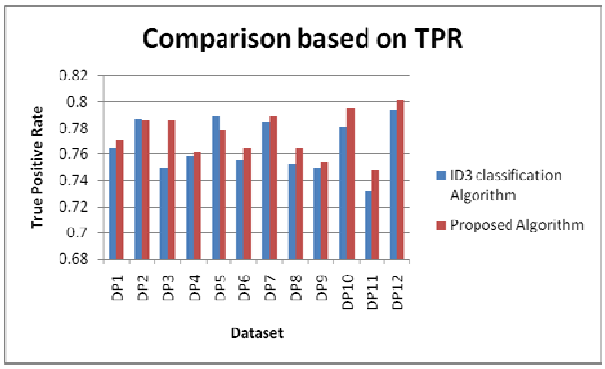

Figure 5: Comparison based on TPR for Selfish packet Dropping dataset

Figure 6: Comparison based on FPR for Selfish packet Dropping dataset

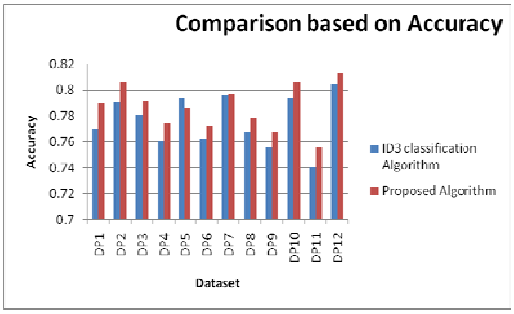

Figure 7: Comparison based on Accuracy for Selfish packet Dropping dataset

Table 10: Results obtained from ID3 for Modification of routes dataset

ID3 classification Algorithm			
Dataset	TPR	FPR	Accuracy
MR1	0.652	0.394	0.656
MR2	0.624	0.358	0.633
MR3	0.685	0.347	0.694
MR4	0.698	0.365	0.706
MR5	0.628	0.325	0.638
MR6	0.645	0.314	0.658
MR7	0.625	0.384	0.634
MR8	0.692	0.361	0.709
MR9	0.638	0.394	0.649
MR10	0.691	0.365	0.706
MR11	0.674	0.397	0.686
MR12	0.682	0.394	0.692

Table 11: Results obtained from proposed for Modification of routes dataset

Proposed Algorithm			
Dataset	TPR	FPR	Accuracy
MR1	0.663	0.386	0.678
MR2	0.638	0.364	0.645
MR3	0.693	0.329	0.708
MR4	0.706	0.359	0.719
MR5	0.639	0.316	0.646
MR6	0.659	0.309	0.668
MR7	0.638	0.376	0.642
MR8	0.702	0.358	0.716
MR9	0.649	0.382	0.658
MR10	0.719	0.358	0.724
MR11	0.698	0.357	0.719
MR12	0.695	0.386	0.705

Figure 8: Comparison based on TPR for Modification of routes dataset

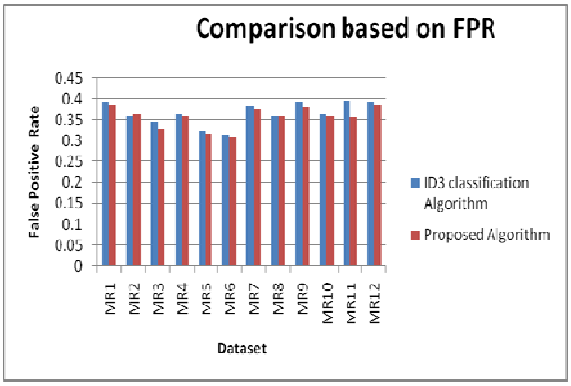

Figure 9: Comparison based on FPR for Modification of routes dataset

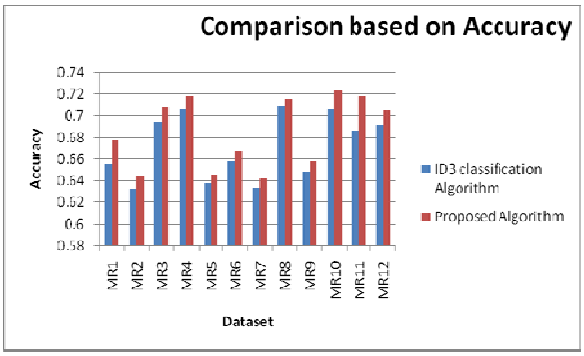

Figure 10: Comparison based on Accuracy for Modification of routes dataset

Conclusion

The proposed approach utilizes the genetic algorithm for finding the sequence in the dataset which facilitates the classification algorithm. This has been proved from the results illustrated in the section 7. MANETS are highly vulnerable to the security breaches because of its inherent features. This paper deploys a model for the Behavior based anomaly detection in the MANETS using the GA trained classifier. The misbehavior is simulated and the experimental results prove that the proposed method is better than the bench mark algorithm. The future work could be done to find the ways to fine tune the classifier, so as to increase the classifier accuracy.

References

[1] Nadeem, A.; Howarth, M.P., "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," Communications Surveys & Tutorials, IEEE , vol.15, no.4, pp.2027,2045, Fourth Quarter 2013.

[2] L. PremaRajeswari, R. Arockia Xavier Annie, A. Kannan, “ENHANCED INTRUSION DETECTION TECHNIQUES FOR MOBILE AD HOC NETWORKS”, IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007), Dec. 20-22, 2007. Pp.1008-101

[3] Oleg Kachirski, RatanGuha, “Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks”, Proceedings of the IEEE Workshop on Knowledge Media Networking (KMN’02) 0-7695-1778-1/02 $17.00 2002 IEEE.

[4] Y. Huang, W. Fan, W. Lee, and P. S. Yu, “Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalie s”, Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, 2003, pp. 478-487.

[5] http://cwi.unik.no/images/Manet_Overview.pdf

[6] Pradip Ghorpade Pravin Ghosekar Girish Katkar. Article: Mobile Ad Hoc Networking: Imperatives and Challenges. IJCA Special Issue on MANETs (3):153–158, 2010

[7] Salvatore J. Stolfo, Shlomo Hershkop, Linh H. Bui, Ryan Ferster, and Ke Wang, Anomaly Detection in Computer Security and an Application to File System Accesses, SMIS 2005, LNAI 3488, pp. 14–28, 2005

[8] Varun Chandola, Arindam Banerjee, and Vipin Kumar, "Anomaly Detection : A Survey", ACM Computing Surveys, Vol. 41(3), Article 15, July 2009.

[9] http://cucis.ece.northwestern.edu/projects/DMS/publications/AnomalyDetection.pdf

[10] Platt, J.2000. Probabilistic outputs for support vector machines and comparison to regularized likelihood methods. A. Smola, P. Bartlett, B. Schoelkopf, and D. Schuurmans, Eds. 61-74

[11] De Jong, K. "Learning with Genetic Algorithms : An overview," Machine Learning Vol. 3, Kluwer Academic publishers, 1988
[12] http://cs.gmu.edu/~eclab/papers/TAI92.pdf
[13] J. Hall, M. Barbeau, E. Kranakis, Anomaly-based intrusion detection using mobility profiles of public transportation users, in: International Conference on Wireless And Mobile Computing, Networking And Communications, vol. 2, Montreal, QC, Canada, 2005, pp. 17–24.
[14] F. Li, N. Clarke, M. Papadaki, P. Dowland, Behaviour profiling on mobile devices, in: International Conference on Emerging Security Technologies, Canterbury, UK, 2010, pp. 77–82.
[15] D. Samfat, R. Molva, Idamn: an intrusion detection architecture for mobile networks, IEEE J. Sel. Areas Commun. 15 (7) (1997) 1373–1380.
[16] G. V. Nadiammai, M. Hemalatha, An Enhanced Rule Approach For Network Intrusion Detection Using Efficient Data Adapted Decision Tree Algorithm, Journal Of Theoretical And Applied Information Technology, January 2013. Vol. 47 No.2
[17] D.Asir Antony Gnana Singh,E.Jebamalar Leavline, Data Mining In Network Security - Techniques & Tools: A Research Perspective, Journal Of Theoretical And Applied Information Technology, November 2013. Vol. 57 No.2
[18] https://wiki.cse.buffalo.edu/services/content/glomosim
[19] M. Kaniganti. "An Agent-Based Intrusion Detection System for Wireless LANs", Masters Thesis, Advisor: Dr. DipankarDasgupta. The University of Memphis, December 2003.
[20] T. V. P. Sundararajan, A. Shanmugam, Behavior Based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (2)
[21] http://www.hcis-journal.com/content/pdf/2192-1962-1-4.pdf
[22] Deng H, Li W, Agrawal DP (2002) Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine 40(10):70 – 75. doi: 10.1109/MCOM.2002.1039859
[23] http://ijcsi.org/papers/7-4-1-12-17.pdf
[24] Rutvij H. Jhaveri, Ashish D. Patel, MANET Routing Protocols and Wormhole attack against AODV, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010