International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 909–924

A Virtuous Reckoning on security enhancement of mobile Adhoc network using artificial intelligence

A.Vani
Assistant Professor
Chaitanya Bharathi Institute of Technology
Hyderabad-75
avani_ece@cbit.ac.in

Abstract

Mobile ad hoc networks (MANET) have revolutionized our culture through their self-configured autonomous communications modes that have no framework and have thus been aimed at exploring means of making good use of the potentials of MANETs, more and better. The latest introduction of new machine learning technology has enabled the creation of the best protocols for artificial intelligence. Mobile ad hoc networks (MANETs) face different problems related to protection caused by malware attacks. Its transient existence makes nodes more sensitive to threats by nodes or by attackers as any node acts as a router to transfer data without centralized control. Therefore, to identify the wrong entry of misbehavior nodes, MANET requires very precise security policies. The networks perform better if the nodes are confident and cooperate correctly. This paper proposes an effective artificial intelligence algorithm-based security framework as an approach that recognizes and distinguishes insider threats in real-time by categorizing data packets as normal or abnormal, as well as identifying and detecting packet falling nodes through the vector support and logistic regression machine. The results suggest that LR was higher than SVM with an exact prediction rate of 97 %.LR is therefore more appropriate to identify malicious attacks in MANETs.

Keywords: Mobile ad hoc network, Security, Attacks, Artificial intelligence, support vector machine (SVM), Logistic regression

1.Introduction

Wireless technologies have achieved a phenomenal development concerning the implementation of connectivity in the 21st century compared to past times. Contrary to the cable component, there are various benefits of the wireless network. Wireless mobile nodes can demonstrate a complex topology, connect different variations in capability, and can provide endless results. Wireless techniques also catalyze low-cost, but efficient, mobile communications transceivers [1]. Mobile networks are known as mobile ad-hoc networks, dependent on technology and infrastructure (MANET). The nodes themselves serve as adapters in MANETs which makes the network less costly. In various environmental contexts, the existence of the revolutionary change of MANETs contributes to their high speed [2]. Also, MANETs can demonstrate a conceptual disposition dependent on customers' wishes. MANETs are adapted to an ad hoc vehicle network (VANET).

MANET is primarily responsible for connecting and finding an appropriate path to data packet transmission and then transferring packets to the existing network. Because routing is performed by the hosts/nodes, they adopt a packet transmission protocol that can be one-hop or multi-hop. In an area where economic growth is impossible or unwanted [2, 3], MANETs are seen as a transitional system. The MANET scheduling algorithms realize the importance to create routes and transport packages to the endpoint from the origin [4]. As the related topology is

ISSN: 2233-7857IJFGCN

complex, multiple device nodes join and exit the network in a certain case. Because of the lack of facilities, MANETS is always at risk of drowning and crises [3, 5], leading to a lack of information security.

The safety issues in MANETs can arise from

- Lack of appropriate and strong hacker intransigence
- Probability of catastrophic threats in the MANET
- Dynamic topology
- Massive energy factor influence in mobile nodes
- Federated framework and structure without utility services etc.

The MANETs can be summed up in two types of security risks, namely routing security and data security. MANETs use proactive protocols to detect attacks, and constructive protocols to address opposition against hackers in the network. Because of their infrastructure-free existence, MANETs do not have the main increase in the reliability that is useful to create a network link, thereby contributing to the lack of a confidence routing system. In comparison, internal and external intrusions are several times more likely [6]. These attacks are primarily aimed at the mobile node activities and data from these nodes. MANETs often face internal and external attacks, which are more important for internal attacks because they affect mobile node operations directly. The nodes transmit illegal transmission of misinformation to nearby mobile nodes during the internal attacks, which makes the adjacent nodes fully controllable and weaken the attackers [4, 5]. Two types are active and passive for unauthorized threats. If the attackers attack nodes specifically, they are called active attacks and if they do so inherently, they are called passive attacks.

As the MANETS technologies are growing, the privacy issues that are relevant to them are also increasing. Although a variety of methods are necessary to protect Manet's systems, a mechanism needs to be developed earlier to anticipate and identify the attack and intrusion [6]. The architecture of an Artificial Smart MANET is directed at the conception of smart protocols to identify and address these risks and security concerns. The paper first highlights current safety risks and remedies and also reflects on the use of artificial information to guarantee high protection for MANETs.

2.OVERVIEW OF MOBILE AD HOC NETWORKS

In1996, a MANET response group was set up by the Internet Engineering Task Force (IETF) to standardize data collection in ad-hoc mobile networks. The main goal is to normalize the IP routing method functionality for wireless applications [6,7]. The example of MANET is seen in Figure 1. MANET is a dynamically structured network composed of two or more mobile devices that don't require manufacturing as a whole or unified fixed administration [4].

ISSN: 2233-7857IJFGCN

Fig 1: Mobile Adhoc Network
https://www.androidsim.net

Each MANET node is equipped with architecture for wireless transmission/receiver which allows the coordination of nodes within the radio communication distance with other nodes [6]. Even though two nodes are outside the distributing range, a data packet can still be transmitted and interacts in many hopes if the other routing details on MANET are open. Per node should therefore be a wireless connection and host concurrently. As MANET was originally conceived for the defense and relief efforts because of its "infrastructure-less" existence, networking networks and mobile nodes are spread over a domain of war and no connectivity is available to support them shape a system [8].

In recent times, MANET applications have developed and are progressively being utilized in many critical places, from industrial, enterprise, and weapons systems, as MANET networks can be established and maintained without current facilities or communication between individuals[7,8] for instance in emergencies, battlefields, campuses, and meetings. Thus, as one of the commonly deployed ad-hoc networks, the security problem of MANET has been one of the main issues.

3.Literature survey

Since its conception, machine learning has become an important part of wireless communication. Machine learning refers to a range of ways to 'read' the computer that is to say to gradually enhance its accuracy and categorize large quantities of data [9]. The data can either have prepared responses, or they can be considered non-supervised learning, where the system attempts to deduce significance from correlations in data sets. The configuration is called supervised training. A variety of works have used the development of effective algorithms for MANETs via machine learning principles.

Feng and Chang et al [10] designed a system using an H-SVM to forecast potential node position and to calculate the level of complexity that is existing in networks to apply successful demodulation algorithms.

In an approximation of channel parameters in CR (Cognitive Radio), Choi and Hossain et al [11] have used the Hidden Markov Model [HMM]. The aim is that a secondary user (SI) will gain access to the empty primary user (PU) without disrupting propagation through the PU efficiently to detect any parameters influencing a channel. The criteria then are PU traffic pattern, PU to SU channel growth, and SU noise density. The fundamental states describing PU activities are concealed from the SU, as the PU is modeled on the Markov mechanism and this former can only perceive the outcome [12]. These secret states are inferred from Bayesian learning. Bayesian learning is a deduction of the normal distribution from the reference series of the dependent variable. This assignment is based on the EM algorithm. While this paper recognizes a special solution, it also points out that in some situations the HMM model can't be identified due to the failure of the EM algorithm. It is also relevant only to HMM models, as well as issues that make it non-versatile.

Donohoo et al. [13] have researched several wireless data analysis methods to prevent energy-efficient parameters. The list of methods to be investigated involves linear discrimination [14], linear regression, k-nearest neighbor, vector support, and neural networks[15]. The list of approaches is also discussed. The Bayesian method was used in Linear Discriminate Analysis (LDA). The input data is regarded as random parameters of a prior distribution. It has proven to be a fast and impartial algorithm, but it is not good for data with very specific supersymmetric computations.

ISSN: 2233-7857IJFGCN

Pravin R. Kshirsagar et al. [4] presented a hybrid Artificial Neural Network Model for the classification and prevision of various neurological disorders and also designed Hybrid Heuristic Optimization for Benchmark Datasets [5]. He also discussed the Performance Optimization of Neural Network using GA Incorporated PSO [6]

Alnwaimi et al.[21] have implemented enhancement models in a distributed communication environment to self-configure/optimize femtocells (HN). The HN is a "layer of LTE femtocells (FCs) in closed-access, which is superimposed on an LTE radio access network" As the FCs are self-organizing, the radio atmosphere is sensed and its specifications can be adjusted to prevent network disruption.

Alireza, S. et al. in [16], This paper proposed a multi-model called on the MANET PSO algorithm. The PSO algorithm is higher than GA multi-cast route accuracy and speed. The emphasis on renewable energy and delay is the subject of multicast routing. This implies in particular that the node can be selected with less electricity usage and a multichannel tree built with less time delay. The concern was expressed here as a concern with PSO. It was proposed that a new algorithm for multicast routing would draw on the PSO algorithms.

Al-Ghazal, M. et al. in [17], This paper is implemented in mat lab based on the GM and Cluster Heath Gateway (CGSR) method to enhance routing of cluster analysis. This paper is published in the following sections: Genetic algorithm (GA) keeps up to date on neighboring network state knowledge, and GA structures make systems autonomous. Genetic algorithms can determine the fastest route from sender to recipient in the network, but they don't need to be the shortest route, because the node can quickly and easily upgrade routing data to continuously change local topology, causing fewer connection fragments and growing overhead of lower MAC layer.

4.MANET Security Challenges

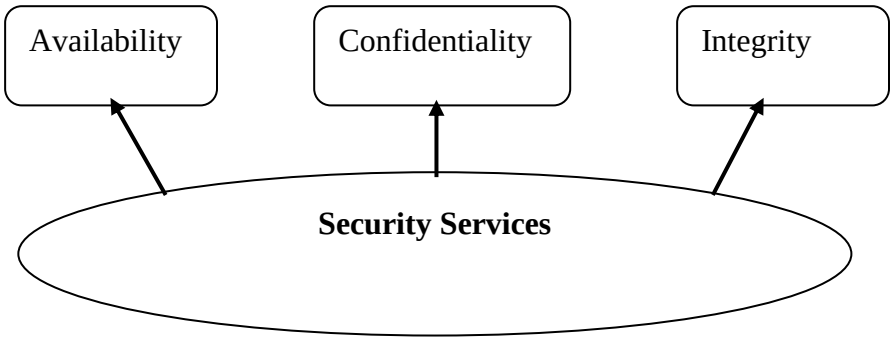
Certain security issues in MANET have arisen from research areas in ad hoc networks [9]. Two critical aspects of security generally exist:

- Security services
- Attacks.

Services refer to such protectionist measures to keep the network safer, while attacks, a security service are defeated by network defects.

4.1 Security Services

Security in wireless networks is a critical condition in comparison with wired networks. Security, particularly for those authentication applications, is a significant matter for ad hoc networks [10]. Wireless data security is becoming increasingly relevant as the use of cellular or laptop devices is growing enormously.



ISSN: 2233-7857IJFGCN

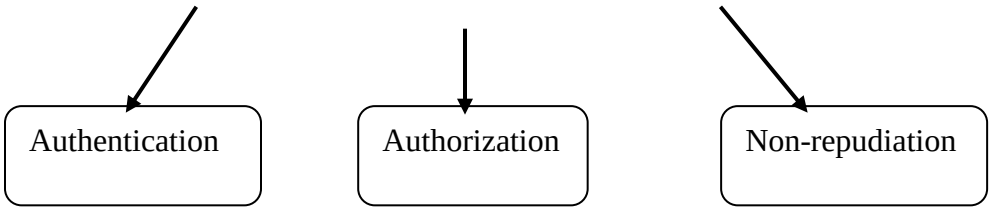


Fig 2: Security services in Manet's

MANET's protection is harder to accomplish and complex when there is no main controller or ground station. In reality, [11] the Adhoc networking security issue is not only the ad hoc networking themselves, but the connection to other networks which it supports.

1) Availability: Availability ensures that the funds are available at a reasonable time to approved parties. Data, as well as facilities, are offered. Despite a denial of access, it guarantees the survival of the data network [6, 7].
2) Confidentiality: Confidentiality guarantees that only authorized persons view computer-related resources. Security of the data exchanged via a MANET. Any attacks on transparency including unauthorized downloading of the message must be covered
3) Integrity: Integrity means that only approved persons or authorized parties may change properties. Integrity ensures that a message is never altered [5].
4) Authentication: Authentication is simply the guarantee of verification and not of impersonation of parties in the conversation. The authorized nodes can enter the network remedies.
5) Authorization: This property grants various rights of entry to various classes of consumers. For eg, only a network manager can control a network.
6) Non-repudiation: Failure to repudiate would allow perpetrators to be identified long after the attack occurs. This avoids the denial of hackers. This means that the creator does not doubt that the letter has been delivered [10, 13].

4.2 Attacks

MANET was popular for malicious nodes due to unique editions like hop-by-hop communication, wireless media [12]. The following are some of the key attacks in MANET:

4.2.1 Passive Attacks

Passive attacks do not interrupt routing networks activities or contact among nodes, but attempt, through reacting to the congestion, to find and get meaningful information. Passive attacks are normally hard to identify, making defending against passive attacks more complicated. Eavesdropping, traffic control, and analysis [8, 1] are examples of passive threats.

- Eavesdropping attacks: Eavesdropping is identified as a passive attack. The correspondence between nodes is not interrupted but packets and communications are intercepted and read by unauthorized nodes. In MANET mobile nodes mostly use the Frequency band in communications and broadcasting networks. Thus, the transferred packets can be eavesdropped on to capture, copy, save, or review data packages [15].

ISSN: 2233-7857IJFGCN

- Traffic analysis attacks: Traffic analysis is an intrusion where the MANET network traffic is observed by an attacker, which deducts critical and essential information from services and the corresponding device. The hacker then analyses the traffic and tracks modifications to the traffic pattern in the network. Confidential material covers node identity, MANET traffic habits, and their modifications. One of the most delicate safety assaults against MANET remains unresolved in the alleged traffic analysis [7].
- Monitoring attacks: Confidential information can be monitored by an intruder or malicious node, but the data cannot be changed or modified.

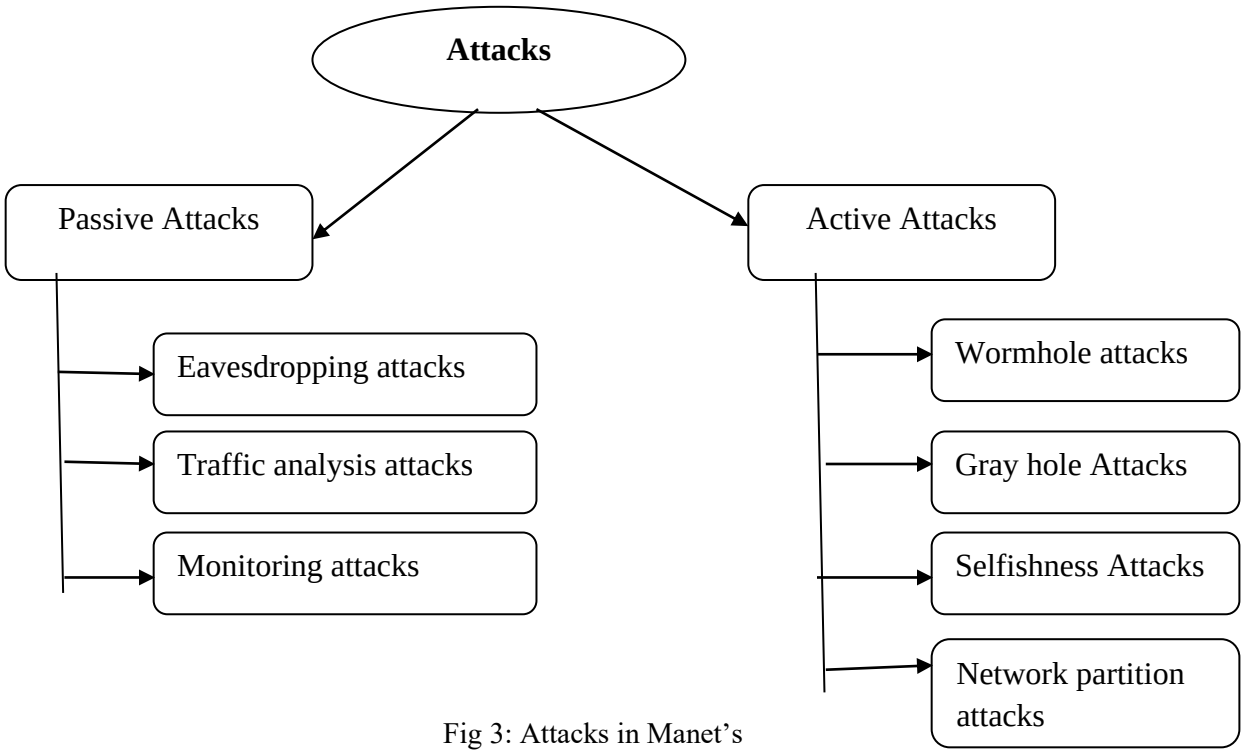


Fig 3: Attacks in Manet's

4.2.2 Active Attacks

A deliberate effort to perturb or hinder the regular operation of the MANET specification is to inject its information into the data stream [13]. This attack aims to modify or remove data exchanged in an ad-hoc network to limit the accessibility, validate or attract packets destined for the other nodes. Examples of successful attacks can be found in the following

- Wormhole attacks: Wormhole aims at a more unambiguous mode of active attack, which comprises two malicious nodes that provide a channel (virtual link). Where routing control signals have to be tunneled, wormholes can be used in the face of a routing algorithm on-demand like AODV or DSR, to prevent any other route than the wormhole.

ISSN: 2233-7857IJFGCN

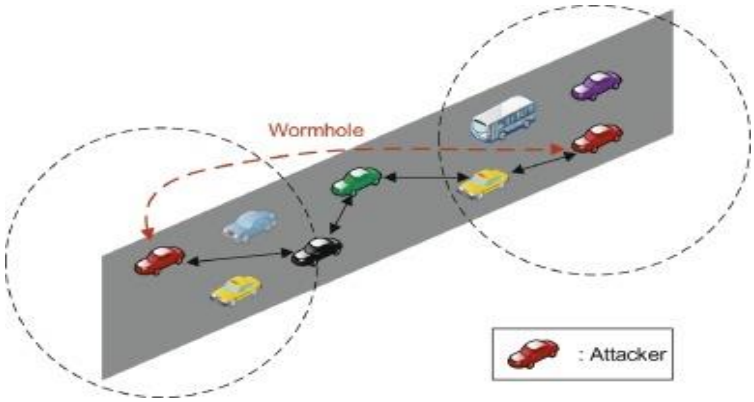


Fig 3: Wormhole attack on Manet
https://www. 2Fnetworksimulationtools.com

- Gray hole Attacks: The Grayhole attack was trickier than the black hole attack; the intruder picked up some of the packet headers randomly, then dropped packets from some nodes, and then forwarded packets from the other nodes. Unless a reliable routing algorithm can block Grayhole attacks quickly.
- Selfishness Attacks: For purposes such as preserving system resources, the node in the selfishness attack doesn't serve as a conduit to other nodes. If the node does not want network access, it does not also engage in route optimization and transmission [1, 14]. Selfishness nodes want to conserve their assets as they use the facilities and resources of others.
- Network partition attacks: This ad hoc network is split into sub-networks that do not interact with nodes on a fixed path.

5.Artificial Intelligence and Security

MANETs and their protocols search for a multitude of security problems and risks. Intelligent network development is one way to secure and prevent the nodes in the MANETs. A method to transform nodes in the network to intellectual and intelligent can be hypothesized on artificial intelligence (AI) [15,16]. The insight contained in the nodes enables them to decide independently like people. Artificial intelligence is also used for sports, logic, and analysis of natural languages, and so on. Artificial intelligence is focused on mathematical, biological neuronal, computer, linguistic and engineering principles.AI may also be used in wireless networks to improve other considerations, such as efficiency and speed, in addition to the security implications [17]. The efficiency of networking in a wireless network is improved by Q-learning and automatic learning. By using Bayesian Leaning and k-means clustering, the channel power of the network could be enhanced. Perspective methodology and decision-making tree may be used in wireless network intrusion prevention systems. A Structural Equation Analysis could improve the connectivity process in a wireless network.

For the following aspects, in MANETs, artificial intelligence techniques may be used to improve security [2, 10,14]:

1. Managing big data volumes: The difficulties in information collection are huge in MANET and manage the data file and packet protection represents a difficulty. AI could be used to pick the corresponding data from all log files and device alerts produced. The use of AI could make the data collection process more complicated.

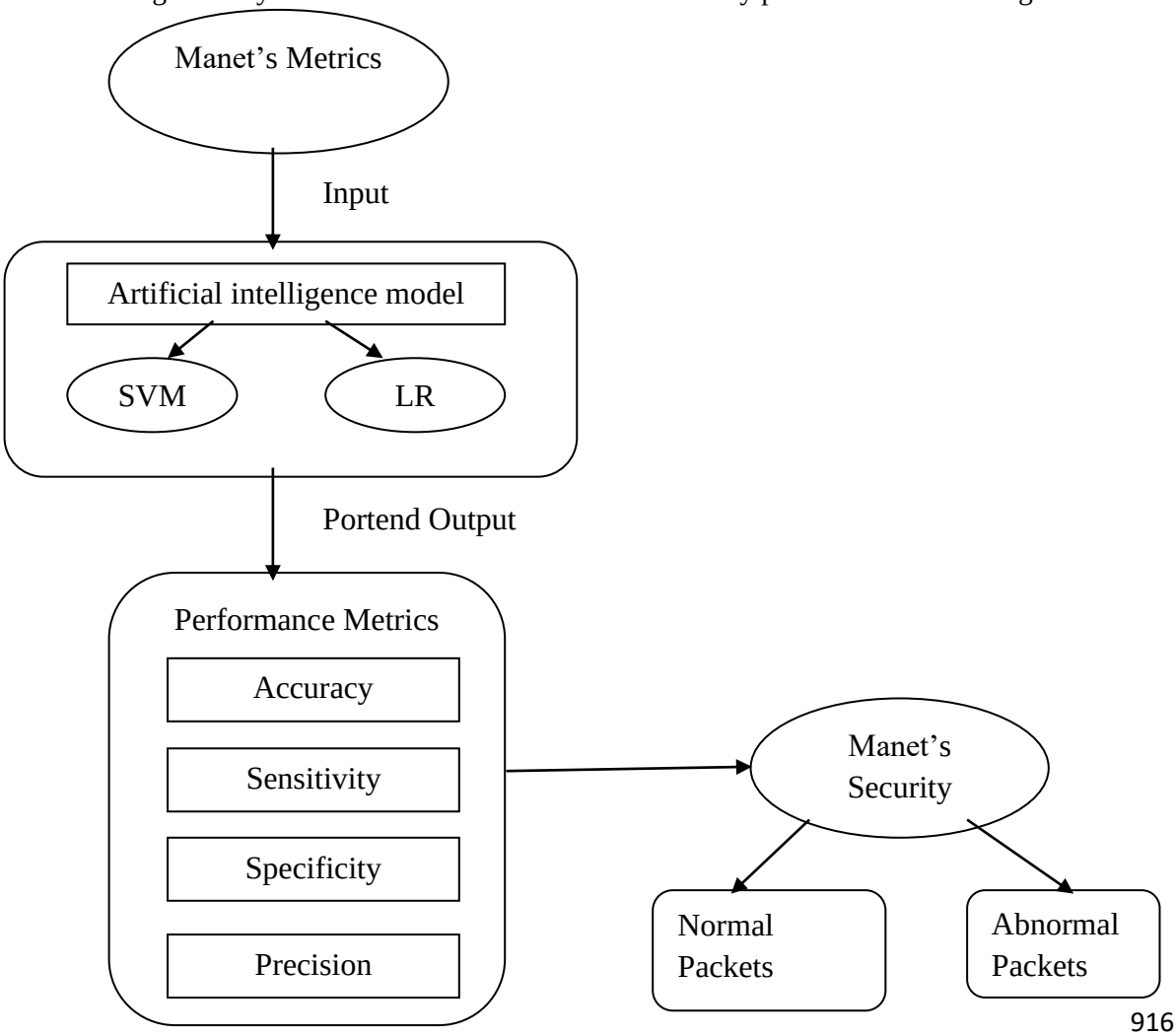
ISSN: 2233-7857IJFGCN

2. Exposure to risks appropriately: A node like MANET that adds and leaves nodes rapidly is ever threatened. AI can help with extreme accuracy in discovering enemies or attackers even quicker. Ai technologies utilize both the consumers' and the network's self-learning and study conduct methods. Decisions are taken in the network based on the known behaviors.
3. Increased reaction time: highly accurate and accurate hazard identification and higher information processing with a high degree of certainty in detecting safety risks are essential to the AI.

Several threats and opponents currently arise in a network and must be identified and obstructed before significant allergic events can occur. These threats can take the form of apps or other abnormalities [5]. A decentralized MANET has an extremely high safety risk and is a major challenge to secure the nodes in the network. In addition to that, in a MANET node, the chances to be vulnerable to internal and external attacks are often enormous to provide higher rates of packet supply and connectivity. Formatted protocol registration in MANET is rather boring because the definition is based on cost efficiency. Another element that chattels protection in a MANET is parallelization [9, 16]. The continuous flow of nodes in and out of the network makes it more difficult to update security measures on all nodes of a MANET at once. The syncing of safety protocols to routing protocols is another problem in the security provision.

6. METHODOLOGY

The technique for choosing an analytical model in MANETs based on activity packets is shown in Fig. 5



ISSN: 2233-7857IJFGCN

Fig 5: Block diagram of the analytical model in MANETs based on packets a behavior

6.1 Model Parameters

The specifications of the models are given by the parameters used:

- Dependent
- Independent.

The independent variables are data from MANET packages, which are inputs in the simulations in the form of metrics like PDER and PMMR. These measurements were used to evaluate each node's activity and efficiency in the process. However [16], PMMR metrics were referred to as PMOR and PMISR. The efficiency of the models is determined by the accuracy rate. Below are their calculations:

$$PDER = \frac{Number\ of\ packets\ transmitted}{Total\ number\ of\ incoming\ packets} \qquad 1$$

$$PMMR = \frac{Number\ of\ packets\ misrouted}{Total\ number\ of\ incoming\ packets} \qquad 2$$

The increase the likelihood of PDER in Equations 1 and2, the higher the mobile node results PMMR displays changes found during transmitting in the packet content caused by attacks. Any of the network nodes may be achieved inadvertently or deliberately. It may also be caused by nodes that transmit packets during contact to incorrect addresses [15]. These measures are used for assessing LR and SVM's results. The quantities to be estimated are the dependent variables. They have MANET data objectives, in which the quality of the class relies on the metric.

6.2 Model structure

This section presents the construction of the models:

- SVM
- LR.

6.2.1 Support vector machine: Consider the issue of splitting data from MANET packets into normal and abnormal packets [13] of two different classes for the SVM model and illustrated in equation 3 below

$$G(y\{z,b\}) = z.y + k = 0 \qquad 3$$

Where G is the function that divides the two classes.
y is the true n-dimensional input sequence of packet data and n signifies MANET data subsets.
z is the equilateral element or support vector for the design of the curved SVM.
k is a concept of bias used to characterize the parallel spectrum of the original hyper-plane.

$$z.y + k \geq +1 \qquad if\ p_i = 1 \qquad 4$$

ISSN: 2233-7857IJFGCN

$$z.y + k \leq -1 \qquad if\ p_i = -1 \qquad 5$$

The two parallel, hyperplanes that divide the two groups into normal or abnormal packets are equations 4 and 5. Equation (4) refers to a linear MANET data hyperplane with regular packet support vectors. The label= 1 is a vector depending upon the normal packet class.

Linear equation (5) indicates the side of the abnormal packet hyperplane separation. The label= -1 indicates an abnormal packet vector, and y denotes the binary value input data.

6.2.2 Logistic regression: LR is given by:

$$V(t) = \frac{e^t}{e^t + 1} = \frac{1}{1 + e^{-t}} \qquad 6$$

The metrics denote independent variables in t € Ᵽ. Where Ᵽ denotes the real numbers. Dependent V (t) variable may represent "normal packet" or"0" or "abnormal packet" or"1".[10, 11].

6.3 Data Evaluation

Model evaluation: Classification technique and uncertainty matrix used to test the efficiency of the built models. A cross-validation is a mathematical approach that examines the learning algorithms and assesses them by splitting data into two categories: training and a test set [30]. It also used the testing package to train the models for both SVM and LR models, while the training dataset tests or validates the models [2,4, 5]. We used the confirmation of the k-folds. To test the output of the built models, the neural network is used. An uncertainty matrix can then be used to calculate the amount of accurate and wrong MANET packet data estimates.

Accuracy is a performance calculation of the correct grade rate as defined by ACC. The ratio of accurate prediction and total prediction is determined in Eq 7

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \qquad 7$$

The sensitivity analysis is to measure the real positive percentage of non-diabetes modules, properly defined. As indicated in Eq 8, this can be determined as

$$Sensitivity = \frac{TP}{TP + TN} \qquad 8$$

The specificity is measured as a genuinely negative rate, which shows the amount of right classified software modules and can be expressed in Eq 9.

$$Specificity = \frac{TN}{TN + FP} \qquad 9$$

Precision is defined as the ratio of True Positive and (true and false) positives. It can be expressed as in Eq 10

$$Precision = \frac{TP}{TP + FP} \qquad 10$$

ISSN: 2233-7857IJFGCN

These criteria are used in both training and evaluation to measure the efficiency of SVM and LR models, which contrasts SVM and LR algorithms efficiency.

7. Flow chart for the logistic regression method detection of normal and abnormal packets

Detecting suspicious nodes using methods of artificial intelligence [16]. In our approach, we are using the Logistic regression (LR) technique for detecting and classifying malicious nodes according to the behavior of nodes as shown in Figure 6.

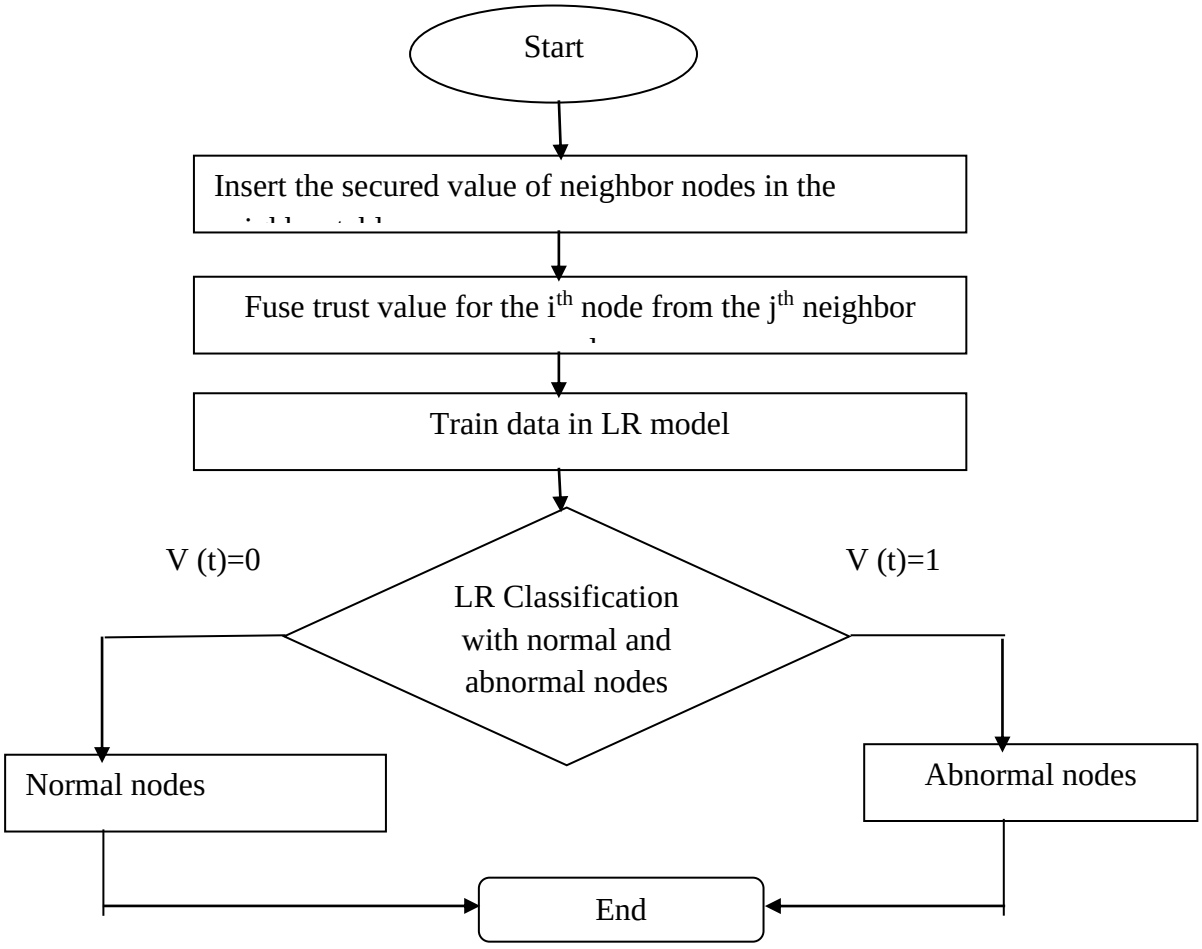


Fig 6: Flow chart for the logistic regression method detection of normal and abnormal packets

LR Misbehavior classification algorithm:

STEP 1: The logistic regression technique is used essentially to identify and limit the propagation of information across malicious nodes.

STEP 2: A collection of input data is provided for each input LR defined. In this method, LR captures the behavior, reinforces and classifies these nodes according to the node's behavior. All of the nodes are classified as either trusted or entrusted with the help of the LR classifier integrating with MANET.

ISSN: 2233-7857IJFGCN

STEP 3: Use the LR technique to classify two-class normal or abnormal nodes.

8. RESULTS AND ANALYSIS

The training samples of the data using the chosen Artificial Intelligence Algorithms, PDER, and PMMR are presented in this section to estimate models' efficiency as shown in figure 7.

Table 1: performance of SVM and LR algorithms

Algorithms	Accuracy	sensitivity	Specificity	Precision
SVM	93	92.45	87.89	93.01
LR	97	96.87	95.12	98.67

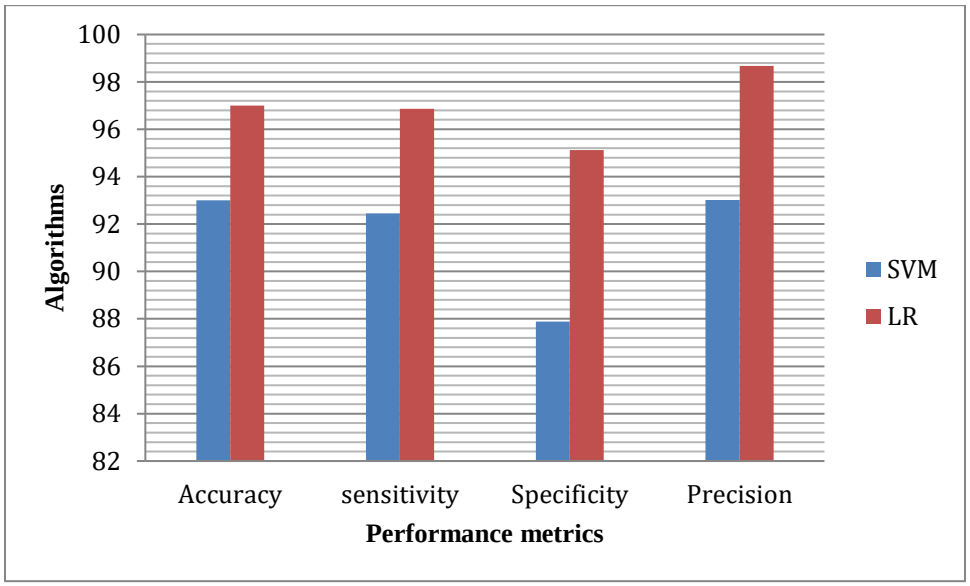


Fig 7: Performance of SVM and LR algorithm

SVM Analysis: This segment shows the effects of the SVM model classification. The data captured or arbitrarily gathered using the uncertainty matrix is shown in Table 1. It provides data on SVM's output in the MANET packet classification as normal or abnormal as transmitted or modified across the network.

LR Analysis: LR offers awareness and power on interactions and data traveling within the network between MANET packets. Table 1 displays the output parameters achieved with high precision in all stages from the uncertainty matrix. It is suggested that distributed MANETs packages are accurately labeled as normal or abnormal. That is, system performance interference or failure, or misleading routing information was detected appropriately.

We evaluated the output metric such as the packet delivery ratio and end to end delay to evaluate the performance of AI algorithms

(i) Packet Delivery Ratio: Complete number of packets sent by all nodes divided by the total number of packets.

ISSN: 2233-7857IJFGCN

(ii) End to End Delay: Packets first take some time to transmit the first packet from the source node and then withdraw the first packet from the target node.

(iii) Average Throughput: The average packet quantity is considered as throughput from the transmitter to the receiver.

(iv) Normalized Routing Overhead: The ratio of data streams to monitor packets across the channel of communication is calculated as the overhead routing.

Packet Delivery Ratio

This reduces the PDR for a packet drop attack according to the scheme suggested. To solve the problem, we took 40% of malicious nodes to evaluate the metric in the packet drop-out attack. The following figure 8 shows the similarity of the AI algorithm with the PDR falling attack.

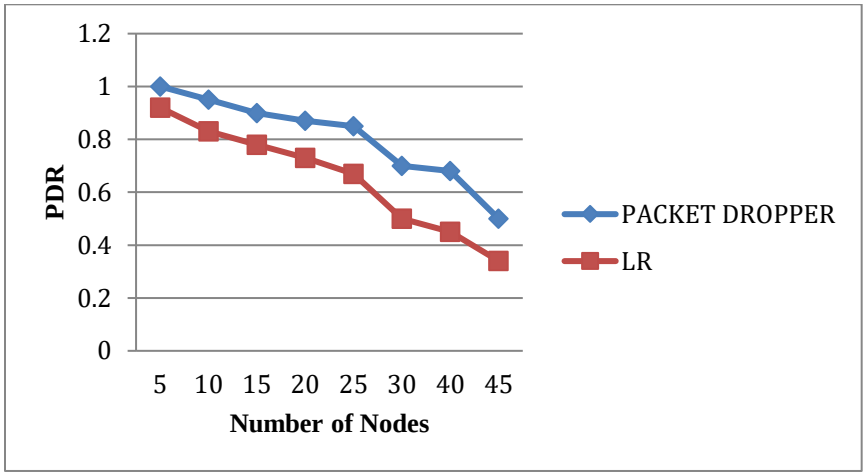


Fig 8: PDR during packet transmission

End to End Delay

It measures the average delay among senders and receivers by the data packet. The following figure 9 outlines the contrast of the planned scheme with the packet dropping attack about the end-to-end delay. In comparison with the designed method, the delay is raised in the package drop attachment.

ISSN: 2233-7857IJFGCN

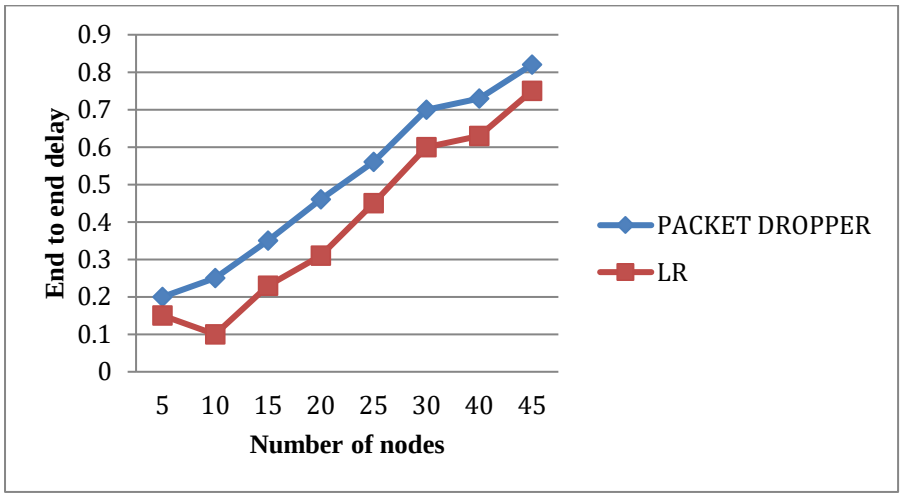


Fig 9: End to End delay measured during packet transmission

C. Average Throughput

It calculates the average effective packet transmission through a transmission medium from origin to destination. In this case, network output in the case of LR is improved as shown in figure 10.

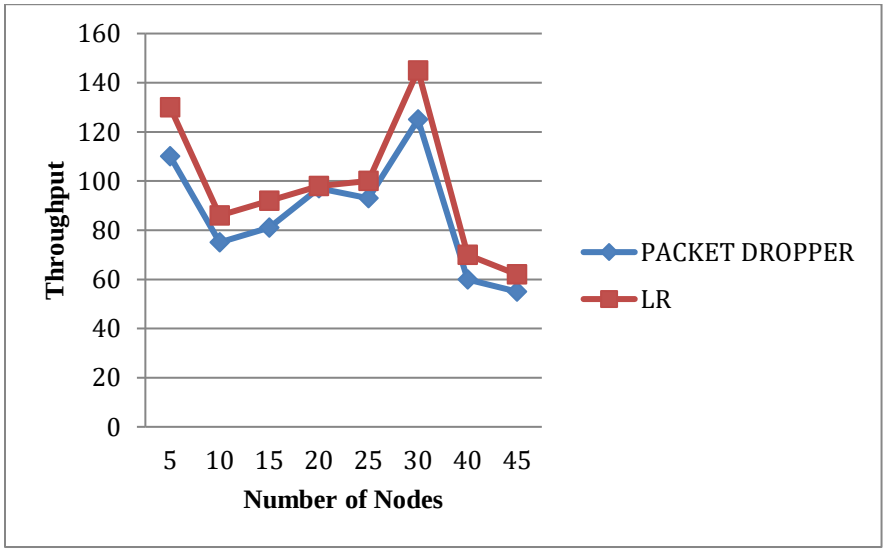


Fig 10: Average Throughput during packet transmission

D. Average Energy Consumption

It calculates the average energy used during the transmission period by mobile nodes. In comparison with the suggested technique, this increases usage in a packet dropping attack as illustrated in figure 11.

ISSN: 2233-7857IJFGCN

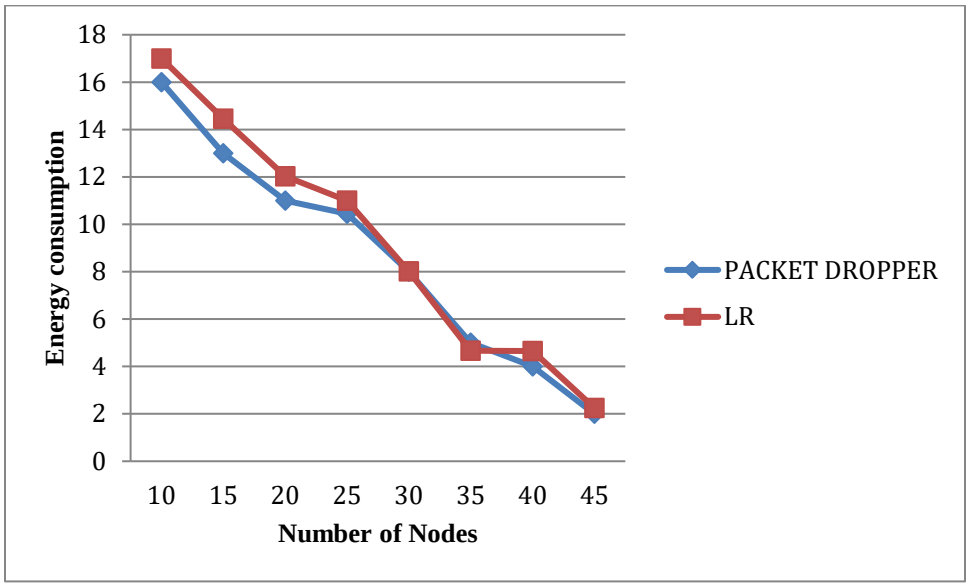


Fig 11: Energy consumption during transmission of packets

9.Conclusion

MANET is a network of cooperation with less autonomy. This feature leaves MANETs vulnerable to a range of threats like gray hole, wormholes, black hole, and other attacks that could violate interaction protocols' security and privacy. The consequences of the SVM and LR models are analyzed and discussed with Manet data packet data details. The objective was to find the best mathematical model based on packet dynamics for malicious MANET attacks. This is a high-precision and low-failure warning model for MANET packet interaction and network supply. The results showed that LR exceeded SVM 97 % while SVM showed 93 % predictive precision. This means that the detection or variations between the "normal" and "abnormal" MANETs of the SVM algorithm are difficult. LR has retained continuity in terms of accuracy, specificities, sensitiveness, and misidentification and FP rates as well as measured the Packet Delivery Rate (PDR), End to End Delay (E2ED), Average Throughput.Wireless network energy is of great importance in each node.

References

1. Mukesh Madanan "*Designing an Artificial Intelligent MANET to reduce and detect security threats and concerns*" In Proceedings of the 2006 14th IEEE International Conference on Network Protocols, 2020. ICNP'06, pp. 75– 84, 2006
2. Farhan Abdel-Fattah "*Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs*" IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) pp. 103–135, Springer 2019
3. Mandhare, Archana, and Sujata Kadam. "*Performance Analysis of Trust-Based Routing Protocol for MANET*." In Computing, Communication and Signal Processing, pp. 389-397. Springer, Singapore, 2019
4. Singh, A., M. Kumar, R. Rishi, and D.K. Madan, "*A Relative Study of MANET and VANET: Its Applications, Broadcasting Approaches and Challenging Issues*". Advances in Networks and Communications, 2018: p. 627-632.

ISSN: 2233-7857IJFGCN

5. P. Francis Antony Selvi et al., "*Ant based multipath backbone routing for load balancing in MANET*," IET Communications, 2017 vol. 11, no. 1, pp. 136-141,
6. P Kshirsagar, S Akojwar -2016,**"***Novel Approach For Classification And Prediction Of Non Linear Chaotic Databases***"**. International Conference On Electrical, Electronics, International Conference On Electrical, Electronics, And Optimization Techniques IEEE
7. Shuja J, Gani A, Shamshirband S, Wasim Ahmed R, Bilal K. "*Sustainable Cloud Data Centers: A survey of enabling techniques and technologies. Renewable and Sustainable Energy Reviews"* 2016; 62: 195–214.
8. J. J. Ferronato et al., "*Analysis of Routing Protocols OLSR, AODV and ZRP in Real Urban Vehicular Scenario with Density Variation*," IEEE Latin America Transactions, vol. 15, no. 9, pp. 1727-1734, 2017.
9. P. Kshirsagar, S. Akojwar, Nidhi D. Bajaj , "*A hybridised neural network and optimisation algorithms for prediction and classification of neurological disorders*" International Journal of Biomedical Engineering and Technology ,vol. 28,Issue 4,2018
10. M. Conti and S. Giordano. "*Mobile Ad Hoc Networking: Milestones, Challenges, and New Research Directions*" IEEE Communications Magazine, Vol. 52, pp. 85-96. 2014.
11. Pravin K, Akojwar S. 2016d. **"***Prediction of neurological disorders using PSO with GRNN***"**. IEEE SCOPES International Conference, Paralakhemundi, Odisha, India.
12. Li, Wenjia, Anupam Joshi, and Tim Finin., "*SMART: An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks*." In MIL· ITARY COMMUNICATIONS CONFERENCE, 20Il-MILCOM 20Il, pp- 1102-1107, IEEE,2011.
13. Pravin Kshirsagar and Sudhir Akojwar**, "** *Hybrid Heuristic Optimization for Benchmark Datasets***"** International Journal of Computer Applications 146(7):11-16, July 2016
14. Ismail Butun , Salvatore D. Morgera , Ravi Sankar , "*A Survey of Intrusion Detection Systems in Wireless Sensor Networks,*" IEEE Communications Surveys & Tutorials ,Volume: 16 , Issue: 1 , 17 May 2013
15. Ahmad, Shahnawaz. "*Alleviating Malicious Insider Attacks in MANET using a Multipath On-demand Security Mechanism*." International Journal of Computer Network and Information Security 10, no. 6 (2018): 40.
16. Vanitha, K., and AMJ Zubair Rahaman. "*Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol*." Cluster Computing (2018): 1-9
17. Keerthika, V., & Malarvizhi, N, "*Mitigate black hole attack using trust with AODV in MANET*," Computing for Sustainable Global Development , pp. 470-474), 2016

ISSN: 2233-7857IJFGCN