International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 925–942

Deplete And Discernment Of Security Hazards In Mobile Ad-Hoc-Networks (Manet) Using Artifical Intelligence

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

Abstract

MANET which have been autonomous and conscience may be adapted to any scenario. The configuration of these network nodes is complex in the ad hoc networks and this fundamentally changes the interdependencies among them. The network devices connected to these mobile nodes need to link, execute, and make routing that provides high levels of performance and resistance to any risks and security issues that could emanate from the network easier for this integrity of deployment. Artificial intelligence technologies may be provided to provide and manage a stable and safe infrastructure for the MANET to run. This paper explores in particular how AI techniques can be used for safer routing and networking between mobile dynamic nodes in MANETs. The paper examines different types of threats facing MANETs and different routing protocols that interact with nodes in MANETs. In MANET, to protect contact the preventive method is important. Multiple challenges such as worm-hole attack (WH), Greyhole (GH) attack and blackhole (BH) attacks can easily affect MANET, in which sender hubs can not pass the response from the target node as a result of their misconduct. This research proposes a new routing protocol as the Protocol of the African Buffalo Monitoring Area to prevent assaults in MANET. This framework constantly tracks the contact channel and detects the threat. The ABMZP solution consecutively avoids dangerous nodes and identifies the alternative connectivity path.

Keywords: Mobile Ad-Hoc Networks (MANET), MANETs Attacks, Security, Artificial Intelligence, ABMZP.

1. Introduction:

Due to the cost efficient benefits of connectivity, Mobile Ad-hoc Network (MANET) has been a constant subject in research from the last decade. Since MANET lacks infrastructure, its unstructured environment gives rise to faster communications efficiency. Regardless of MANET's different implementations, they still have a number of crashes. MANET's decentralized architecture and complex topology lead to random changes in routing information is the main reasons behind the problems associated with it [1]. The main reasons for MANET security concerns are

- Lack of effective and durable opponent protection.
- Reasonable probability of violent attacks in a device.

ISSN: 2233-7857IJFGCN

- No general administration.
- Connectivity conflicting.
- The energy factor inside the node is very limited.

Up to now, it has been investigated that security approaches in MANET are essentially two forms. The first type concerns routing protection and the second type concerns data security [2]. The typical method of using routing protocols is the privacy concerns in which routing protocols are used to identify and respond quickly to threats while table-driven routing schemes are primarily intended to resist intruders [1]. Due to the lack of any facilities, the use of main compromise protocols is not allowed by MANET.

MANET is essentially responsible for establishing a link and finding an appropriate way of transmitting packets of data and then transmitting the packets through the system. Since hosts/nodes perform the routing feature, they use a packet transmission system that can be a single-hop or multi-hop[4]. In an area in which economic growth is complicated or unfavorable, MANETs are used as temporary networks. The MANET routing protocols take charge of defining routes and transporting packets to the destination to the target. Since the topology is complex, several mobile nodes connect to the network and leave it at a particular time case. MANET wireless links will tie attacks from unlawful removal to successful intervention[5]. Wireless connections are available. Assaults on a custom cellular connection will access from any device and reach any node and thus violate the fundamental safety criteria. Therefore, it is impossible to find precise nodes in the network.

Customized services are growing in popularity for implementations on broad scales with the growth of functional equipment as well as communication services. It permits devices to link to the infrastructure with the counting and removal of network nodes[4]. MANET apps range from wireless networks to extremely dynamic phones and devices to battery-intensive small fixed networks [5]. Furthermore, MANET for its services requires the application:

- Military fighting area.
- Division in trade.
- Local level. .
- Web of Personnel Region.
- Platforms of the detector.

The MANETS implementations are growing considerably, the safety problems which are also important for them are increasing. While a range of methods last to safe applications for MANETs, a framework needs to be planned early to forecast and identify attack and intrusion. The concept of an artificial intelligence MANET is aimed at developing smart protocols to identify and resist certain threats and security problems [4]. In the first place, the paper underlines current safety risks and remedies. The paper then focuses on the implementation of appropriate MANETs in Artificial Intelligence [5].

2. Review of Literature

Pratik Gite, et.al (2017)[8] The new mobile ad-hoc network technology in this document, which is currently used for wireless access is proposed in the paper. Mobility, wi-fi, and freedom are

ISSN: 2233-7857IJFGCN

some of the features of this innovation. The mobility of nodes and the power scarcity are factors in the Ad-Hoc Multi - hop Network that cause network failure. In this paper, proposed a new routing protocol that prioritises the existing routes based on their track stability. For the analysis, they employed the relation estimation methodology based on the signal frequency. With regard to the AODV routing protocol, the proposed routing principle was applied. The tests have led to the conclusion that the efficiency of the approach proposed is higher than the current algorithms. Based on these trials. This approach significantly improves the problems of overhead routing, electricity usage and throughput for various numbers of experiments.

Sayan Majumder, et.al, (2018)[9] Proposed the mathematical solution to preventing wormhole attack (AD (Absolute Deviation)) Due to the use of absolute deviation and association covariance, wormhole attack can be detected in very little time. There are no additional conditions to perform the proposed algorithm. A false tunnel is created from source to place by the Wormhole attackers. Even so, the initial route requires a significant amount of time. Therefore, it is necessary to determine here how much time is required to avoid a wormhole intruder accessing the network. By means of simulations, absolute variance technology has been shown to provide improved results compared to AODV. Furthermore the Total Variability Coefficient Of determination is used to calculate the packet drop trend for the wormholes.

Roshani Verma, et.al, (2017) [11] The main purpose of this paper was to identify and eliminate wormhole assault during propagation and replication. This suggested algorithm improves the security of ad hoc networks. Such attacks by this network are avoided. The packet distribution ratio is expanded and the latency regulation is reduced by enhanced system routing. The column entrants at the destination network are improved here to classify the wormhole nodes at high speed. The new strategy also contributes to deploying effective approaches from which DoS attacks and hybrid attacks can be avoided from entering the networks in order to strengthen their stability.

Pravin Kshirsagar et al, [10] , To achieve its objectives, several computer models were developed, including one layer inhibition, first layer expectancies, Rbf, Ffnn, Pnnn, Grnn, etc.This particular human brain was understood to be ideal for a limited range of moderately executed information and architectures. But the number of data to be analysed and the time of developing applications have been limited by emerging technological advances. Many researchers then changed classical machine learning, allowing a vast number of predictions and less time to accumulate. Neural networks may describe or deliver complex and reliable knowledge outcomes.

Kavitha T, et.al (2017)[13] Addressed the key problem of the mobile ad hoc network connection breakdown due to high movement of the nodes. In this article, they therefore suggested a protocol for the automatic movement of the route, by means of which path distance and hop count are assumed indefinitely. They also introduced a partial topology-sensitive mechanism to obtain the shortest path at once. Using this process, packets to the destination can conveniently be re-routed to each cache node maintenance, in the event of a connection breakdown. The

ISSN: 2233-7857IJFGCN

outcome is that, relative to current schemes, the proposed solution has optimum capacity, less end-to-end wait and instantaneous path migration.

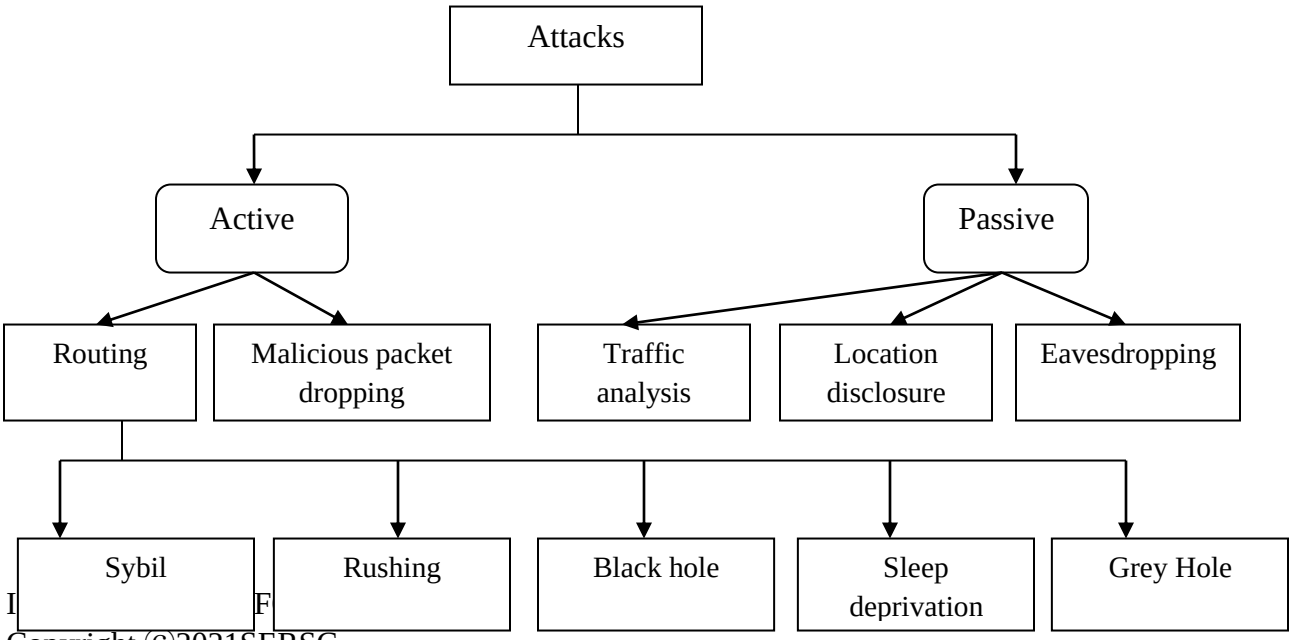
Chitra Gupta, et.al, (2016)[14] Analyzed that, according to the obtained results in traditional works, it is critical that MANET routing protocols have reactive, anonymous and status free properties. Various methods are proposed here for wormhole attack. The possible explanation based on mobility or a neighbor-based solution gives improved results with regard to various elements such as packet distribution ratio, throughput, and overall routing decline. For abrupt network expansion, further network parameters are measured. A number of other forms, through the introduction of the proposed solution, of possible network layer attacks are stopped from entering the network. In addition, the process suggested could be expanded in future to enable mobility of nodes and dynamic algorithm adjustments.

3. Mobile Ad-Hoc Network (MANET)

MANET systems, particularly exchanges of knowledge with mobile devices, are used in industrial and consumer applications. Mobile mesh systems can also be a low-cost fault resistant to the mobile network. Defect army wants are consistent with IP services for handheld wireless networks. Many of the topological sectors are highly complex and autonomous[3].

3.1 Attacks in Mobile Ad-Hoc Network:

MANETs have infrastructure free connectivity between mobile nodes and have improved their use in internet of things (IoT). To make the data accessible, IoT uses the cloud. Implementation of MANET's mobile nodes into IoT could affect the processing and analysis of data, as the job is moved to mobile network devices. Remote node data collection improves data acquisition efficiency, provides improved redundant data maintenance, and gives greater assistance for emergency services. The mobile nodes are exposed to various networks due to complex changes in topology and are subject to attack by viruses, malware and spywares[4]. In addition, an effective route must be planned for the transmission of data packets that both stabilize connectivity and protection. The MANET attacks are categorized as two-active and passive attacks. The mobile node location can be revealed, eavesdropped and dropped by passive attacks. Routing and malicious packet dropping[5] are several examples of successful attacks.



I F

Figure 1: Attacks in MANET

3.2 Characteristics of MANET Networks:

The MANET network is made up of mobile platforms known as "nodes" which can be transferred randomly. Aircraft, cars, lorries and even people can have nodes and each router can have a lot of hosts. MANET is an independent mobile node system. The device can operate either alone or with gates or fixed communication protocols. In the last example, a stub network connecting to a fixed network is typically considered. End channels convey nodes of traffic[12]. However, the transfer of "transit" transport is not permitted.

The MANET modules are fitted with cellular transmission and reception that use symmetric antenna for transmitting guided to pixel links. These antennas could also be used in configurations. The power level and level engagement of its recipients and transponders between both the network service image sources in the shape of a natural multi-hair or an ad-hoc network, at any point depending on the position of the nodes[13]. As a consequence of moving nodes, the topology of such a network can alter or change its receipt and transmitting specifications.

Four distinguished MANET features are presented in Figure 2.

3.2.1Dynamic topology:

Nodes in the network can switch dynamically and network topology can move into unpredictable moments easily and predictably and can have two-way and one-way links as well.

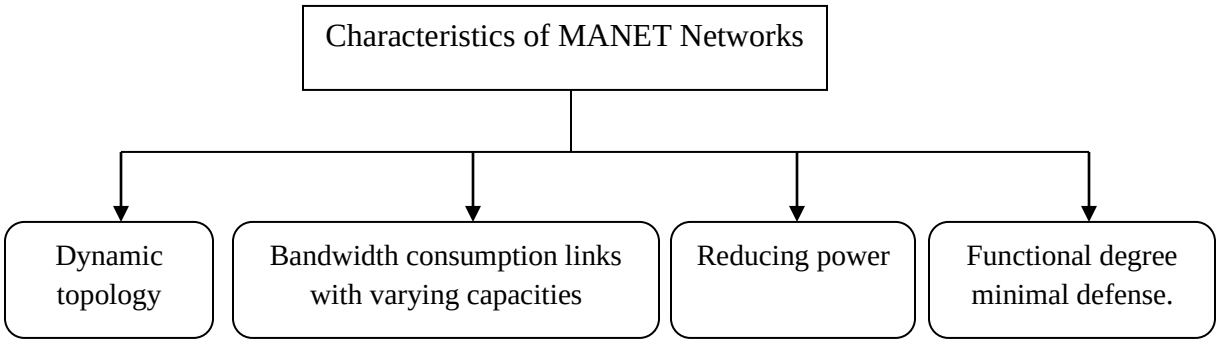


Figure 2: Characteristics of MANET Networks

3.2.2 Bandwidth consumption links with varying capacities:

Significantly damaged network technology in the network bandwidth. Moreover, the wireless communication performance is frequently slightly smaller than the radio site's optimum speed, taking into account the impact of multiple entry, attenuation, noise, interruption, etc..[12]. Complete applications often have close or networking capability - relative low bandwidth causes latency within the network rather than exceptions. As cell telephone networks mostly only

ISSN: 2233-7857IJFGCN

extend current infrastructure, customers typically want the same facilities as a fixed link. The number of applications increases with graphical growth and the expansion of network cooperation.

3.2.3 Reducing power:

A capacitor or other low power source can be used to operate all or part of the MANET cluster heads. For these nodes, problems of energy conservation play a significant role.

3.2.4 Functional degree minimal defense:

In addition, cellular communication systems are less secure than cable systems from physical safety risks. A higher risk of communication acquisition and replacement, and attempts on access denial must be taken into consideration. Communication systems typically employ various channel protection methods[13]. In contrast to centralized schemes, for example, a decentralised network control MANET offers additional fault tolerances.

3.3 Protection assault in Mobile ad-hoc network Layers

MANET deployment faces various forms of networking problems. Different types of networking layer attacks or incursions have been detected in MANET throughout that process. Figure 3 presents various forms of assaults at various levels in MANET.

3.3.1Application Layer Attack:

Procedures on the application layer provide user-level info. It facilitates many protocol modes, including HTTP, TELNET and SMTP. Application layer is susceptible to some negative attacks[13]. It has several bugs and assault entry points.

- **Repudiation Attack:** Applies to DoS of involvement, and security systems are used on various layers and authentication system, to avoid certain forms of attacks. Authentication and protection application layer should be taken into consideration to guarantee packet protection against several attacks [12].
- **Infectious and parasite assaults :**various forms of the Layer framework virus or worms attack. The malicious software attack is sometimes named. The malicious codes are viruses, worms, spyware, and Trojan cheval, and all operating systems and software can be attacked. Using various types of antivirus software to block certain kinds of attacks[12].

3.3.2 Transport Layer Attack:

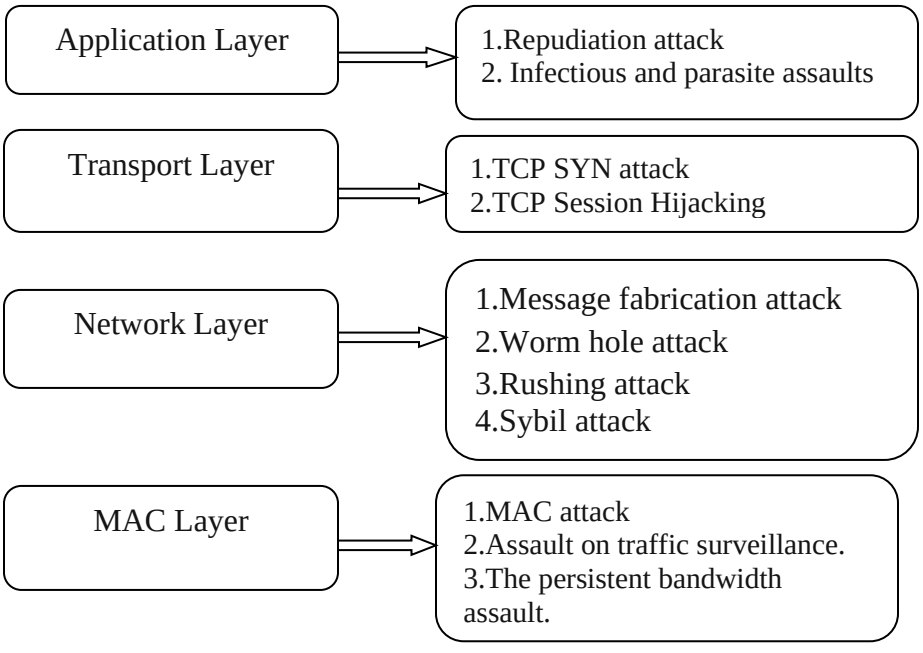
- **TCP SYN Flooding Attack:** SYN is a DoS attack, where attackers send the order to the target machine for SYN progression. In an effort to make machine unacceptable to legal traffic, use a lot of server power. A lot of semi-open TCP connections with the victim node are generated for the attackers [13]. The handshake to the completely opened link is never done.
- **TCP session hijacking:** Attackers benefit from the use of insecure session after their initial development process in TCP session hijacking. The assailants spoofed the node of

ISSN: 2233-7857IJFGCN

the survivor to attempt to gather confidential communications and other hidden node data. The hijacking attacks to rob or foresee a legitimate session token that allows web application authorization. Various forms of threats, such as sniffers, client side attack, and middle guy, are accessible as shown in Figure 3.

3.3.3 Network Layer Attack:

- **Message Fabrication, Modification:** The attackers send a falsified response to the neighbouring nodes in response to the attacker's relevant valid route requests during fabrication attacks without acquiring associated messages.
- **Wormhole Attack:** In the wormhole attack a data packet is sent by an attacker node to a point of the network's tunnels. There are two nodes of intrusion called the wormhole. The tube occurs between them. Wormhole attacks are serious risks to protocols for MANET routing. Assailants make their nodes look more appealing with this kind of attack on the system to transport maximal data packets through their nodes. The assault will avoid all other routes than across the wormhole being discovered.
- **Rushing Attack:** Rush attacks are primarily directed at protocols for routing on request. Such attacks interrupt the exploration of the pathway. On-demand routing protocols using duplication removal are susceptible to threats in the course of the path discovery process[9]. When an intrusive node receives an RREQ packet from the reverse path, it can swell across the entire network rapidly before other nodes can respond, which also obtain a path request packet.
- **Sybil Attack:** Each node in MANET needs a unique address for the routing of the unique address nodes. There is no legal framework for checking such identities, however, in a MANET. This is used by an intruder and exploits nodes, and transfers control packets, such as RREQ or RREP, using sensory expectations. This attack could cause chaos in the routing process by attacking random identities or other nodes [14].



ISSN: 2

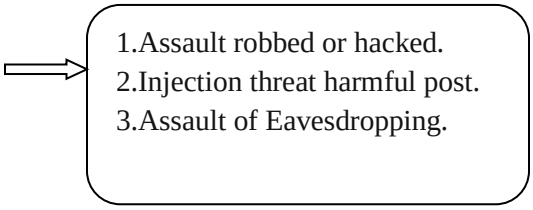


Figure 3: MANET-layered types of attacks

3.3.4 MAC Layer Attack:

- **Assault on traffic surveillance:** The study of traffic is a passive form of attack. The attacker performs such an inspection to determine the type of contact. It tracks the packets of data we use for communication[13].
- **The persistent bandwidth assault:** The assailant's node unlawfully stabs the large part of bandwidth because of this network problems in this assault.
- **MAC Targeted Attack:** In all the pieces of data shared across various nodes, MAC layer plays a crucial role to ensure that the data is effectively gathered to their intended receiver. The targeted attacks of the MAC interrupt the whole MAC method and are thus considered a targeted attack of the MAC.

3.3.5 Physical Layer Attack:

- **Assault robbed or hacked:** Such assaults are caused by infected individuals or stolen devices such as physical node capture.
- **Injection threat harmful post.:** Injecting malicious fake messages into the true messages streams that run across intermediate nodes, and the network functionality is disturbed by the attacker due to malicious message injection.
- **Assault of Eavesdropping:** If unintentional recipients receive emails and speak, then eavesdropping is named. The nodes of MANET attach a wireless media, and the large network traffic uses the RF-spectrum and transmissions by nature that can be intercepted easily by recipients tuned at the suitable time.

3.4 Security Goals of MANET

The objectives of the MANET protective measure are outlined briefly as follows:

3.4.1 Availability:

Maintain the communication services are available in connection with multiple environmental assaults. The biggest challenge is the availability of tools that will quickly heal network service[14]. Some threats have configured counteractive devices such as data encryption, while some attacks require various kinds of behavior to restrict or reverse losses to accessible resources.

3.4.2 Confidentiality:

ISSN: 2233-7857IJFGCN

Confidentiality guarantees that only the dependent party has access to the results. Encrypt consumers from threats.

3.4.3 Integrity:

Integrity means that it is only allowed to alter knowledge or communications to parties authorised to do so. It also preserves the document, since there is no harm to the communication. Every kind of communication, whether it's message flow, message or area defined in the message, is covered by credibility providers.

3.4.4 Authentication:

Authentication ensures the accuracy of the relation. Otherwise malicious nodes will attempt to obtain unlawful connections to assets and confidential information and will also seek to disturb other node activities

3.4.5 Non-Repudiation:

Failure to deny a received message puts an end to the sending or receiver. Therefore, the destination will demonstrate that the information has been sent by the intended sender and vice versa when a response has been sent.

3.4.6 Scalability:

In terms of protection, scalability is very critical. There is a MANET with a big node. In handling vast networks, external protection must be controlled. In the event that the attacker does not use the new added node intentionally in the system to attack the machine as a whole.**3.4.7**

3.4.7 Anonymity:

This means that any data used to classify an approved node user must be kept secret and not allocated to the same node or framework.

3.5 Evolution of AI in Security

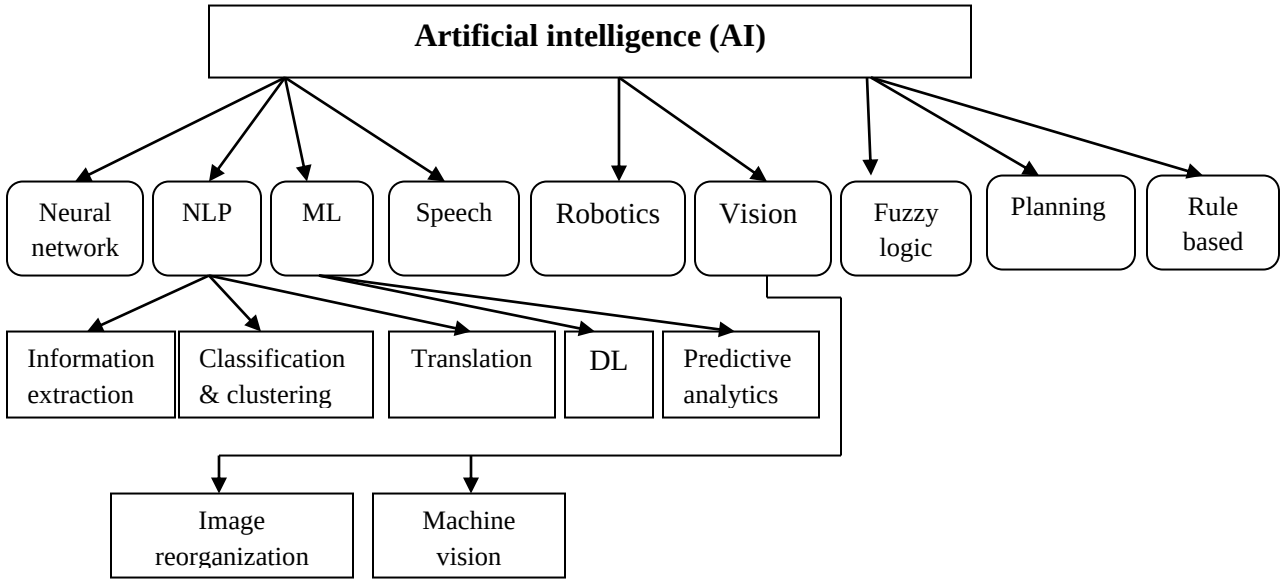


Figure4: Artificial Intelligence and Its Branches

ISSN: 2233-7857IJFGCN

In sports, logic and language processing analysis, artificial intelligence is widely used[18]. The principles of mathematics, biological neurons, analytical science, language and engineering shape artificial intelligence [6]. Figure 4 shows the division of AI and its divisions.
For the following purposes, artificial intelligence methods may be used in MANETs in order to improve the security:

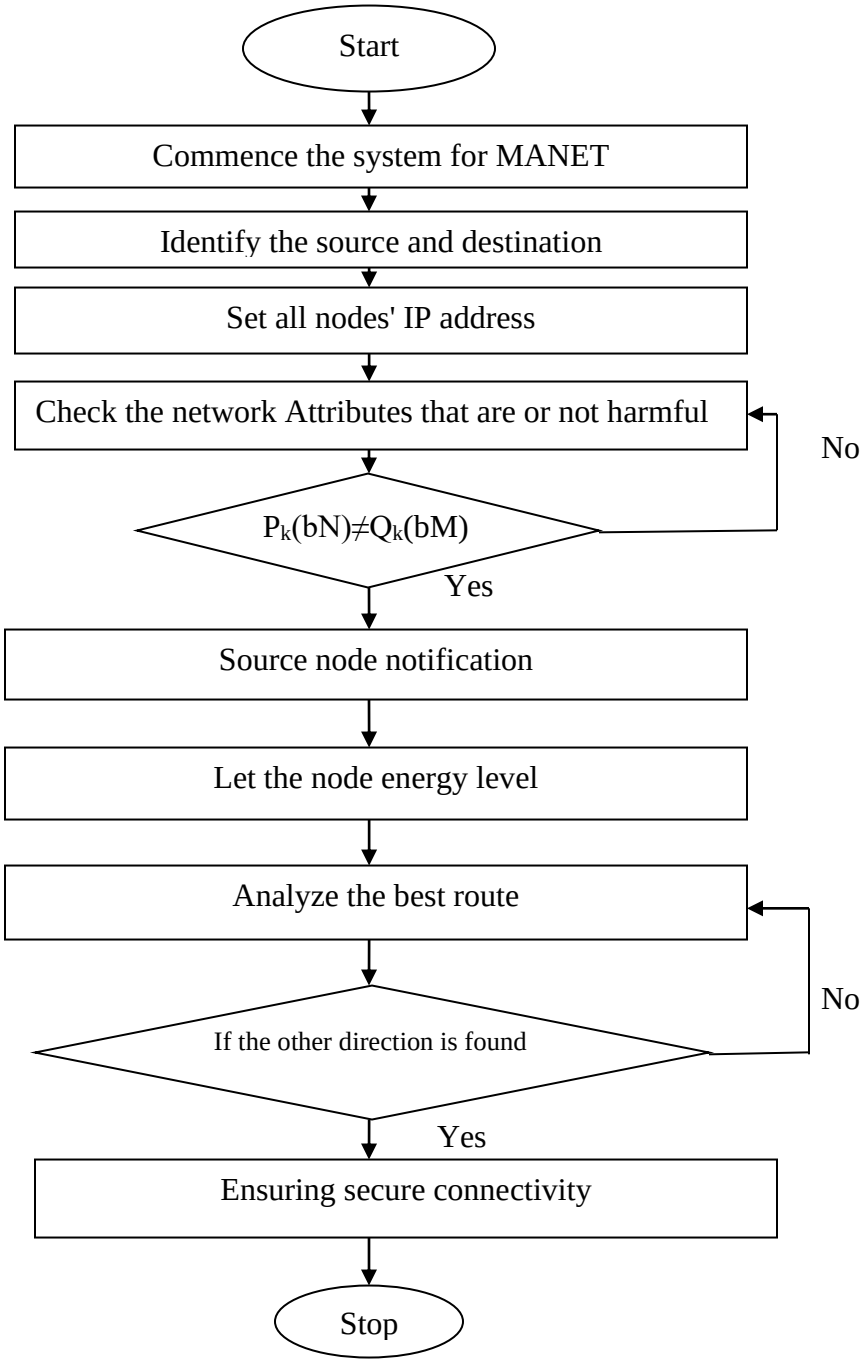
3.5.1 To Manage Huge Volume Of Data:
MANET is extremely complex in information collection and managed data files and packets are a challenge[3] to maintain their stability. The AI system warnings and log files created can be used for selecting the relevant data. The use of AI will make the selection criteria more complex[17].
3.5.2 To effectively expose the threats:
A network like MANET in which nodes are added dynamically and are still threatened. AI could help with even more precise exploration of enemies or attackers[19]. AI approaches use self-learning methods and consumer and network behavior. Decisions are made in the network based on the defined behaviors[4].
3.5.3 To increase the response time:
Highly precise and accurate threat monitoring needs to be carried out and AI promises higher processing speed for greater performance in detecting threats to security[5].
In order to provide nodes protection on the MANET, artificial information and techniques can be used. This is achieved through the incorporation of intelligence into the MANET routing protocols. The paper focuses on MANET safety solutions focused on AI algorithms and methods [14].
4. Methodology
4.1 African Buffalo Monitoring Zone Protocol (ABMZP):
ABO) and ZP is ABMZP. The fitness feature of ABO predicts the malicious activity and determines another safe route for communication in this strategy. The ABMZ protocol initially creates the data transfer routing field. This routing area has multiple signal level (N) everywhere in the contact network. The source hub initially transfers packet data through neighbouring nodes which lead to packet transmission. to the recipient. MANET is vulnerable to hacking activity in order to understand the targets under threat and boost connectivity into an alternate route in the suggested solution. In the proposed ABMZP model, attacks such as the WH, BH and the GH attack are identified. This method starts the multi-node network zone (N)[4].
The RReq message for all adjacent nodes is mostly sent via the sender node and the message is sent by routers to the sender node. The suggested ABMZP tracks the network in order to find the right way of improving connectivity. In addition, for each node in the network the suggested ABMZP classifies the IP address. The best way to properly communicate through equations (1).

$$k'_w = P_k + N\left(ln_1(bN - Q_k) + ln_2(bM.k. - Q_k)\right)\text{----------(1)}$$

ISSN: 2233-7857IJFGCN

As N defines the whole communications protocol, k shows the communication path, Pk displays all sensor node, ln1and ln2 are the teaching specifications and the IP address of all the nodes is indicated.

The ABMZP constantly scans the network to identify the dangerous knots. As harmful nodes are identified, the source node is alerted and safe contact is provided by the finest path explained in Figure5.



ISSN: 2233-7857IJFGCN

Figure5: Flow Chart for ABMZP

4.2 Performance Metrics:

The framework introduced by ABMZP measures parameters like bandwidth, impedance, PDR, packet delivery and delay. The MBDP-AODV[19], OLSR[29] and CLPDM-SI[3] are found in comparison to this approach. The suggested scheme has shown better outcomes for maintenance, message delays, PDRs and over put.

4.2.1 Attack prevention rate:

This is a test of the effectiveness of the mitigation rate for network attacks. The number of replies sent and the sum of data streams achieved to the requirement is a part of that. Equation 2 reveals the computational framework.

$$.A = \frac{(Tn' + Tp')}{(Tn' + Tp' + Fn' + Fp')} \quad \text{----------(2)}$$

4.2.2 PDR calculation:

The ratio is determined with equation 3 between both the entire number of data packets achieved and the sum of packets received.

$$PDR = \frac{Number\ of\ received\ packets}{Number\ of\ sent\ packets} \times 100 \quad \text{----------(3)}$$

4.2.3 End-To-End delay calculation:

The default rate is measured whether the information consume a while to reach its target base station of the transmitter and the fixed time period using equation 4.

$$End\ to\ end\ delay = \frac{Received\ packets\ time}{Sent\ packets\ time} \text{----------(4)}$$

4.2.4 Throughput calculation:

It concerns the rate of service transfer of information through physical or virtual connects.

5. Result and Discussion

The avoidance rate of attacks demonstrates the reliability of the ABMZP procedure. This is compared to any of the MBDP-AODV, OLSR and CLPDM-SI techniques. In this case, the lower threshold of prevention is reached for MBDP-AODV while 90%, OLSR and CLPDM-SI are at 98.3% and 97%. However, ABMZP's proposed rate for prevention of attack is 99.98 per cent high, as seen in table 1 and Figure 6.

S.No	Method	Detection of assault rate (%)
1	Mbdp-Aodv	90
2	Olsr	97.3
3	Clpdm-Si	98
4	ABMZP	99.98

ISSN: 2233-7857IJFGCN

Table1: Analysis of detection assault Rate

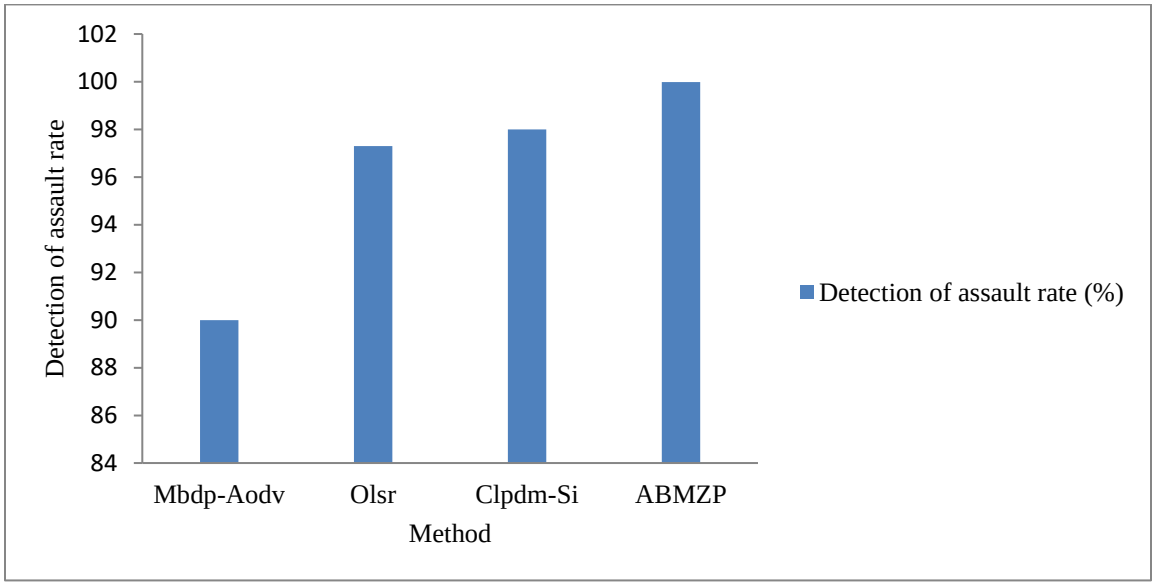


Figure 6: Analysis of detection assault Rate

5.1 PDR Calculation:

Nodes	PDR (%)			
	Mbdp- Aodv	**Olsr**	**Clpdm-Si**	**Abmzp**
15	95	49	86	99.97
25	94	79	98.7	99.87
35	93	83	99.2	99.75
45	91	89	98.1	99.66
55	93	96	99.3	99.33

Table2: Evaluation of PDR

The PDR ratio is calculated and measured using the analytical methods. The PDR ratio will be determined in this case according to the number of transmission nodes. With 55 entities included, MBDP AODV accounted for 93 percent of PDR, OLSR for 96 percent and CLPDM-SI for 99.3 percent. The proposed ABMZP process, provided in table 2 and as illustrated in Figure 7, achieved a 99.33 percent high PDR score.

ISSN: 2233-7857IJFGCN

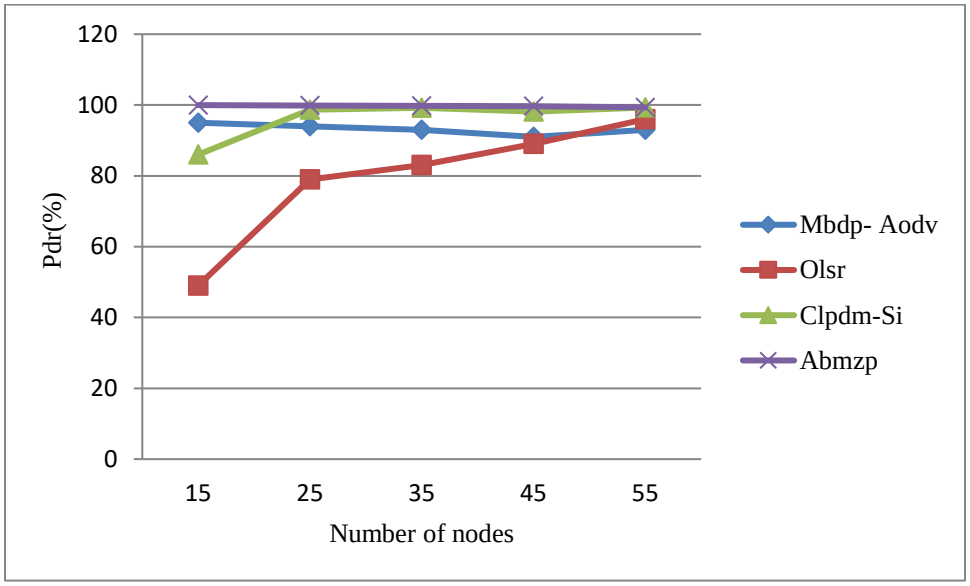


Figure 7: Evaluation of PDR

5.2 End To End Delay Calculations:

Nodes	End - End Delay (s)			
	Mbdp- Aodv	Olsr	Clpdm-Si	ABMZP
15	41	19	9	4
25	82	30	12	7
35	111	39	15	11
45	161	59	29	14
55	181	65	31	21

Table 3: Assessment of delay from end to end

Generally, the number of retransmitted RReq messages and data packets increased with high packet delay. Often, network resources can be reduced quickly and node energy waste. This results are related to the MBDP-AODV, OLSR and CLPDM-SI results. Here, a high time for transmitting packets is charged with the MBDP-AODV process. The innovative ABMZP method

ISSN: 2233-7857IJFGCN

therefore provides low reception time for the packets provided in Table 3 and seen on Figure 8 at the destination.

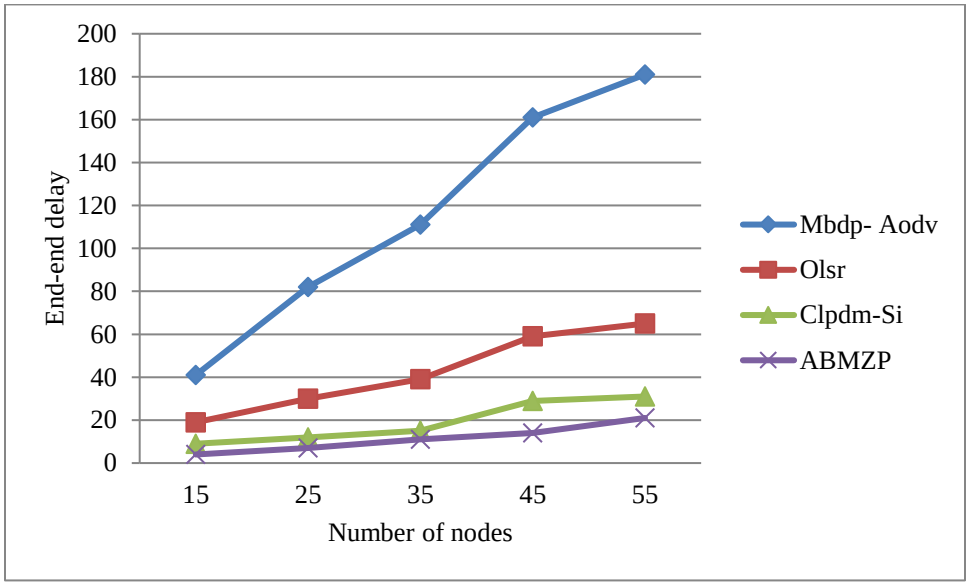


Figure 8: Assessment of delay from end to end

5.3 Throughput calculation:

Nodes	Throughput (Kbps)			
	Mbdp- Aodv	**Olsr**	**Clpdm-Si**	**ABMZP**
15	21	37	146	161
25	19	49	199	251
35	18	54	202	321
45	16.5	89	199	351
55	18.73	96	202	346

Table 4: Evaluation of throughput

The suggested solution achieves high performance values that are confirmed by other methods detailed in Table 4. Recent approaches like MBDP-AODV have been achieved here with 18.73kbps, OLSR reached 96kbps and 202kbps have been used in the CLPDM-SI solution for

ISSN: 2233-7857IJFGCN

the transmission of 55nodes. But in comparison with other techniques represented in figure 9, the proposed ABMZP reached 346 kbps of high performance.

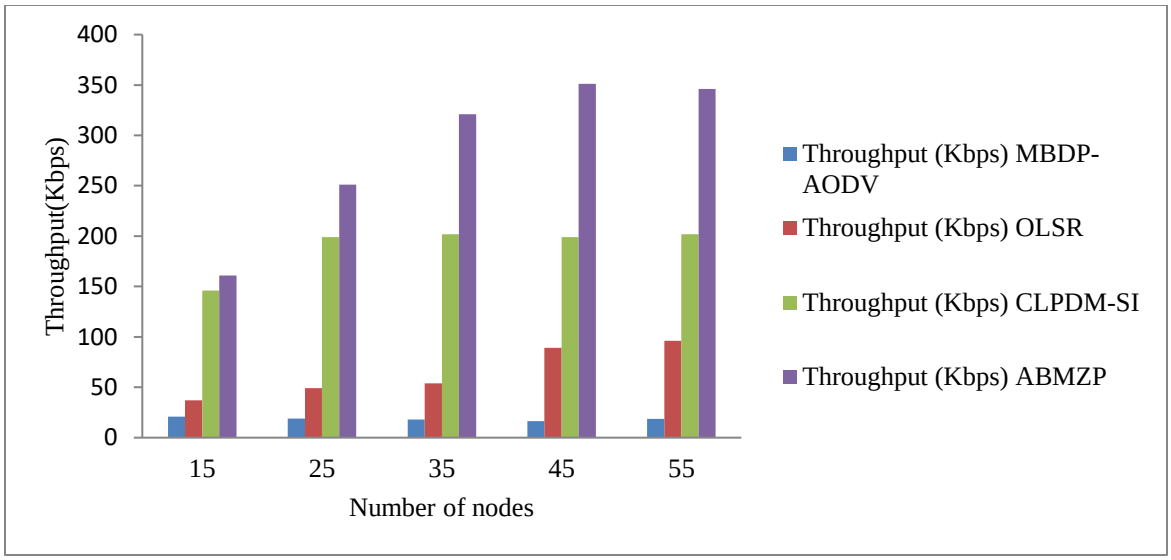


Figure 9: Evaluation of throughput

6. Conclusion

This paper explores implementing numerous techniques of artificial intelligence for security applications in MANETs. While these responses are dependent on conditions and types of attacks, it was clear and concluded that its topology, which changes and adapts itself, is the key consideration for safety threats in MANETs. A node must be safeguarded when interacting in a network, and energy use is the mechanism. This is another MANET defense stumbling block. Future work on the construction of an intelligent system to be designed using AI algorithms will be focused on. Every node in MANET is also focused on cost efficiency and detailed behavior. The avoidance of attacks is important to secure the information during data transmission. The new preventive approach for protecting contact was then presented in this paper, as ABMZP. This means that the ABMZP solution preserves information from wormhole and other harmful networking. Therefore, ABMZP warns the source node when it detects malignant behaviors. In addition, the attack is neglected and the transmission is secured by an optimized way. The rate of avoidance of attacks is therefore 99.98% high, 99.33% PDR, less delay and a high output ratio.

References:

[1] Anzer, Ayesha, and Mourad Elhadef.2018, "A Multilayer Perceptron-Based Distributed Intrusion Detection System for Internet of Vehicles." *In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), pp. 438-445. IEEE.*

[2] Mukherjee, Saswati, Matangini Chattopadhyay, Samiran Chattopadhyay, and Pragma Kar.2018, "EAER-AODV: Enhanced Trust Model Based on Average Encounter Rate for

ISSN: 2233-7857IJFGCN

Secure Routing in MANET." *In Advanced Computing and Systems for Security, pp. 135-151. Springer, Singapore.*

[3] Pravin Kshirsagar And Sudhir Akojwar- July 2016 **"**Hybrid Heuristic Optimization For Benchmark Datasets**"** *International Journal Of Computer Applications* 146(7):11-16,

[4] Shivashankar.T.M, & S.B.Shivakumar. (2019). Insights on Security Improvements and Implications of Artificial Intelligence in MANET. *Communications on Applied Electronics(CAE).*

[5] Silva, V., Mitrovic, S. J., & Handschuh, S. (2018). WordNetGraph: Structuring WordNet Natural Language Definitons. *Science Conference*.

[6] S.Dadras, S.Dadras, & C.Winstead. (2018). Identification of the Attacker in Cyber-Physical Systems with an Application to Vehicular Platooning in Adversarial Environment. *Annual American Control Conference*, (pp. 5560-5567).

[7] P. Kshirsagar, S. Akojwar, **"**Optimization of BPNN parameters using PSO for EEG signals**"** Proceedings of the International Conference on Communication and Signal Processing, 2016 (ICCASP 2016).

[8] Pratik Gite, 2017, "Link Stability Prediction for Mobile Ad-hoc Network Route Stability", *International Conference on Inventive Systems and Control.*

[9] Sayan Majumder, Prof. Dr. Debika Bhattacharyya, 2018,"Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach", *IEEE.*

[10] P. Kshirsagar, S. Akojwar, Nidhi D. Bajaj -2018 "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,

[11] Roshani Verma, PROF. Roopesh Sharma, Upendra Singh,2017 "New Approach through Detection and Prevention of Wormhole Attack in MANET", *International Conference on Electronics, Communication and Aerospace Technology ICECA* .

[12] Pravin R. Kshirsagar, Pranav P. Chippalkatti, Swagat M. Karve ,2018," Performance Optimization of Neural Network using GA Incorporated PSO" *Journal of Advanced Research in Dynamical and Control Systems.*

[13] Kavitha T, Muthaiah R,2017, " Instant Route Migration During Link Failure In Manets", *International Journal of Mechanical Engineering and Technology (IJMET) Volume 8, Issue 8.*

[14] Chitra Gupta, Priya Pathak, "Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET", 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[15] Kaur, A., Wadhwa, D.S.2013: Effects of jelly fish attack on mobile ad-hoc network's routing protocols. *IJERA 2248(9622), 1694–1700* .

ISSN: 2233-7857IJFGCN

[16] Pravin Kshirsagar and SudhirAkojwar, "Prediction of neurological disorders usingoptimized neural network" International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES),2016.

[17] Gondaliya, T.P., Singh, M.2013: Intrusion detection system on MAC layer for attack prevention in MANET. *In: IEEE-31661* .

[18] P Kshirsagar and V Deshmukh, -2013, **"** National Conference On Innovative Paradigms In Engineering & Technology". Proceedings Published By *International Journal Of Computer Applications*®(Ijca),

[19] M. Jeevamaheswari, R. Anandha Jothi, V. Palanisamy. (2018). AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack In MANET, IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011, ISSN: 2395-602X.

ISSN: 2233-7857IJFGCN