A MACHINE LEARNING APPROACH TO DETECT NETWORK LAYER ATTACKS IN MOBILE AD HOC NETWORKS

N. Sivanesan .[1] K.S.Archana[2,]

[1]Research Scholar, Dept. of CSE, Vels Institute of Science, Technology & Advanced Studies, Chennai, India

[2] Asst. Professors, Dept. of CSE, Vels Institute of Science, Technology & Advanced Studies, Chennai, India

Abstract

For the past few years, Mobile Ad hoc Networks (MANET) have an improbable progression and fast reputation due to the accessibility of in-expensive mobile devices and its capability to afford prompt wireless networking. The MANET forms are created without the use of any stand-supporting devices, dynamically allotted topology, loosely coupled etc. Additionally, it is an energetic system and nearby no eternal arrangement and similarly no essential organization. For these networks, security is the utmost and important facility to deliver safety to avoid malicious attacks happening in the nodes. The topology and atmosphere of MANET creates attention to several categories of attackers and ensure more or less redundant actions by means of mobile nodes. In recent trends, Machine learning (ML) approaches afford the system with learning competence and inspire variation into the atmosphere which depends on numerous rational and arithmetical procedures. Till now, several kinds of ML approaches are executed for the MANETs security. Because, MANETs with the infrastructure-less surroundings pretends an excessive task in execution of security arrangements. The security methodologies in MANETs essentially concentrate on eliminating malicious attacks, selfish/misbehavior nodes and providing secure routing. This research paper presents an exclusive research for several types of network layer attacks of typical holes, (gray, worm, black) and flooding attack occurring in the MANET and using the ML approaches for increasing security in MANETs.

Keywords: Attack detection, Machine Learning, Mobile ad hoc networks, Network Layer attacks, Security.

1. Introduction

Over the years, the globe has turned out to be an international rural community through the feature of high-tech innovation. Day-by-day Information Technology (IT) grows has a tendency to exploit additional multifaceted network surroundings. Even though, the determinations of IT merchants and network proprietors protect the work out situations, but, the warnings impersonated to private secrecy, business secrecy and numerous resources by attacks upon setups [1]. Mobile Ad hoc Networks (MANETs) are considered as one of the definite portion in high-tech innovation. MANETs are a group of mobile nodes that construct a provisional network dynamically exclusive of relying on available network infrastructure. Because, these nodes consume boundless flexibility and connectivity to further nodes transmitting. Also, every node performs as a router and system director to alternative node. To provide a secure transmission between the networks, considerate the accountable security attacks is a challenging assignment in MANET [2]. Additionally, MANETs agonize from an assortment of security warnings and attacks for example: black-hole attack, worm-hole attack, impersonation attack, Denial of Service (DoS), gray hole attack, flooding attack and so forth [3].

In MANET, security is an important constraint for any system processes such as routing protocols and packets. Despite the fact that, planning some profound tenders, the life-threatening security structures of the setup must be deliberated. Nowadays, Machine Learning (ML) approaches support in planning an extrapolative design where exemplary is accomplished through the training facts for definite attack configurations and formerly tested by residual test facts [4]. The learning exemplary precision is calculated which depending upon the accurateness of recognizing novel attack configurations. The distinctive characteristics of MANETs are reorganization, self-administration etc. which fascinates several attacks in the network. For the past few years, an assortment of security appliances is suggested to identify the attacks and alleviate the influences. In outer layer, an amount of cryptographic techniques was implemented in earlier to present security characteristics in MANETs. But then again, there is a modification in setup prototype as new machineries in recent period for instance, ML which have turned out to be a substantial option for investigators in recognizing operative and enhanced results for security [5]. For that reason, this research elaborates efficiently in terms of prevention, detection, extrapolation and moderation of cooperated nodes and numerous secure routing procedures depends on ML approaches were observed.

2. Overview of Network Layer Attacks

The routing procedures are exploited as a tool while deliberating definite malicious actions ever since it is exploited in the experimentations conferred all over the study [6]. Figure 1 illustrate es the overview of network layer attacks.

An attack is any unauthorized individual obtaining access to data in a network setting.

Source of attacks:

a. Internal attacks: the attacker node acts like any other node, dropping all incoming packets or rerouting the path so that the intruder receives all packets.

b. External attacks: the attacks that are initiated by a node that is not part of the network. These attacks generate network traffic, distribute faulty routing algorithms, and, in certain cases, shut down the network.

Nature of attacks:

c. Active attack:

Impersonation attacks, disclosure attacks, DoS attacks, black hole attacks, man in the middle attacks, and eavesdropping are examples of active attacks that cause substantial network damage and insert or modify information in the network.

d. Passive attack:

This attack without interacting with the protocol, but listens directly with the medium of communication for data. Cryptography, firewalls, and intrusion detection systems are employed in security approaches to protect against cyber threats. Example of passive attack: traffic analysis, message disclosure.

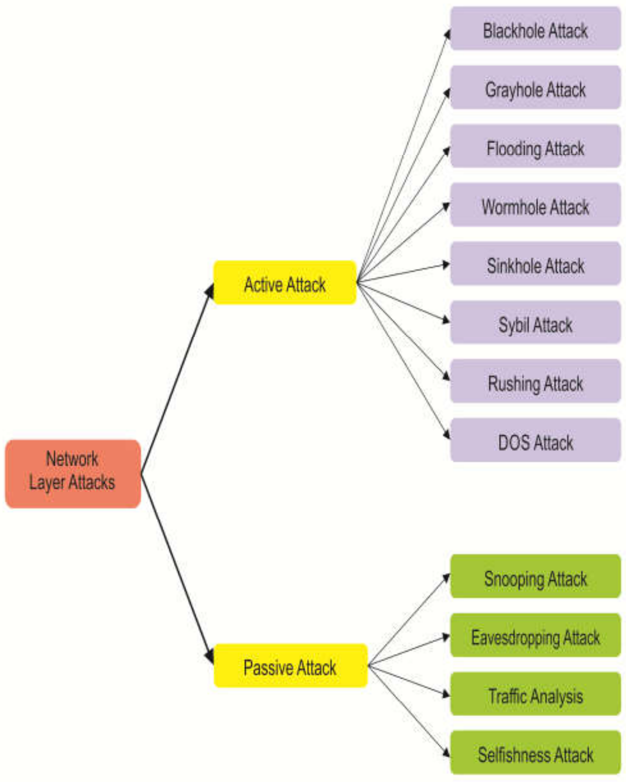


Figure 1. Overview of Network Layer Attacks

2.1 Black-hole attack

For this type of attack, the chief aim is to decline the arriving and departing data amongst the recipient and supply. In this type, the invader will seize every data packets and remove it, as an alternative of progressing into the end point. It's termed as complete packet dropping attack or a complete denial of service attack is what, such as black holes: In FDoSA, there is no communication between the source and destination nodes through the malicious node. The black hole node sends a bogus route reply to the source node, lowering network performance. With respect to the number of **attacker** nodes the Black hole attacks are classified as single and cooperative black hole attacks. In a single black hole assault only one attacker node is active, whereas the cooperative black hole attack involves a number of attackers cooperating to decrease network resilience.

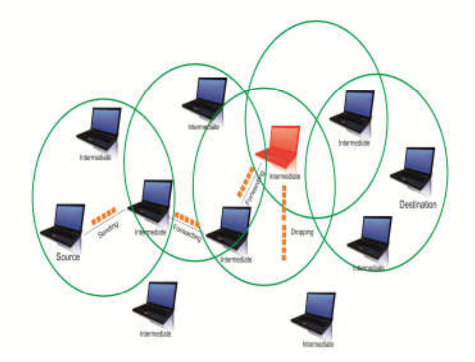


Figure 2: Blackhole Attack

2.2 Grey Hole attack

The grey hole attack is correspondingly recognized as routing mischievousness assault that causes a data packet loss. After that, the nodes will descent the data discriminatory. Another sort of DoS attack is the grey hole attack, that comes in two flavours: sequence number based attack and smart grey hole attack. The partial packet dropping attack is also known as the grey hole attack. The malicious node is responsible for the partial communication between the nodes. It takes part during the route detection of destination node. It follows a valid path to the destination.

It's also known as a partial packet loss attack or a partial DoS attack.

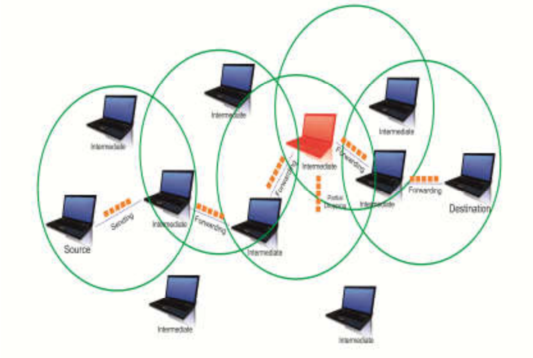


Figure 3: Grayhole Attack

2.3 Flooding

This flooding attack produces a foremost disturbance of setup operations and utilized to pretend flooding action. It is accomplished through directing outsized capacity of traffic over the setup that causes the damage in distinct node properties and inclusive bandwidth. To determine whether a node is malicious in a flooding attack, algorithms use the route detection history data of nodes falling in the same class.

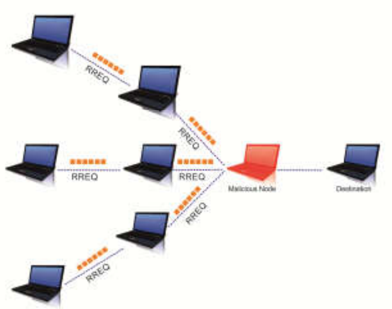


Figure 4: Flooding Attack

2.4 Wormhole attack

These attacks are considered as one of the most unembellished attacks that are tough to identify and secure from the invaders. While the total transmission on the network delivers truthfulness and privacy, but a wormhole attack may occur and delivers a severe damage to the protocols**.** Because the attackers are directly connected to each other through a tunnel in a worm hole assault, they can communicate at a faster pace than the other nodes in the sensor network. At least two malicious nodes utilizing a private channel called a tunnel detect a worm hole attack. At this point, the wormhole tunnel will begin collecting data packets and sending them to a different destination. A control packet and one side of the tunnel are sent to a malicious node. If the packets are transferred to another interesting node over a private channel at the other end, the packets are retransmitted locally.

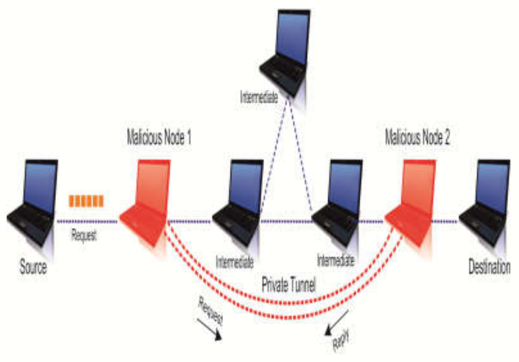


Figure 5 : Wormhole Attack

2.5 Sinkhole attack

One of the more serious assaults in which the attacking node uses an enticing, incorrect routing link known as a gateway to draw all network traffic to it is termed as sinkhole attack. When it obtains the entire traffic and then modifies the specific secret information, this malicious node strives to get hold of secure information from all surrounding nodes because they create the most efficient communication path to the destination.

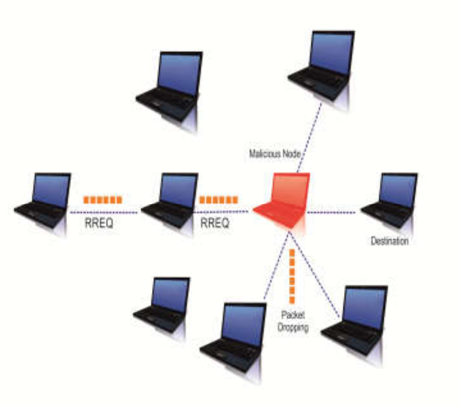


Figure 6 : Sinkhole Attack

2.6 Sybil attack

This attack is a way of confronting by thieving the characteristics of supplementary expedients on the setup. The invader will exploit these characteristics to function as numerous characteristics to remaining network expedients.

2.7 Rushing

In this rushing type, a mischievous node disrupts the detection process and rises the chance of unsympathetic node is involved in particular path. Then, the cooperated node quickly transmits the route request communications to confirm prompt appearance commencing from remaining nodes**.**

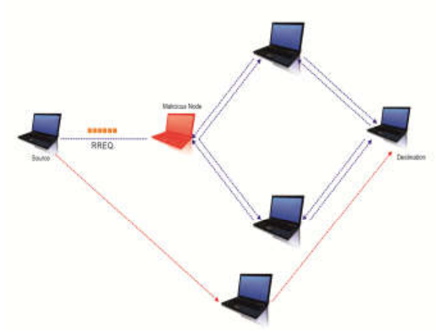


Figure 7 : Rushing Attack

2.8 Denial of Service attack

Here, the invaders create a challenge to cause the network properties momentarily unreachable to authentic consumers. The invaders direct false demands to the providers, therefore, it turns out to be unreachable to provision, its anticipated consumers and providers possibly will be momentarily miserable.

3. Overview of Machine Learning in MANET

Machine learning (ML) is utilized to create processers appear smooth, and characterization of ML is training processers to acquire. Recent days, ML is turning out to be widespread due to large quantity of data employed in indicators. Hence, here revolving to processers to sort out the investigation and approximately referred as data analytics [7]. Generally, ML approaches descent into dual classes: one is supervised learning and other unsupervised learning which are illustrated in figure 2.

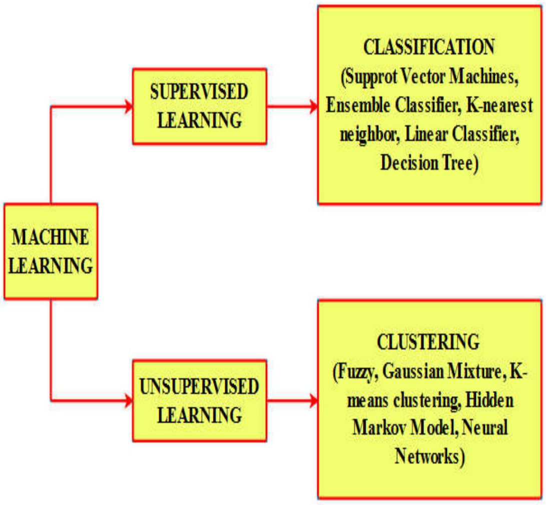

MACHINE LEARNING
SUPERVISED LEARNING
CLASSIFICATION (Supprot Vector Machines, Ensemble Classifier, K-nearest neighbor, Linear Classifier, Decision Tree)
UNSUPERVISED LEARNING
CLUSTERING (Fuzzy, Gaussian Mixture, K-means clustering, Hidden Markov Model, Neural Networks)

Figure 8. Overview of Machine Learning Techniques

3.1 Supervised Learning

Supervised training is a designation which specifies that training process can be a trainer in the occurrence of administrator. In this situation, the information in which the statistics tag is designated and need to be trained. The expedient with definite information have previously noticeable through the accurate response. There's a portion of supervised learning procedures such as Support Vector Machine (SVM), Artificial Neural Network (ANN), Decision Trees, K-Nearest-Neighbors (KNN), Linear / Ensembles classifiers which are most widespread supervised learning procedures.

3.2 Unsupervised Learning

In unsupervised learning, the analysis of unrestrained training is completed by controllers deprived of supervision. Responsibilities are accomplished on the source of previous practice through unsupervised learning which denotes to the issue of undamaged information verdict a top-secret arrangement. Here, there are definitely not strong ideas or ecological calculation for respective admission, dissimilar to supervised learning. There's a portion of unsupervised learning procedures such as Fuzzy Logic, K-means Clustering, Association Rule Learning, Hidden Markov Model, Gaussian Mixture are popular unsupervised learning algorithms.

4. Literature Survey

Numerous researches are proposed by scholars in the concept of network layer attack detection in MANET by using Machine Learning Algorithms. In this situation, ephemeral assessments of some significant contributions to the previous literatures are obtainable in below table 1.

Table. 1. Comparative analysis of existing methods

Author & Year	Attack Type	Methodology	Advantage	Disadvantage
Ms. Katakam Tejaswini, Mrs. Yannam Adilakshmi [11] & 2020.	Black Hole Attack	Here, in this paper, Random Forest (RF) method is developed to identify and classify the attacks in MANET. In addition to examine the performance of the nearby nodes.	This projected RF method provides the advanced precision and improved recognition rate when associated with existing SVM method, Logistic regression and Decision tree.	On the other hand, the confusion matrix of RF method display additional false positive rate as soon as related through the method of logistic regression.
Gholamreza Farahani [12] & 2021.	Black Hole Attack	This research suggested a novel method to identify the attack by expending K-nearest neighbor (KNN) procedure for clustering and used fuzzy method for choosing the cluster leader in MANET.	Furthermore, this proposed machineries deliver a controlling obstacle to attackers, a supplementary level of protection termed as intrusion detection is frequently exploited to secure the MANET.	But then again the possibility attained is not appropriate, consequently, the reliance is not equivalent to untrustworthy. Because of these difficulties, a characteristic detection system is not appropriate for fresh atmosphere.
Muhannad Tahboush and Mary Agoy [13] & 2021.	Worm Hole Attack	This research proposed a hybrid Wormhole Attack Detection (HWAD) procedure to identify mutually in-band wormholes over K-means Clustering algorithm.	The projected HWAD method confirms that the attack is preserved for mutual kinds such as in-band and out-of-band. After analyzing with both the situations, the suggested HWAD method outclassed remaining methods in a fixed set of restrained limits.	Even though, this method overwhelming dynamism because of the inadequate energy source and comprises additional composite environments.
Masoud Abdan, Seyed Amin Hosseini Seno [14] & 2021	Worm Hole Attack	This research proposed a novel method to identify the attacks via Decision Tree (DT) procedure. A dataset with training process is essential to train prototypes in one training mode. Datasets could be attained from present situations or checks for ordering.	The proposed method achieves better extent of performance parameters such as precision and sensitivity. From the outcomes, it clearly shows the potential of the proposed DT method by attaining more precision and sensitivity when compared with existing classifiers.	On the other hand, the presentation of specificity parameter is having a reduced amount while associated through existing SVM and KNN classifiers.
D. Badru, P. Deepthi and B.Sankaraiah [15] & 2017	Sybil Attack	This research paper projected a Classification based inference rule which is exploited to separate the nodes and provides a trained ML processed nodes to eliminate Sybil attack from the assumed portion. This proposed method supports to remove difficult arithmetic Calculation commencing from a practical system network.	The significant advantage of suggested classification rule was discover some quantity of Sybil attacks and similarly minimalize the occurrence of false positive rate by appropriate approval percentage.	The suggested set of rules effectively identifies the attacks with nearly 100% precision but then again attacker speed and its density of node possibly will alternate the Percentage.

Pooja Rani et al [16] & 2017	Gray Hole and Black Hole Attack	This research recommended a machine learning based algorithm name called ANN. This method provides the security in contradiction of double attacks adjacent through the optimization method termed as Artificial Bee Colony (ABC) method.	The combination of suggested ANN and ABC method provides a slight increment in the rate of packet delivery ratio. Correspondingly, it is detected that the performance of delay by proposed ANN-ABC method achieves enhanced results when related with previous methods.	For the duration of this proposed progression, the probabilities of packet drop rises due to respective node which comprises a information used for a extensive interval.
Houda Moudni et al [17] & 2019	Black Hole Attacks	This research proposed a novel combination of hybrid method name called 'Adaptive Neuro Fuzzy Inference System (ANFIS) and Particle Swarm Optimization (PSO)' to identify the attack in MANET.	Here, the projected PSO is exploited to enhance the ANFIS presentation via altering the membership rules and formerly decreasing the inaccuracy. Furthermore, this suggested method contains a better recognition level and produces a less false alarm rate.	Even though, the recommended technique has deliberated and analyzed with a lesser amount of node counts. And does not analyzed with various node counts.
Mohanapriya M, Santhosh R [18] & 2021.	Black Hole Attack	Here, the authors have demonstrated a light weight method termed as secure-Dynamic Source Routing (DSR) to secure the MANET from the attack and permits transmission between the nodes when the attackers are existing.	The substantial benefit of this secure DSR technique was consuming less energy consumption while associated with existing methods; Furthermore it identifies the attack short of any computational overhead performance and similarly achieves smallest packet loss.	On the other hand, if the setup is jammed or in exceedingly vibrant, there is an intensification in route request packets which rises the overhead in the dispatching process.
Ngoc T. Luong, Tu T. Vo and Doan Hoang [19] & 2019	Flooding Attack	This research suggested a novel method name called 'Flooding Attacks Prevention using Routing Protocol (FAPRP)' throughout spreading the actual AODV procedure and incorporating the proposed process.	From the simulation outcomes, it clearly indicates that the recommended FAPRP accomplishes sophisticated misbehaving recognition level when related by previous procedures.	In definite circumstances, the mischievous path detection rate was unclear from the ordinary ones. Therefore, a monitoring node could not obtain packets commencing from a malicious node till some far ahead time.

Mukul Shukla, Brijendra Kumar Joshi [20] & 2020.	Worm Hole and Black Hole Attack	Here in this research, the author recommended a procedure which is a grouping of scalable-dynamic Elliptic Curve Cryptosystem and Ad hoc On demand Distance Vector (ECCAODV) procedure.	The projected ECCAODV process ensuing in improved outcomes through least energy depletion. So, the suggested practice concretes the manner and retains the prospective to secure the MANET.	Even though, the security of recommended schemes was completely based on the logarithmic problem resistance. Similarly the synchronization curve was nominated lacking the management amongst both groups might outcome in inaccuracies.
T.J.Nagalakshmi, A.K Gnanasekar [21] & 2021	Black hole attack	The k-means cluster classifier, Support vector machine classifier, random forest, and feature selection are utilized in this paper to detect the black hole attack as well as assess the node performance.	Excellent accuracy and attack detection for the intrusion detection system using k means cluster classifier with/without feature selection.	When the number of features increases, there is a risk of over fitting.
S.Sankara Narayanan G.murugaboopathi [22] & 2018	Wormhole attack	Worm hole attacks are more widespread in mobile ad hoc networks, and they're one of the hardest to spot.	Without the use of any specific gear, the technology aids in the detection of active and passive attacks. In comparison to SODV, the enhanced secure AODV finds PFR and RTT for each node rather than the entire network, resulting in improved service quality.	With increase in number of attackers, the systems may get complex.

5. Proposed system

Network Layer Attack Detection a feature is a characteristic of data in machine learning that is relevant to a ML task. Data sets are sometimes referred to as its dimensions. As a result, a data set with n features is referred to as a data set with n dimensions. In the present work the attacks are generated using Network Simulator 2.

Specification of simulator:

Area of simulation: 1500 * 1500

No. of nodes involved: 100

Routing protocol: AODV

Network traffic: Constant Bit Rate

Packet size: 512 bytes

Network: 802.11 MAC

The network layer attributes listed below are used to detect network layer attacks

1. The number of routes that have changed
2. The hop count alterations.
3. The sequence number's maximum number of modifications
4. The total number of hops
5. Mean difference between series numbers
6. Mean variation in hop counts
7. Delay percentage changes
8. Percentage change in receiver power
9. Fraction of change in packet transmitted count
10. Fraction of change in the number of neighbors
11. Mean percentage change in neighbor count with all neighbors.
12. Percentage change in packet drop ratio.

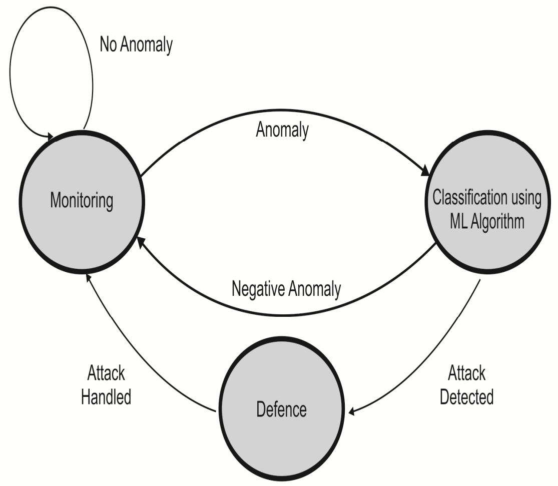


Figure 9 : Attack Detection using ML

An intelligent method for attack recognition in MANET[8] by means of cross layer method. In addition, display a prototype of SVMs, and AI methodologies for distinguishing the sink hole attack. The projected set of rules is employed to advance the precision of organization. As well as the efficiency of novel exemplary for enlightening recognition accurateness, that is established over numerous models. But on the other hand, cross layer method was not totally removing the layered process and not even incorporating every layer.

In [9], the author has proposed a "Epilson Swarm Optimized Cluster Gradient and deep belief classifier" for attack recognition in MANET. The projected method focuses on the problem of node flexibility and vitality to develop a clustering procedure stimulated through Dual Network Centrality for cluster leader appointment. The performance of suggested processes is considered in terms of dissimilar constraints for instance memory depletion, recognition rate and calculation time for classifying and separating the attacks. The outcomes display that the suggested technique expansively reduces the circulation, complete memory depletion and preserves an extraordinary attack recognition rate through negligible calculation time.

In [10], the author has demonstrated a Method for Detection and Prevention against Security Attacks in MANET. It is executed by means of Type 2 Fuzzy method that deliberates data from packet header. In preprocessing stage, arithmetic regularization and programming structures are deliberated which is appropriate for some appliances. In the process of feature extraction, Mutual Data is exploited and obtain ideal features set for classification, where Bootstrapped Optimistic Procedure through ANN is utilized, that classifies packets and formerly Association rule are exploited categorize whether the attack is regular or infrequent.

6. Results and discussions

The following metrics were used to calculate the performance metrics of the network layer attack detections in this study..

$$\text{Detection Rate} = \frac{\text{Number of Attackers identified}}{\text{Number of Attackers available in the networks}}$$

$$\text{False positive rate} = \frac{\text{False positive}}{\text{True negative + false positive}}$$

$$= \frac{\text{Abnormal node}}{\text{Numbers of Normal Nodes}}$$

$$\text{Accuracy} = \frac{\text{True Positive + True Negative}}{\text{(True Positive + True Negative + False Positive + False Negative)}}$$

False Positive = Normal nodes identified as abnormal nodes
False Negative = Abnormal nodes identified as the normal nodes
True Negative = Normal nodes identified as the normal nodes
True Positive = Abnormal nodes identified as the abnormal nodes

Table –2 Accuracy

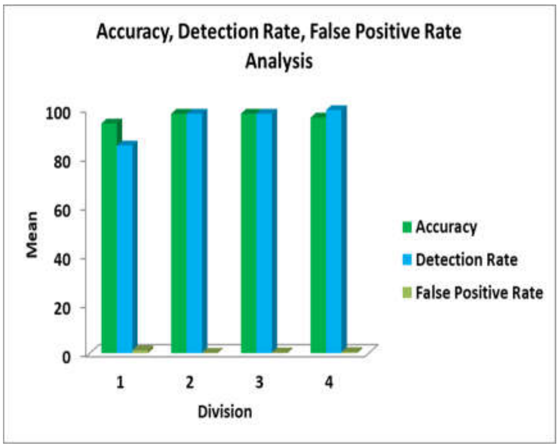
Division	Node	Mean	Std Deviation	Std Error
1.00	15	94.00	0.00	0.00
2.00	15	98.00	0.00	0.00
3.00	15	98.00	0.00	0.00
4.00	15	96.44	1.51	0.360

Table – 3 Detection Rate

Division	Node	Mean	Std Deviation	Std Error
1.00	15	85.00	0.00	0.00
2.00	15	98.00	0.00	0.00
3.00	15	98.00	0.00	0.00
4.00	15	99.52	1.406	0.336

Table – 4 False Positive Rate

Division	Node	Mean	Std Deviation	Std Error
1.00	15	1.15	0.00	0.00
2.00	15	0.199	0.00	0.00
3.00	15	0.299	0.00	0.00
4.00	15	0.800	0.00	0.00



The thorough analysis of the four divisions designed in the current work is shown in table 2, 3, and 4. The accuracy of the model is 97 percent, and the assault detection rate is 95 percent, which is a very high rate for a method designed with feature selection. This feature selection method performs better than other detection methods which do not have feature selection. Furthermore, the false positive rate of 0.612 was incredibly low in the strategy that used feature selection.

CONCLUSION

This research delivers an outline for creating the significance of analysis and it offers route for the research enquiries and assumptions. In order to understand the recent security problems concerning MANET, this review of collected works was the initial stage that facilitated the improvement in-depth information on various security attacks associated to MANET. This collected works analysis facilitate to recognize that numerous attacks on MANET have established a slight consideration from exploration communal in terms of appropriately describing and classifying network layer attacks. To improve the security concerns, an amount of security methods are already suggested in previous works. From that, Machine Learning approaches have higher prospective to discover unobserved or unfamiliar attacks, therefore it has turned out to be a passionate select between scholar’s group. This research paper has expansively characterized numerous ML approaches dependent security in MANETs. And it will support the scholars to apprehend the contemporary progression of various network layer attacks and its security processes.

REFERENCES

[1] Yasin, Adwan, and Mahmoud Abu Zant. "Detecting and isolating black-hole attacks in MANET using timer based baited technique. " Wireless Communications and Mobile Computing 2018 (2018).

[2] Gurung, Shashi, and Siddhartha Chauhan. "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET." Wireless Networks 25, no. 3 (2019): 975-988.

[3] Hammamouche, Assia, Mawloud Omar, Nabil Djebari, and Abdelkamel Tari. "Lightweight reputation - based approach against simple and cooperative black-hole attacks for MANET." Journal of information security and applications 43 (2018):12-20.

[4] Ponguwala, Maitreyi, and D. R. Rao. "Secure group based routing and flawless trust formulation in MANET using unsupervised

machine learning approach for IoT applications" EAI Endorsed Transactions on Energy Web 6, no. 24 (2019): 160834.

[5] Ramesh, Swaminathan, Calpakkam Yaashuwanth, and Bala Anand Muthukrishnan. "Machine learning approach for secure communication in wireless video sensor networks against denial-of-service attacks." International Journal of Communication Systems 33, no. 12 (2020): e4073.

[6] Marathe, Nilesh, and Subhash K. Shinde. "ITCA, an IDS and trust solution collaborated with ACK based approach to mitigate network layer attack on MANET routing." Wireless Personal Communications 107, no. 1 (2019): 393-416.

[7] Arappali, Nedumaran, and Ganesh Babu Rajendran. "MANET security routing protocols based on a machine learning technique (Raspberry PIs)." Journal of Ambient Intelligence and Humanized Computing 12, no. 6 (2021): 6317-6331.

[8] Usha, G., and K. Mahalakshmi. "Machine Learning Cross Layer Technique to Detect Sink Hole Attacks in MANET." International Journal of Modern Education and Computer Science 8, no. 7 (2016): 61.

[9] Dilipkumar, S., and M. Durairaj. "Epilson Swarm Optimized Cluster Gradient and deep belief classifier for multi-attack intrusion detection in MANET." Journal of Ambient Intelligence and Humanized Computing (2021): 1-16.

[10] Islabudeen, M., and MK Kavitha Devi. "A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks." Wireless Personal Communications 112, no. 1 (2020): 193-224.

[11] Tejaswini, Ms Katakam, and Mrs Yannam Adilakshmi. "Black Hole Attack Detection Using Machine Learning Algorithms in MANET–Performance Comparision." International Research Journal of Engineering and Technology (IRJET) Volume: 07 Issue: 06 | June (2020).

[12] Farahani, Gholamreza. "Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks." Security and Communication Networks 2021 (2021).

[13] Tahboush, Muhannad, and Mary Agoyi. "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)." IEEE Access 9 (2021): 11872-11883.

[14] Abdan, Masoud, and Seyed Amin Hosseini Seno. "Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad-Hoc Network (MANET)." (2021).

[15] Badru, D., P. Deepthi, and B. Sankaraiah. "Analysis on intrusion & detection of sybil attacks in mobile adhoc networks using classification." IJARF 4, no. 3 (2017): 1-5.

[16] Rani, Pooja, Sahil Verma, and Gia Nhu Nguyen. "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network." IEEE Access 8 (2020): 121755-121764.

[17] Moudni, Houda, Mohamed Er-rouidi, Hicham Mouncif, and Benachir El Hadadi. "Black hole attack detection using fuzzy based intrusion detection systems in MANET." Procedia Computer Science 151 (2019): 1176-1181.

[18] Mohanapriya, M., and R. Santhosh. "Detection and elimination of black hole attacks in mobile ad hoc networks." Materials Today: Proceedings (2021).

[19] Luong, Ngoc T., Tu T. Vo, and Doan Hoang. "FAPRP: A machine learning approach to flooding attacks prevention routing protocol in mobile ad hoc networks." Wireless Communications and Mobile Computing 2019 (2019).

[20] Shukla, Mukul, and Brijendra Kumar Joshi. "A novel approach using elliptic curve cryptography to mitigate Two-Dimensional attacks in mobile Ad hoc networks." Materials Today: Proceedings (2021).

[21] T.J. Nagalakshmi, A.K gnanasekar, " Machine learning models to detect the black hole attack in wireless ad hoc network." Elsevier Material Today: Proceedings (2021).

[22] S.Sankara Narayanan, G.Murugaboopathi, "modified secure AODV protocol to prevent wormhole attack in MANET",john wiley & sons ltd, special issue (2018)