Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 8, August : 2022

IMPROVED AODV ROUTING PROTOCOL DEVELOPMENT AND ANALYSIS FOR ENHANCED NETWORK PERFORMANCE IN MANETS BASED ON MACHINE LEARNING MODEL

[1]Jhansi Modem, [2]Veluru Hirish Reddy, [3]Amgoth Naresh, [4]Banda Meghana

[1,2,3]Assistant Professor, [4]UG Student, [1,2,3,4]Dept. of Computer science Engineering, Visvesvaraya College of Engineering and Technology, Mangalpalle, Telangana, India.

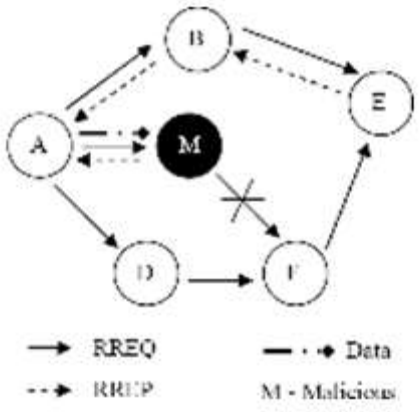
ABSTRACT

A MANET is a wireless ad hoc network that is self-configurable and does not allow for demobilization. This flexibility makes the route vulnerable to several security risks. Thus, the performance of IDS should be modified to address this. In this research, a strategy for improving IDS for the AODV routing protocol is given based on the Machine Learning (ML) algorithm in terms of accuracy and detection rate.

Key Words: MANET, Support Vector Machine, Intrusion Detection System, AODV(Ad-hoc On-demand DistanceVector) routing protocol.

INTRODUCTION

Prior to the rogue node(s) posing a security danger to the network, IDS is to identify the assault. It examines topics related to monitoring, detecting, and alerting. On MANETs, the Blackhole attack type is the most detrimental. Using an abnormality With the use of a machine learning technique, SVM Malicious Node(s) Causing Black Hole Attack in AODV Routing Protocol, IDS defends the network against Black Hole Attack. One of the main assaults on MANETs is the black hole attack. The data, including Source node, Destination node, and Neighboring node, is held by the malicious node(s) responsible for this assault on MANET security. In order to find the route destination, the source node broadcasts an RREQ (Route Request Packet) to its neighbouring nodes. Nevertheless, the source node receives a bogus route reply from the black hole node, which results in 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

RELATED WORK

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)

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

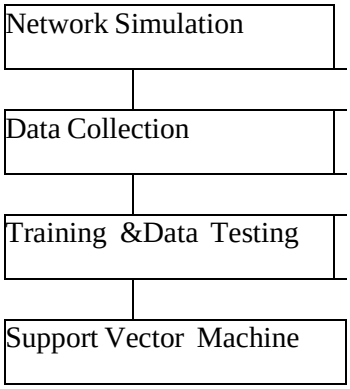
Muhannad Tahboush et.al The proposed algorithm HWAD was executed using NS-2 network simulator. The performance metrics was taking into consideration to evaluate the performance of the proposed algorithm the throughput, end to end delay, packet delivery ratio, and consuming energy. The proposed algorithm utilized Ad- hoc On-Demand Distance Vector (AODV) routing protocol to improve the detection method.

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

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, proabilistic approach is implemented, here optimal proabilistic 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.

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, infrastructure less 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

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 8, August : 2022

Parameter	Value
Simulator	Ns-2.35
Simulation Time	50 Sec
Area	1000*1000 m
Node Energy	50 Joules
No. Of Nodes	20
No. Of Malicious Nodes	3,4,14,18
MAC Specification	802.11
Packet Size	1000
Routing Protocol	AODV

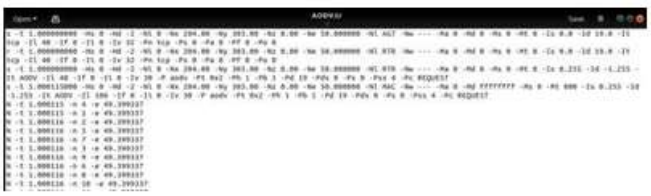
Table(1): Simulation Environment

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 AODV

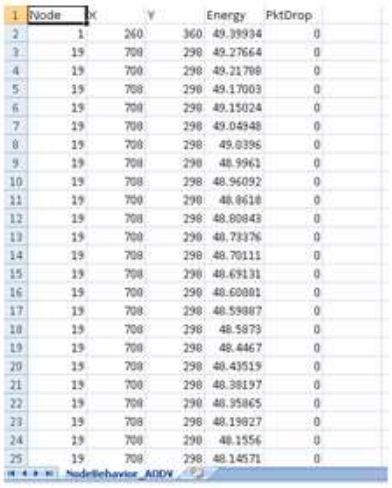
Step-ii) Data Collection

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

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 8, August : 2022



	Node	X	Y	Energy	PktDrop
2	1	260	360	49.39934	0
3	19	708	298	49.27664	0
4	19	708	298	49.21708	0
5	19	708	298	49.17003	0
6	19	708	298	49.15024	0
7	19	708	298	49.04948	0
8	19	708	298	49.0396	0
9	19	708	298	48.9961	0
10	19	708	298	48.96092	0
11	19	708	298	48.8618	0
12	19	708	298	48.80843	0
13	19	708	298	48.78376	0
14	19	708	298	48.70111	0
15	19	708	298	48.69131	0
16	19	708	298	48.60801	0
17	19	708	298	48.59807	0
18	19	708	298	48.5873	0
19	19	708	298	48.4467	0
20	19	708	298	48.43519	0
21	19	708	298	48.38197	0
22	19	708	298	48.35865	0
23	19	708	298	48.19827	0
24	19	708	298	48.1556	0
25	19	708	298	48.14571	0

NodeBehavior_AODV

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 insuch away that the distancefrom the hyperplane to the nearest node on each side is maximized.

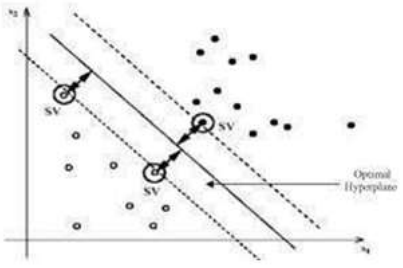
Algorithm-

I. Initialize Vector v and b to 0
II. Dataset D = (x1, y1), …, (xn, yn) ,where x, y are labeledsamples
III. Train SVM to learn decision function
IV. For each sample of D do
V. Classify xi using decision function f (xi)
VI. If (function margin < 1) then Calculate w', b' forgiven data
VII. Add sample example to known data vii)Use Eq. (w) =½"w" ^{2} for reducing errors
VIII. Use Eq. f(x) = sign ($w^T x^i$ + b) to predict.
IX. If (prediction is correct) thenDo it Again
X. Else

Train SVM AgainEndif Endif

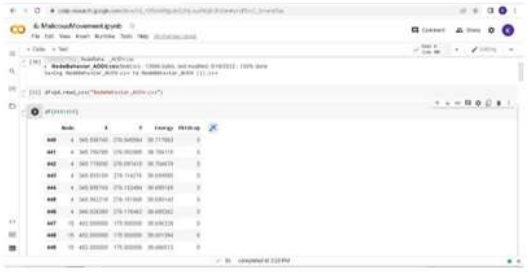
viii) Classify xi as benign or malicious

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 confusionmatrix. Theoutputisshown in Fig (9).

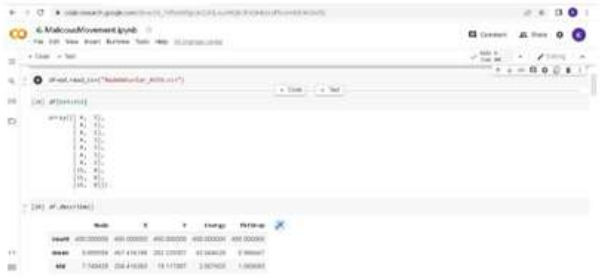


Fig(6): SVM Classification

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 8, August : 2022



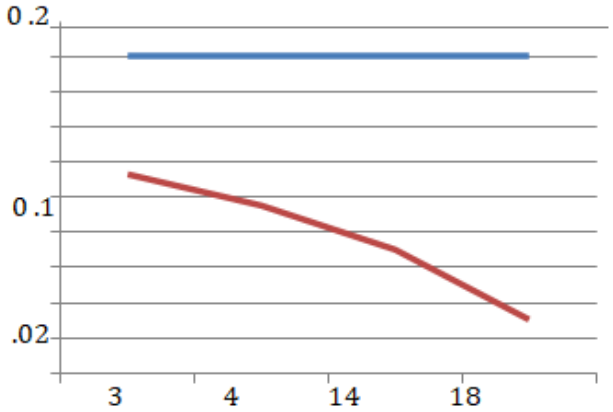
Fig(7): Data Sampling in SVM



Fig(8): Data Preprocessing in SVM

Fig(9): Confusion Matrix and Accuracy Score

From SVM Algorithm , it is observed that an accuracy of 82.35and the confusion matrix showing less false positiverate



Average Throughput without MaliciousNodes
Average Throughput with Malicious Nodes

Fig(10): Average Throughput

CONCLUSION

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

REFERENCES

1. 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
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. Muhannad Tahboush ,Mary Agoyi, A hybrid wormhole attack detection in MANET, IEEE Access, January-2021.
5. Indira N, Establishing a secure routing in MANET using a Hybrid Intrusion Detection System, International ConferenceonAdvanced Computing (ICoAC) Dec,2014
6. Sujithra L R, Nivethaa V, Pavithra B, Pavithran M, Heterogenous Based Intrusion Detection system in Mobile AdHoc 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 ,Bhuvaneswaran 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 ofAdvanced 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.
13. Patel M, Aggarwal A, Chaubey N,Wormhole attacks and countermeasures in wireless sensor networks: a survey. International Journal of Engineering and Technology (IJET), IApril,2017
14. Patcha A, Park J M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks,Aug,2007