Detection and Interception of Black Hole Attack with Justification using Anomaly based Intrusion Detection System in MANETs

Syeda Hajra Mahin, Fahmina Taranum, Lubna Naaz Fatima, Khaleel Ur Rahman khan

Abstract—Mobile adhoc network, a derivative of the adhoc network is sensitive to heterogeneous forms of attacks in particular passive and active attacks. Black hole attack is one such continually prevailing threat in mobile adhoc networks (MANETs), where specific nodes operate spitefully in the course of data transmission. Throughout this work, we intend to present an effectual approach to detect and intercept this attack taking into account Dynamic MANET on-demand (DYMO) routing protocol. This work presupposes working in three modules- planting, detection and ultimately the interception against the black hole attack. An IDS is initiated on the notion of machine leaning using MATLAB software. A relative scrutiny of IDS grounded on classifiers like K-Nearest Neighbor, Support Vector Machine, Decision tree and neural network is also conducted to make it certain that the best feasible classifier is settled on for administering the IDS. The analysis of the put forward work is subsequently accomplished taking miscellaneous metrics covering packet drop rate, average transmission delay, Packet Delivery Ratio along with throughput.

Index Terms— Black hole attack, DYMO, Intrusion Detection system, MANETs

I. INTRODUCTION

As the utilization of mobile devices for the means of trading information has progressed, the demand for affording security to it has eventually enhanced. In MANET it is interpreted that the nodes straightforwardly transmit the data employing some sketched routing protocols. The attacks prevailing on this network can be tagged as either passive or active attacks [1][2]. Throughout the black hole attack the spiteful nodes in the network drop the channeled data packets, thereby leading to unavoidable delay in dispatching.

In our work DYMO routing protocol is preferred for relaying the packets. DYMO stands for dynamic MANET On demand, which is an improvement of the extensively used AODV. It operates alike the AODV but is regarded to be more power economic than the later.

The behavior of the network is inspected under normal condition where all the nodes acquit themselves faithfully. This network is then manipulated by deploying a few black hole nodes in it. The deploying of the spiteful nodes is done by enhancing their capabilities at distinct layers. Post this, an IDS is proposed based on dissimilar classification algorithms to discover the occurrence of the intrusion i.e., the Black hole attack. The performance degradation is subsequently examined and jotted down.

Revised Version Manuscript Received on 10 September, 2019.

SyedaHajraMahin, Computer Science and Engineering, M.J.C.E.T, Hyderabad, Telangana, India
(Email: **:** jayamaniraaja07@gmail.com)
FahminaTaranum, Computer Science and Engineering, M.J.C.E.T, Hyderabad, Telangana, India.
LubnaNaaz Fatima, Computer Science and Engineering, M.J.C.E.T, Hyderabad, Telangana, India
Khaleel Ur Rahman khan, Computer Science and Engineering, Ace Engineering college, Hyderabad, Telangana, India

II. RELATED CONCEPTS

A. Black hole Attack

Once a spiteful node acquires a packet requesting route to the target, the black hole node confirms an up to date, direct and shortest route through it to the target whilst it actually lacks in having such route. Once the sending node (also referred to as originator) picks a path via the black hole node, this node commences to drop the relayed packets through it either discriminatingly or wholly [2][3].

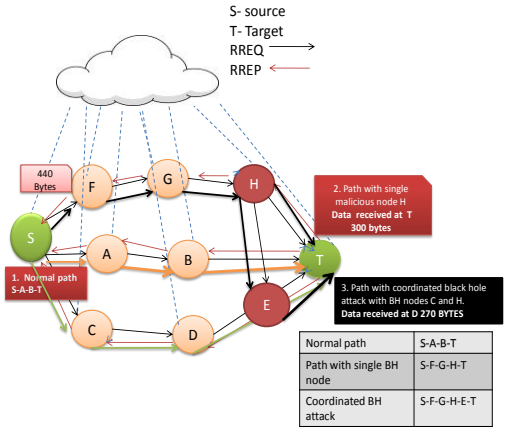

Fig.1: Black hole attack

Fig.1 can be studied for better understanding of the black hole attack. The illustrated network encompasses 10 nodes with S and T being the source and the target. The first scenario shows a normal path which is likely to be opted for transmission when a DYMO is taken (S-A-B-T).

The second scenario renders the network with an incorporated black hole node H. This node engages all the traffic by flaunting that it has the shortest route to the target. Later on, the data packets are effortlessly dropped. The third scenario represents the coordinated version of the black hole attack, where the nodes H and E coordinate their activities to furthermore lower the overall network performance.

B. Intrusion Detection System

The sole important function of the IDS is to examine the data relating to the conduct of the network and to be able to diagnose the intrusions, hence operating as a shield against the attacks [10]. The IDS are commonly graded as signature based, anomaly based or reputation based. An anomaly based system is settled on for carrying out this proposal, mainly because this system fabricates a model built on trusted and reliable system activities and collates current conduct against this model therewith yielding finer generalization when contrasted against any of the other IDS. This IDS operates on the knowledge of machine learning. In this paper we have worked with the following algorithms.

1. Decision tree:

This is a widely used Data Mining algorithm implemented to perform classification for IDS. A decision tree encompasses of nodes, edges together with leaves. This works by simply generating rules of if-else format. Following these rules, the classification of records is done into varied classes. For our IDS the classes decided are malicious and non malicious.

2. K-Nearest Neighbor:

The *k*-NN operates by saving all the accessible data records and classifies the upcoming records by taking into consideration the distance metric. The distance of the test record is computed against the training data set records and those instances which lie closest to the testing data is regarded for next step, where these instances poll for discovering the class to which the test data record should belong.

3. Support Vector Machine:

SVM is chiefly used for pattern detection problems and can also be used for classification. SVM collects the data points belonging to different classes and split them on the feature space by means of a margin. It formulates a hyper plane to discriminate between different classes. This plane is devised such the distance between the two classes is wide enough. SVMs works by deducing a range of support vectors from the sample data inputs on the hyper plane.

4. Neural network:

NN comprises of varied layers of neurons for processing and training the records. MATLAB's NprTool is taken up to solve the classification problem, which is a 2 layer feed-forward network. In our work, we have created a NN with 10 hidden neurons that do the processing. It utilizes sigmoid function for output neurons. In NN confusion matrix is considered for performance evaluation together with cross entropy.

III. LITERATURE SURVEY

In [4], the authors brought forward a mechanism to counter the black hole attack by segregating the comprising nodes into different classes. The originator simply splits up the communicated data packet and channels this to the different classes of nodes appending the id of the packet, its id of split together with the sum of ids of split in the encrypted form. After carefully examining their proposal it is noted that this mechanism leads to excessive delay.

In [5], black hole attack is prevented by using the idea of sequence numbers. This works in a manner such that the Seq no's of every possible path to the target is collected and its average is computed by the originator. The idea behind this proposal is that if a node depicts a seq no. exceeding the aggregate routes is handled as a black hole node.

In [6], the black hole attack is tackled by executing a BDS mechanism pondering DYMO protocol. The BDS component gauges the power of transmission along with the altitude of antenna for every node with the aim to spot the black hole node. The reason for considering this procedure is that through this approach the high capability node can be easily distinguished.

In [7], cross checking is integrated to identify the black hole attack. A supplementary control message is conveyed to cross check with the prevailing network nodes to observe any discrepancy. Later through Extended Data Routing Information table, the black hole nodes of the detected path are detached from the network.

In [8], hop enumeration scheme is executed to prevent against the black hole attack. This works with the aid of a config packet dispatched by the target node to the originator node only after the data packets are accepted. This process works by implementing two lists namely, black and white lists for detecting the malicious nodes causing black hole attack.

In [9], on AODV supplementary fields are appended to examine the credibility of the data forwarding paths. A route reply is handled and stored provided its appended bit for credibility is set. The ignorance of the black hole node will result in bit value Null, which helps in the easy identification of the attacker nodes.

In [10], the authors have put up a strategy to intercept two sorts of attacks, viz black hole and gray hole attacks. NS-2 simulator is employed and an IDS is initiated by inspecting dissimilar machine learning classifiers. It is noticed by their work that the MLP model has been the most productive one with greater accuracy gain when juxtaposed against the other classification algorithms.

In [11], a mechanism is suggested to diagnose the occurrence of black hole attack rooted on ANN. The simulations and performance investigations were accomplished on the MATLAB. An intrusion detection system is outlined built on ANN. The assessment criteria thought of includes throughput, PDR, jitter along with delay. Their work manifests that the plotted IDS can work well in spotting the existence of a black hole attack.

In [12], a scheme to detect black hole attack is proposed taking DYMO routing protocol. The logic behind the identification of black hole nodes is based upon the time taken by the data packet to make it to the target node. A threshold value is fixed, and the data packets are checked against this threshold value. If a data packet surpasses the threshold time a black hole attack is detected. Later to prevent the occurrence of this attack in the network

Human-in-The-Loop commands are used to deactivate the specific malfunctioning nodes. This work is also evaluated for diversified traffic generators.

IV. PROPOSED SYSTEM

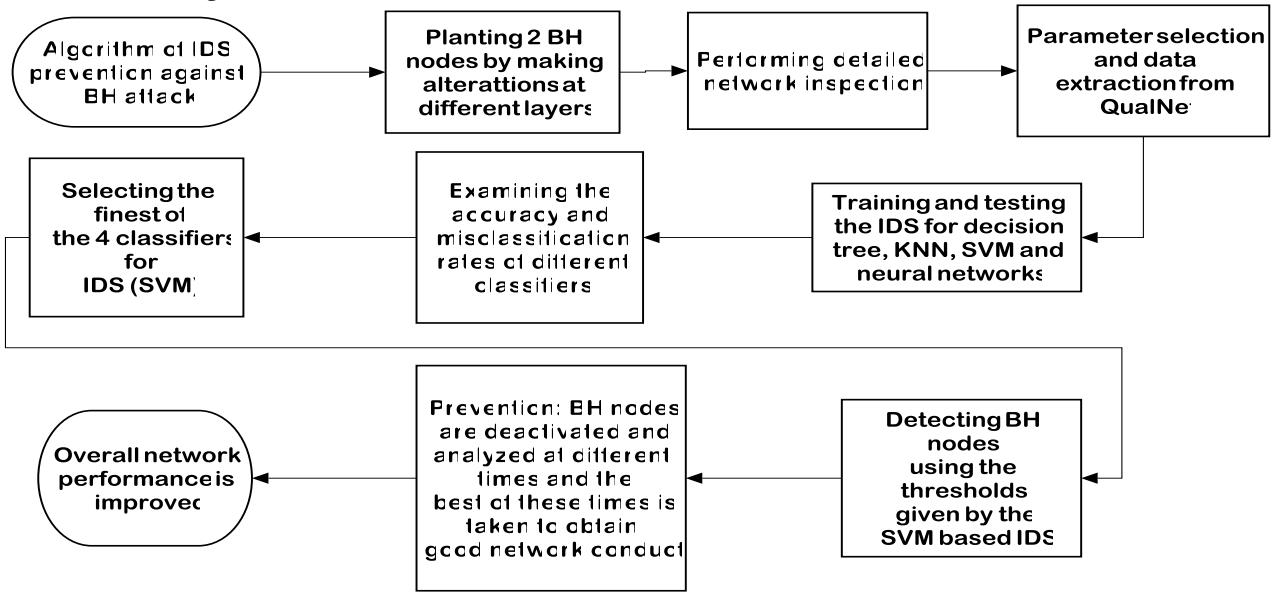

Fig.2: Working of proposed system

The intended proposal can be broken down into the listed modules shown in fig.2

1. Planting a black hole attack:

The black hole nodes are planted in the network by performing certain refinements at differing layers. Some of which includes altering antenna elevation, node traversal time, buffer size, noise and speed levels, reception sensitivity, etc,.

2. Parameter selection and Data extraction:

Planting of black hole attack in the network is followed by gauging the network performance with the help of the stat files generated by the QualNet simulator. After exploring the performance of the network at different layers, the parameters for sketching the IDS are decided which are as follows.

1. Packet drop ratio= (no. of packets gained – no. of packets dispatched) X 100

2. Average transmission delay(s) = aggregate bits / transmission rate (bits/sec).

3. Designing Intrusion detection system:

In this work one constructive IDS is designed which is evaluated on the classifiers like decision tree, KNN, SVM and neural network. After which the conduct of the network is explored for all the classifiers mentioned and based on their accuracy values and mis classification rates the finest of them would be opted.

4. Prevention:

Preventing the network from the attack, post its detection is a crucial concern. The further collaboration of the black hole nodes in the network activities is halted in QualNet using Human-In-The-Loop commands. HITL commands authorize the user to communicate with the simulator throughout a proceeding simulation. With the assistance of these commands the nodes can be activated/ deactivated and also the traffic scale can be refined. Accordingly, with the support of the HITL file, the spiteful black hole nodes are abolished from the network by deactivating them.

V. IMPLEMENTATION

A three sub network architecture involving 16 nodes is modeled and is illustrated through fig.3. The sub networks are mounted with internet protocols of versions 6 and 4 alternatively i.e. (IPv6-IPv4-IPv6). Two among the nodes are setup to perform dual IP roles (3, 8). A CBR traffic from originator 1 to the target 14 is triggered, channeling 1000 packets all of magnitude 100 bytes. The time of the simulation is maintained to be 1000 seconds. A dearth of direct route between the initiator and the target leads to the imparting of RREQ. The role of the dual IP one's is to build a tunnel to redirect the packets to more nodes in the network.

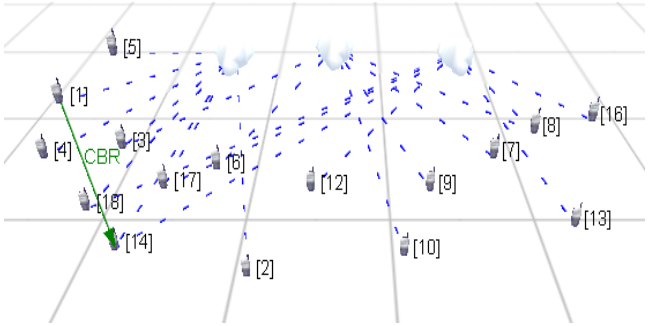

Fig.3: Network architecture

The tunneling notion is chiefly to lessen the inconsistency among the varied versions of IP. Considered topology is examined for DYMO protocol. In the designed system two black hole nodes are planted, viz 17 and 18. The motive to opt for CBR is that it is congruous with both IPv4 and IPv6.

The framework gradually works with the black hole nodes 17 and 18 detaining the packets and subsequently on

discovery of the attack, the spiteful nodes are detached and halted from further association in the network events. The attack is thereafter intercepted by stopping the involvement of the node in the network by employing a HITL file.

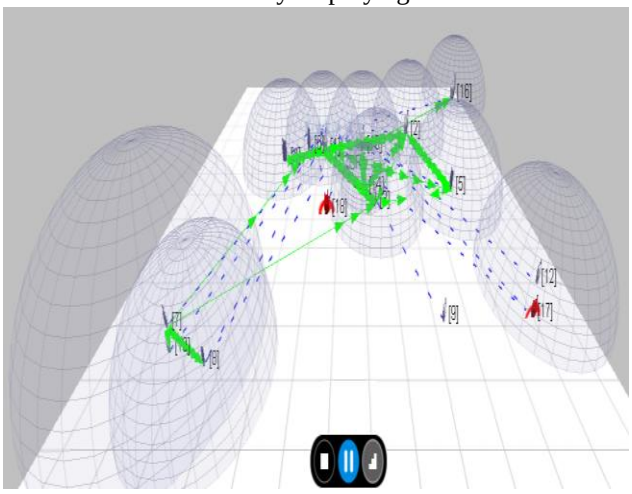

Fig.4: Network architecture after deactivation

The fig.4 conveys that the nodes 17 and 18 are deactivated by appending a HITL file. The de-activated nodes are rendered by a red cross across them.

The conduct of the network is explored by deactivating the spiteful nodes at varied simulation times to assure that the nodes are deactivated only when they commence behaving maliciously.

VI. RESULT ANALYSIS

The parameters regarded while plotting the scenario are tabulated below in table 1.

Table 1: Simulation parameters

Parameter	value
Simulator	QualNet 7.4
Routing protocol	DYMO
No. of nodes	16
No. of black hole nodes	2
Speed	10ms
Pause time	30s
Terrain size	X-1500, Y-1500
Network protocol	IPv4, IPv6
Seed	1
Node placement strategy	File
Mobility model	Random way point
No. of channels	3
MAC protocol	802.11
PHY radio type	PHY 802.11b Radio
Traffic generator	CBR
No. of data packets sent	1000
Item size	100 bytes
Simulation time	1000s
Channel frequency	2.4GHz

In this section the results are taken from the QualNet stat files and are examined to gauge the network performance against the performance metrics. The metrics considered for evaluating the proposed work includes:

1. Packet Delivery Ratio:

It is the proportion of the packets obtained to the packets passed on.

2. Packet loss rate:

It is the difference between the packets obtained and the packets passed on.

3. Throughput:

It is the aggregate of packets dispatched per unit time.

4. Average transmission delay:

It is the average amount of time utilized by a data packet to shift from initiator to the target end.

In the fig.5, the packet drop rate is inspected for the black hole nodes against different deactivation times. By conducting the analysis it is noted that at 25s the packet drop is minimal and soon after that the drop rates have escalated. Hence deactivating the malicious nodes at 25s will result with lowest packet loss.

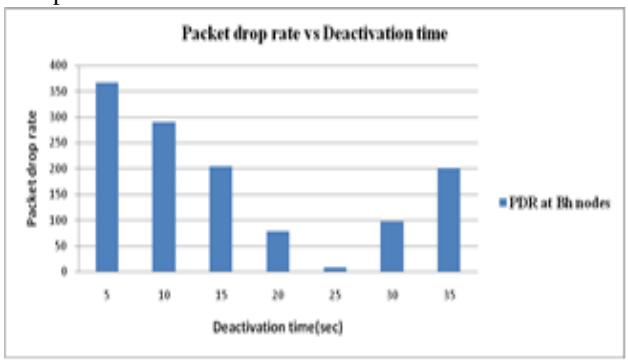

Fig.5: Packet drop rate vs. deactivation time

The fig.6 portrays the total packet drop rate for 3 scenarios. It can be perceived that the packet drop rate is not much when no black hole nodes are planted. Whereas post the deployment the packet drop rate has surged drastically. By deactivating the spiteful nodes at 25s the drop rate has brought under control.

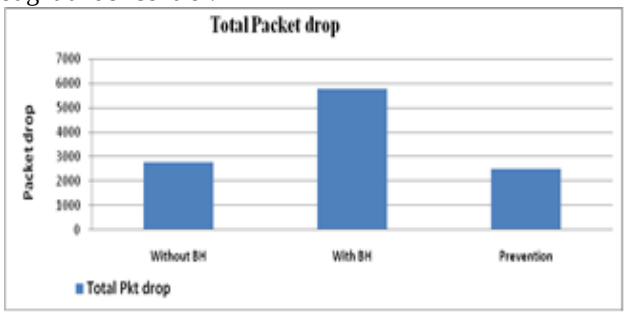

Fig.6: Total packet drop analysis

The fig.7 displays the study of average transmission delay. In the absence of the spiteful attack the transmission delay at different nodes is quantified and it can be perceived that the delay is high in the presence of the attacking nodes in the network. With the applied prevention plan this influence is curtailed.

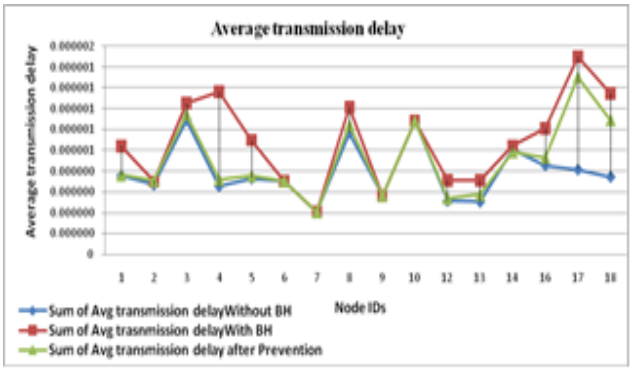

Fig. 7: Average transmission delay analysis

In order to strongly scrutinize the proposal, the performance inspection is furthermore carried out for dissimilar scenarios including variable speeds, pause times and terrain areas.

(a) Simulation parameters for variable speeds

The exact specifications listed in table 1 are thought about but with diverse speeds. The speed values taken are as follows: 5,10,15,20,25ms.

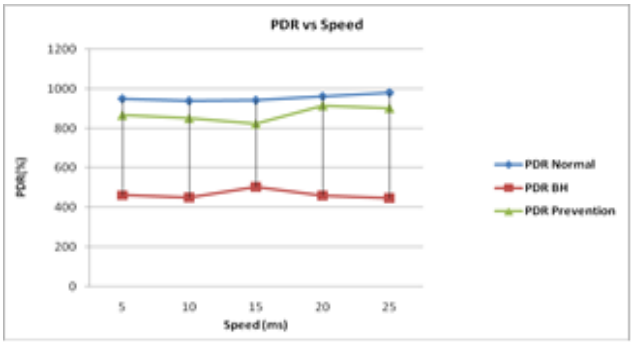

Fig.8: PDR vs. Speed

The fig.8 outlines that for varying speeds the PDR also varies. With the put in prevention plan the PDR levels are discovered to be in close proximity to that of the PDR in the absence of the black hole attack.

According to the fig.9, the throughput is discerned to be good enough under normal circumstances for fluctuating values of speed. After the prevention the throughput values are found to be optimum with negligible difference. By inspecting the throughput against fluctuating speeds we can note that the proposal is practically effective to prevail over the black hole attack.

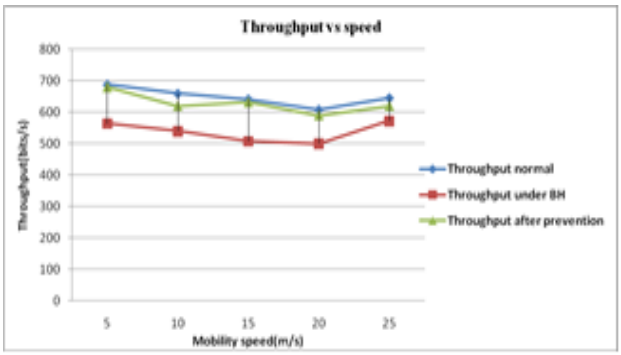

Fig.9: Throughput vs. Speed

From the fig.10, the packet drop rate is contrasted against differing speed. The packet drop rate in the absence of malicious nodes is insignificant, whereas after the spiteful nodes are implanted the packet drop has shoot up enormously thereby striking at the network performance. With the prevention the packet drop rates were successfully lowered.

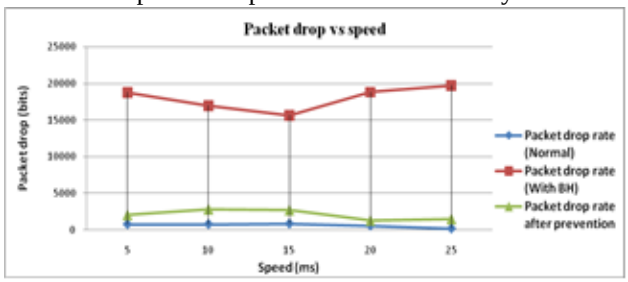

Fig.10: Packet drop vs. Speed

(b) Simulation parameters for variable pause times

The identical considerations listed in table 1 are pondered but with changing pause times. The pause time values selected are: 30, 60, 90, 120, 150 seconds. In the fig.11, the PDR is reviewed against pause time. Under normal state it is discovered that the PDR vaguely intensifies as the pause time escalates. In the presence of the attack the PDR values are noted to show a substantial fall, which is regulated by implementing the proposal.

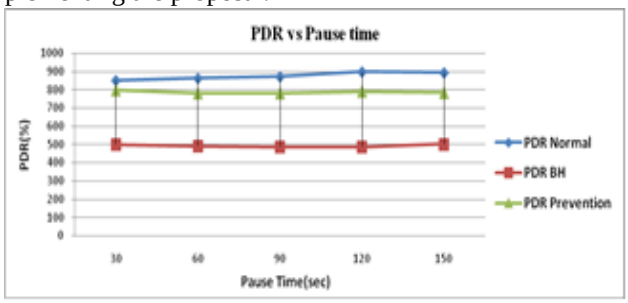

Fig.11: PDR vs. Pause time

In the fig.12, collation is made against throughput and pause times. The throughput of the network deviates with differing pause times. There is no systematic pattern observed. By implementing the proposal, the throughput of the network is amplified and is perceived to be very close to the throughput in the normal conditions.

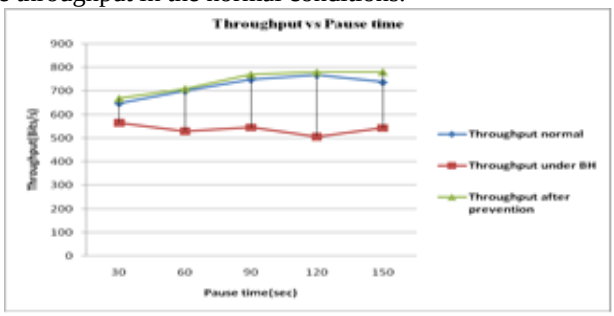

Fig.12: Throughput vs Pause time

In the fig.13, the packet drop rates juxtaposed against the pause times is examined and it is noticed that with rise in pause time, there is a moderate reduction in the packet drop rates. The put forth plan works well to condense the packet drop rates.

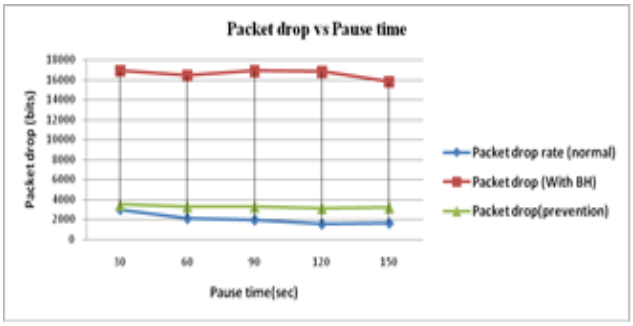

Fig.13: Packet drop vs. Pause time

(c) Simulation parameters for variable terrain areas

The very specifications of table 1 with altering terrain areas are appraised. 1500, 1750, 2000, 2250, 2500 areas are picked up for the simulations.

In the fig.14, the PDR is probed with alterations in the areas of terrain. It is seen that with augmentations in the terrain area, the PDR values dwindle. By deactivating the spiteful nodes, the PDR values are escalated.

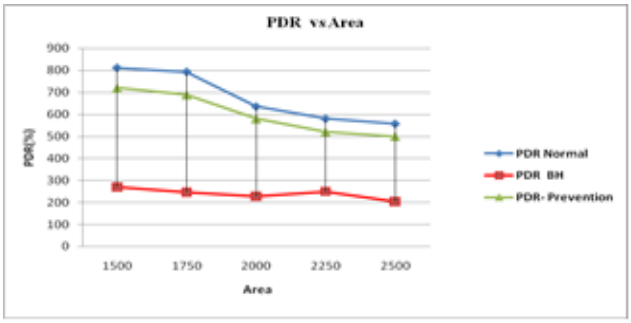

Fig.14: PDR vs. Area

In the fig.15, it can be perceived that as the terrain areas escalate there is gain in the throughput. In the company of the Black hole nodes the throughput of the entire network perceives a fall thereby demeaning the system execution. Post applying the prevention scheme, the throughput of the network is brought back to the standard pattern.

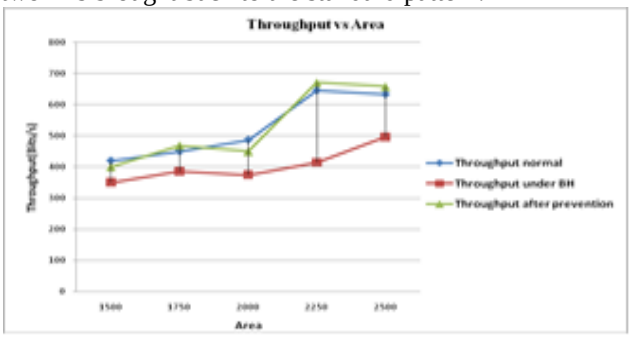

Fig.15: Throughput vs. Area

From the fig.16, the packet drop rates are explored with respect to the areas. With the rise in the area, the packet drop rates also shoots up. In the existence of the attack, the Packet drop rates had an immense surge which is efficiently reined by administering the proposal.

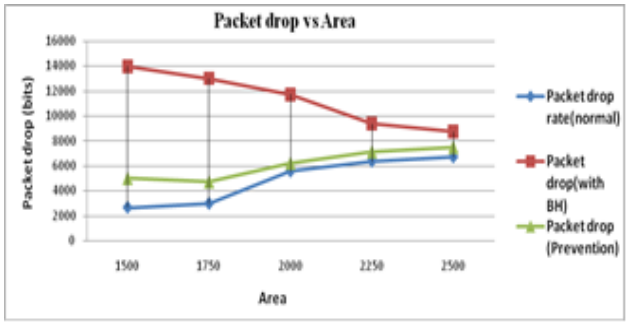

Fig.16: Packet drop vs. Area

The sketched IDS is run on dissimilar supervised machine learning classifiers which encompasses Decision tree, KNN, SVM and artificial neural network. The classifiers are trained for a data set covering 200 records. The juxtaposition of these classifiers is done by considering metrics like

1. Accuracy rate:= $\frac{(TP + TN)}{Total}$
2. Misclassification rate: $\frac{(FP + FN)}{Total}$
3. True positive rate (TPR): TP/Actual YES
4. False positive rate (FPR): FP/Actual NO
5. True negative rate (TNR): TN/Actual NO
6. False negative rate (FNR): FN/Actual YES

Where TP= True positive; TN= True negative; FP= False positive and FN= False negative.

In the fig.17, the accuracy rates of the classifiers are jotted down for scrutinization. It summarizes the inspection done by assessing against the values of table 1.

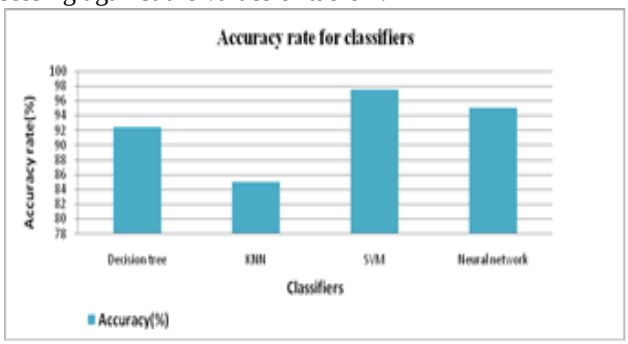

Fig.17: Accuracy rate for classifiers

From the interpretation it can be clearly perceived that for the taken values of specifications and network, the best classifier for the IDS manifested is SVM demonstrating the towering accuracy rate of 97.5%. Hence from SVM, the threshold values obtained for average transmission delay and Packet drop rate are $1.5x10^{-6}$ and 600. For detection, the stat files generated by QualNet simulator are analyzed to identify any nodes violating these threshold values.

The table 2 recapitulates the computed metric values for the examined machine learning classifiers for IDS. It is expected that the classifier exhibiting escalated TPR and TNR values with low FPR and FNR values is the foremost to work for designing IDS.

Table 2: Detailed classifier analysis

Classifier	Accuracy rate	Mis-classification rate	TPR	TNR	FNR	FPR
Decision tree	92.5%	7.5%	83 %	94%	17%	6 %
KNN	85%	15%	0%	100 %	100 %	0 %
SVM	97.5%	2.5%	100 %	97%	0%	3 %
Neural network	95%	5%	100 %	94.4 %	0%	5.6 %

With the aim to make the analysis more robust, we have also surveyed the accuracy rates of the classifiers by modifying the mobility speeds of the nodes. With 5, 10, 15, 20 and 25s as the range of speed values considered. The fig.18 portrays the accuracy of the classifiers for contrasting speeds, from which it is perceptible that the SVM works consistently well compared to the rest of them.

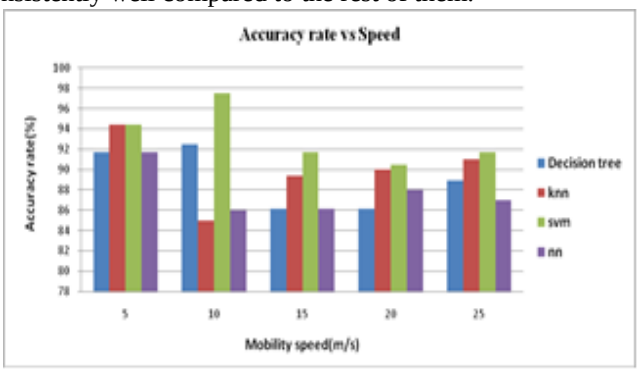

Fig.18: Accuracy vs. Speed

VII. CONCLUSION

In this paper, we have implanted a black hole attack by instigating two spiteful nodes in the network. DYMO routing protocol is administered on the network using QualNet 7.4v simulator. The QualNet stat files are scrutinized with respect to metrics including PDR, packet drop rate, throughput and average transmission delay. An IDS is fabricated by nominating packet drop rate together with average transmission delay as features. This research has also conducted relative investigation of machine learning classifiers viz. decision tree, KNN, SVM and neural network using MATLAB, which infers that the SVM is a preferable classifier compared to the rest of them as it holds the elevated accuracy rates. The put forth mechanism works competently to diagnose the black hole attack and mitigate it by deactivating the spiteful nodes at the right time making the network reach optimal performance. The work is later inspected against diverse range of speed, pause time and terrain areas to reinforce our proposal. After which it is perceived that by applying the proposed strategy the performance of the network has boosted thereby augmenting the PDR and throughput and declining the packet drop rate and transmission delay. Through this work the vulnerabilities of DYMO routing protocol are prosperously bridled.

In time to come, we aspire to formulate an efficacious ID to counter the coordinated version of black hole attack and also on its progressed alternative-wormhole attack.

REFERENCES

1 RahmaMeddeb,BayremTriki,Farah Jemili,OuajdiKorbaa, “A survey of Attacks in Mobile Ad hoc Networks”, International Conference on Engineering & MIS, 2017.
2 SyedaHajraMahin, LubnaNaaz Fatima, FahminaTaranum,Khaleel Ur Rahman Khan, “Proposals on the Mitigation Approaches for Network Layer Attacks on MANET”, International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-6S, 2019.
3 Sonia Verma, Jigyasa Sharma, Dr. Sima, “A Study of Active and Passive Attacks In Manet”, IJSRD - International Journal for Scientific Research & Development, Vol. 4, Issue 09, 2016.
4 ElbasherElmahdi, Seong-Moo Yoo, Kumar Sharshembiev, “Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks”, IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018.
5 TaranpreetKaur, Rajeev Kumar, “Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol”, 6th IEEE International Conference on Smart Energy Grid Engineering, 2018.
6 DhirajNitnaware, Anita Thakur, “Black Hole Attack Detection and Prevention Strategy in DYMO for MANET”, 3rd International Conference on Signal Processing and Integrated Networks (SPIN), 2016.
7 Dorri, “An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET”, Springer Wireless Network, 2016.
8 AvniTripathi, A.K. Mohapatra, “Mitigation of Blackhole attack in MANET”, 8th International Conference on Computational Intelligence and Communication Networks, 2016.
9 Sagar R Deshmukh, P N Chatur, Nikhil B Black holeople, “AODV-Based Secure Routing Against Blackhole Attack in MANET”, IEEE International Conference On Recent Trends In Electronics Information Communication Technology, 2016.
10 KonagalaPavani, “Routing Attacks in Mobile Ad Hoc Networks”, International journal of network security, vol. 6, 2014.
11 RamanpreetKaur, AnantdeepKaur, “Blackhole Detection In Manets Using Artificial Neural Networks”, International Journal For Technological Research In Engineering Volume 1, Issue 9, 2014.
12 FahminaTaranum, Khaleel Ur Rahman Khan, “Maneuvering Black-Hole Attack Using Different Traffic Generators in MANETs”, Intelligent Systems, Technologies and Applications. Advances in Intelligent Systems and Computing, vol 910. Springer, Singapore, 2019