

Development and Analysis of improvised TORA Routing Protocol based on Machine Learning Model for optimal Network Performance in MANETs

M V D S Krishna Murty¹, Dr.Lakshmi Rajamani²

¹M V D S Krishna Murty, Asst.Prof., Dept of CSE, MCET, Hyderabad, Research scholar -JNTUH, mkrishnamurty@gmail.com
²Dr. Lakshmi Rajamani, Prof.& Head(Retd.), Dept of CSE, Osmania University, Hyderabad, drlakshmiraja@gmail.com

Abstract – A MANET is a self configurable wireless ad-hoc network in which node mobility exists. Due to this flexibility many security threats can occur in the routing. So, in order to address this, the performance of IDS should be improvised. In this paper, a methodology is proposed based on Machine Learning (ML) algorithm in terms of accuracy and detection rate for IDS improvisation for TORA routing protocol.

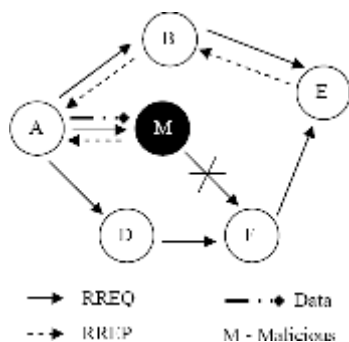
Key Words: MANET, Support Vector Machine, Intrusion Detection System, TORA (Temporally Ordered Routing Algorithm).

1. INTRODUCTION

IDS is to detect the attack before the malicious node(s) causes security threat to the network. It looks into monitoring, detecting and notifying aspects. The Blackhole attack is the most affected type on MANETs. Usage of an anomaly IDS protects the network from Black hole attack with the help of Machine Learning algorithm, SVM

1.1 Malicious Node(s) causing Black hole attack in TORA Routing Protocol.

Black hole attack is one of the major attacks in MANETs. Malicious Node(s) causing this attack on MANET security has the data viz. Source node, Destination node and Neighbouring node. The source node sends a QRY (Query Packet) to its neighbouring nodes to search for the route destination. However, black hole node sends a fake route reply to the source node resulting packet loss which will degrade the performance of the network. In order to prevent this, the performance of the IDS should be improvised with machine learning algorithm by detecting the malicious node(s).



Fig(1) : Malicious Node Causing Black hole Attack

2. RELATED WORK

Kwan Hui Lim et.al Proposed two modifications to improve TORA using a network localization approach and selective node participation approach. The network localization approach initializes and maintains a localized portion of the entire network while the selective node participation approach selects a subset of nodes to participate as part of the network

Pooja Rani et.al In this paper, the protection against dual attacks has been presented for BHA and GHA by using the concept of Artificial Neural Network (ANN) as a deep learning algorithm along with the swarm-based Artificial Bee Colony (ABC) optimization technique. The performance of the system has been increased by the selection of appropriate and best nodes for data packets transmission

Shweta Pandey et.al The proposed approach uses the Artificial neural network (ANN) and the Support Vector Machine (SVM) for the discovery of the black hole attacks in the network. The results are carried out between the black hole AODV and the security mechanism that was provided as the Secure AODV (SAODV), shows an improvement viz. energy consumption of 54.72%, throughput of 88.68kbps, packet delivery ratio of 92.91%, E to E delay of about 37.27ms

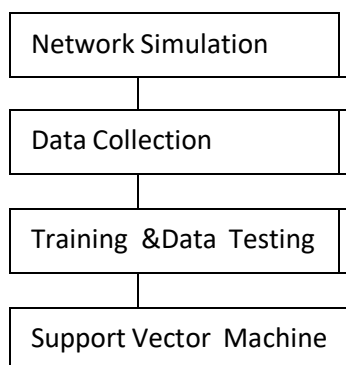
Indira N et.al Proposed Anomaly based intrusion detection technique using the SOM classification method provides higher detection rate than other anomaly detection method. As anomaly-based intrusion detection techniques are based on statistical data they can result in false positive identification of normal pattern as an attack. This false identification of benign behavior as abnormal can result in isolation of non-malicious node as malicious, thus may result in partitioning of the network

Sankaranarayanan.S et. al proposed RSA algorithm in intrusion detection system in MANET. It successfully identifies the malicious node(s) and results show that secure IDS method improvises packet deliver ratio in presence of malicious node(s).

Sujithra L et. al In this paper, the approach improves the conservation of energy in heterogenous network and also reduces the active time of IDS running in the nodes. In order to achieve this, probabilistic approach is implemented, here optimal probabilistic of node is to be set, thus decreases active time of IDS in each node and conserves the energy of the node, hence increases the network lifetime significantly.

3. PROPOSED METHODOLOGY

Nodes in the MANETs share the wireless medium and the topology of the network changes erratically and dynamically. Research in a MANET gets tremendous attention because of its eminent characteristics like instant infrastructure, easy deployment in hostile terrain where geographical conditions are not suitable viz. an earthquake, battlefield. MANET can be build anytime and anywhere. Since the nodes are mobile, the network topology varies rapidly. The remarkable advantages of MANETs such as multi hop, infrastructureless transmission etc., makes it as a best medium to networks. Though MANETs have surplus things, they have some security issues that will cause severe damages and loss in network. Random linking of mobile nodes leads to add malicious nodes in the network accidentally. To suspect and detect the malicious activity in the network, Intrusion Detection System (IDS) is implemented to analyze the behaviour of the neighbourhood nodes. To improve the anomaly based intrusion detection system in MANETs a Machine Learning approach, Support Vector Machine is taken into consideration.



Fig(2) : Flow Chart for the proposed methodology

A three step method is followed for the analysis-

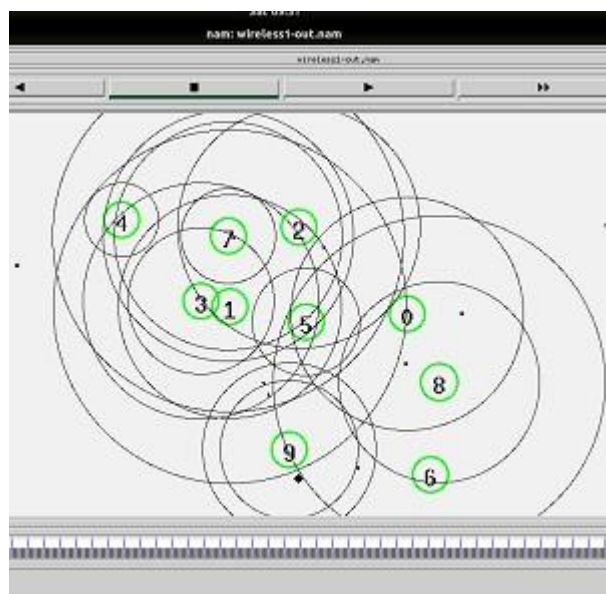
- i) Network Simulation
- ii) Data collection
- iii) Model Training & Data Testing.

Step-i) Network Simulation

Parameter	Value
Simulator	Ns-2.35
Simulation Time	50 Sec
Area	1000*1000 m
Node Energy	70 Joules
No. Of Nodes	10
No. Of Malicious Nodes	4,5,8,9
MAC Specification	802.11
Packet Size	1000
Routing Protocol	TORA

Table(1): Simulation Environment

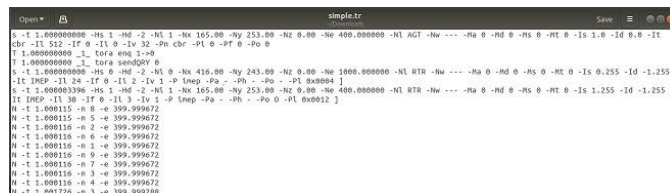
In the present work, Mobile Ad-hoc network(MANETs) is simulated in NS2 with 20 nodes as shown in fig(3).



Fig(3): Malicious Nodes causing Black hole attack simulation in NS-2.35 for TORA

Step-ii) Data Collection

After simulation, a trace file is generated from NS2 which will be an input for .CSV file. The output of trace file and input of .csv file are shown in Fig(4) and Fig(5) respectively. Generally, trace file has more number of attributes however, if the number of received packets are more than the number of dropped packets such kind of attributes have been selected as an input for .csv file



Fig(4): Trace file generated from Black hole attack simulation



	A	B	C	D	E	F
1	Node	X	Y	Energy	PktDrop	
2	1	165	253	49.3993	0	
3	3	125	261	49.2766	0	
4	3	125	261	49.2179	0	
5	3	125	261	49.17	0	
6	3	125	261	49.1502	0	
7	3	125	261	49.0495	0	
8	3	125	261	49.0396	0	
9	3	125	261	48.9961	0	
10	3	125	261	48.9609	0	
11	3	125	261	48.8618	0	
12	3	125	261	48.8084	0	
13	3	125	261	48.7338	0	
14	3	125	261	48.7011	0	
15	3	125	261	48.6913	0	
16	3	125	261	48.6088	0	
17	3	125	261	48.5989	0	
18	3	125	261	48.5873	0	
19	3	125	261	48.4467	0	
20	3	125	261	48.4352	0	
21	3	125	261	48.382	0	
22	3	125	261	48.3587	0	
23	3	125	261	48.1983	0	
24	3	125	261	48.1556	0	
25	3	125	261	48.1457	0	

Fig(5): Dataset generated from Trace file in .csv format

Step-iii) Model Training & Data Testing

In the present work SVM algorithm was used to train and test the data

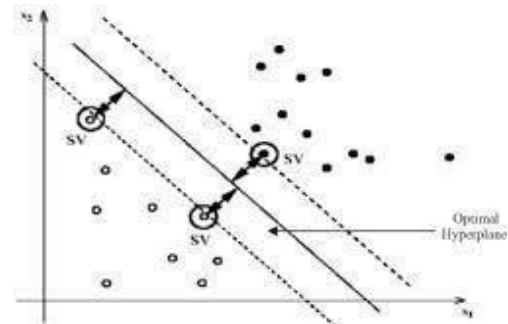
SVM(Support Vector Machine)

The primary aim of support vector machine(SVM) is to separate the normal and abnormal (i.e.malicious nodes) nodes by choosing the best estimated hyperplane . It is selected in such way that the distance from the hyperplane to the nearest node on each side is maximized.

Algorithm-

- i) Initialize Vector v and b to 0
- ii) Dataset $D = (x_1, y_1), \dots, (x_n, y_n)$, where x, y are labeled samples
- iii) Train SVM to learn decision function
- iv) For each sample of D do
Classify x_i using decision function $f(x_i)$
- v) If (function margin < 1) then Calculate w', b' for given data
- vi) Add sample example to known data
- vii) Use Eq. $(w) = \frac{1}{2} \|w'\|^2$ for reducing errors
- viii) Use Eq. $f(x) = \text{sign}(w^T x + b)$ to predict.
- ix) If (prediction is correct) then
Do it Again
- x) Else
Train SVM Again
Endif
- xi) Classify x_i as benign or malicious

In the present paper, the dataset obtained from NS2 is fed into SVM algorithm. The Malicious Node(s) causing black hole attack is detected in terms of accuracy and confusion matrix. The output is shown in Fig (9).



Fig(6): SVM Classification

```

MaliciousMovement.pyrb
File Edit View Insert Runtime Tools Help (Alt+Esc)
Code + Test
[1] Import pandas as pd
Import energy as hp
Import matplotlib.pyplot as plt
Import sklearn
[2] from google.colab import files
upload_files(upload)
NodeBehavior_TORA.csv (text/csv - 3433 bytes, last modified: 5/21/2022 - 100% done)
Saving NodeBehavior_TORA.csv to NodeBehavior_TORA.csv
[3] df=pd.read_csv("NodeBehavior_TORA.csv")
df[0:100]
Node X Y Energy PktDrop
294 5 273 232 42.3187 1
295 5 273 232 42.3076 1
296 5 273 232 42.2962 1
297 5 273 232 42.2864 1
  
```

Fig(7): Data Sampling in SVM

```

MaliciousMovement.pyrb
File Edit View Insert Runtime Tools Help (Alt+Esc)
Code + Test
NodeBehavior_TORA.csv (text/csv - 3433 bytes, last modified: 5/21/2022 - 100% done)
Saving NodeBehavior_TORA.csv to NodeBehavior_TORA (1).csv
[13] df=pd.read_csv("NodeBehavior_TORA.csv")
df.describe()
Node X Y Energy PktDrop
count 448 0.000000 448 0.000000 448 0.000000 448 0.000000
mean 4.718750 222.625000 295.466518 42.662263 0.252232
std 2.344284 142.350000 95.936168 2.801262 0.434779
  
```

Fig(8): Data Preprocessing in SVM



```
In [11]: from sklearn.svm import SVC
         svc=SVC(kernel='linear')

In [12]: svc.fit(x_train,y_train)

Out[12]: SVC(C=1.0, cache_size=300, class_weight=None, coef0=0.0,
            decision_function_shape='ov', degree=3, gamma='auto_deprecated',
            kernel='linear', max_iter=1, probability=False, random_state=None,
            shrinkage='none', tol=0.001, verbose=0)

In [14]: y_predict=svc.predict(x_test)

In [15]: y_predict3

Out[15]: array([0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0])

In [16]: from sklearn.metrics import accuracy_score
         accuracy_score(y_test,y_predict3) #SV

Out[16]: 0.8232941176470588

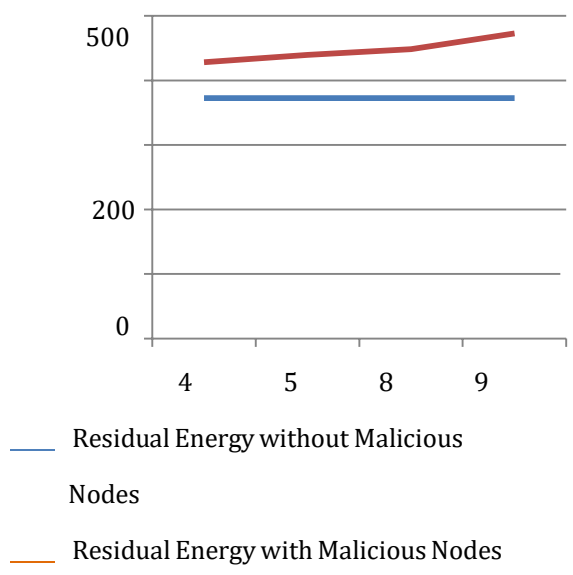
In [17]: cm=confusion_matrix(y_test,y_predict3)

In [18]: cm

Out[18]: array([[10,  2],
               [ 5, 15]), dtype=int64)
```

Fig(9): Confusion Matrix and Accuracy Score

From SVM Algorithm ,it is observed that an accuracy of 82.3and the confusion matrix showing less false positive rate



Fig(10): Residual Energy

4. CONCLUSION

From above results it is concluded that the adopted approach by SVM gives accuracy and detection rate, so that malicious node(s) can be isolated from the MANET and the performance of IDS can be improvised.

REFERENCES

1. Kwan Hui Lim , Amitava dutta,Enhancing the TORA Protocol using NetworkLocalization and Selective Node Participation, IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC),2012.

2. Pooja Rani,Kavita,Sahil Verma,Gia Nhu Nguyen , Mitigation of Black-hole and Gray-hole attack using Swarm inspired algorithm with ANN, IEEE Access, June 2020

3. Shweta Pandey, Varun Singh ,Black-hole attack detection using Machine Learning approach on MANET ,ICESC,August-2020

4. Indira N, Establishing a secure routing in MANET using a Hybrid Intrusion Detection System, International Conferenceon Advanced Computing (ICoAC) Dec,2014

5.Sankaranarayanan.S, Murugabhoopathi.G, Secure Intrusion Detection System in Mobile Ad Hoc Network using RSA Algorithm, Second International Conference on Recent Trends and Challenges in Computational Models. (ICRTCCM) ,Feb,2017

6. Sujithra L R, Nivethaa V, Pavithra B, Pavithran M, Heterogenous Based Intrusion Detection system in Mobile Ad Hoc Network, IRJET,,March,2018

7. Ningrinla Marchang and Raja Datta, A Novel approach for efficient usage of Intrusion detection System in Mobile Ad hoc Networks,IEEE Transactions on Vehicular Technology ,Jan,2016.

8. Y. Zhang and W. Lee., Intrusion detection in wireless ad hoc networks, 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), Aug,2000

9. Sujatha K S,Vydeki Dharmar ,Bhuvanewswaran R.S,Design of Genetic Algorithm Based IDS for MANET. IEEE International Conference on Recent Trends in Information Technology (ICRTIT),April,2012

10. Su, M.Y, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems.Computer Communications,Jan,2011.

11.Maglaras LA, A novel distributed intrusion detection system for vehicular ad hoc networks, International Journal of Advanced Computer Science and Applications,2015

12.Butun I, Morgera S D, Sankar R,A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials,May,2013.

14. Patcha A, Park J M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks,Aug,2007

15. K. H. Lim and A. Datta, An In-depth Analysis of the Effects of IMEP on TORA Protocol, in *Proc. of WCNC*, April, 2012