Chapter 2

CHAPTER 2

LITERATURE REVIEW

The network performance in MANET may suffer from a sequence of number of attacks like wormhole, black hole and DoS attacks. This is due to the confusing privacy and security features in the current routing protocols. The motivation inspired numerous researchers to create and examine various security tools to identify malicious sequential attackers in networks. This section discuss a number of security measures to prevent sequential attacks that have been presented in the literature.

2.1 SECURE ROUTE DISCOVERY

In a MANET, according to Mirza et al. (2018), numerous communicating hosts come together to construct a flexible network architecture employing a range of wireless communication technologies, like radio waves or microwaves. MANET communications require a variety of communication technologies in order to satisfy the stringent end-to-end requirements of QoS-based communication networks. The emerging technology of MANET is wireless multi-hop architecture without fixed infrastructure and prior construction of network nodes. There are a number of noteworthy features of this new networking paradigm, including: support for fundamental networking functions such as data transfer and routing, Using a cooperative strategy lack of network node administrative boundaries and in the absence of a central entity, network node connections are essentially temporary [50].

A new method was proposed by Ndajah et al. (2019) to spot malicious activity and secure data exchange in the specified network. Wireless peer-to-peer networks are

particularly vulnerable to certain sorts of attacks due to their special properties. The blackhole attack is one of the most important attacks and this strategy offers a safe way to avoid it. To determine each node's trustworthiness, this method uses a digital signature methodology along with each node's activity. The proposed approach identifies a node's distrustful behavior based on the predicted trust value. This method's flaw is that it allows for the specification of both one blackhole attack and any other attacks. The number of tables used to maintain the data can increase the memory overhead [54].

Jain et al. (2019) [35] proposed a new strategy for discovering and preventing the two attacks: the blackhole attack and the greyhole attack. Through end-to-end verification, the malicious nodes can be found by breaking up the overall traffic into discrete blocks. This strategy uses prelude and postlude messages two different types of messages. The recipient node receives a preamble message from the initiator node that includes data on the number of packets. Once this message has been accepted by the receiving node, the recipient node sends an acknowledgment using a postlude message that includes information about how many packets it has really received. Using this information, the malicious nodes are located and removed from the network. The majority of the nodes' energy is wasted because they spend most of their time in listening mode.

In order to detect and prevent blackhole attacks in MANETs, Yasin and Abu Zant (2018) [3] used the timer-based approach and trap method to enhance the AODV protocol. The neighbor response stage and the trap stage make up this method's two stages. A timer with a fixed random value is used in the trap stage. When the current time matches the random value, a fake trap request with a false ID is broadcast. Any node that responds to that false request is recognized as a malicious node and added to the blacklist. The initiator

node and all intermediary nodes communicate with all of their neighbor nodes during the second stage of the neighbour node reply phase by sending a greeting packet message. A node determines if its ID is on the blacklist when it receives any response from another node. If so, the response is dropped, or else it is checked to see if it is in the list of nodes next to it. If not, it ignores that response and begins the conversation instead. The usage of additional control packets increases routing overhead and packet loss at the congested level. Here, the fake ID is being utilized as a hook for improving memory storage.

The effectiveness of AODV was evaluated by Prachi et al. (2015) [61] when it was being subjected to a black hole attack. Due to the reason that black hole attacks are also an increasingly common kind in sequential attacks, the authors focused their attention on the detection and elimination of black hole attacks. In order to ensure the security of the network, this was achieved by utilizing the RC6 cryptographic algorithm. The authors also compared the results using quality of service (QOS) characteristics such as PDR, throughput, energy and latency. The findings indicate that the packet delivery ratio has improved.

In the later parts of Patel et al. (2015) [11], an improvement to the EDRI methodology is described. In addition to the detection process, this approach also includes a strategy for preventing the problem. In order to accomplish this, the method uses an alert packet that is very similar to the one that is used to observe all of the nodes in the system concerning the malicious nodes that have been detected with the assistance of data routing tables.

By counting the RREP packet, Mahmoud et al. (2015) [74] were able to identify a black hole attack. According to their findings, a node is regarded to be a valid destination

if it sends at least one RREP. In the event that it receives more than one RREP, then only one of the messages arrives from the correct destination and the other messages were generated by the malicious node. In addition to this, the author maintains the Route Reply Table (RRT), which logs the sequence number and arrival time of the RREP message. The identification of black holes in MANET is accomplished by the use of a modified AODV.

According to Jhaveri et al. (2017) [64], a trust-based method has been developed. Within the context of this method, previous data communication is evaluated and trust values are determined. This is based on the total number of packets that the node in the network was able to successfully transmit. Before accepting the RREP, the network provides periodic examinations to ensure that these trust values have been properly updated. The RREP will be accepted if the forwarding node can be trusted and it falls on a routing table with a trust value; otherwise, it will be refused.

Nestled message authentication or NMAC, was designed by Arya et al. (2014) [37] as an alternative to hop-by-hop authentication. It protects the routing packets in AODV and prevents the attacks that happen the most frequently, such as black hole attacks, changing routing information and impersonation attempts. AODV is a distributed routing protocol. The author of this passage previously employed summit authentication on nodes by validating all different kinds of routing control packets. The continual verification cannot be used for substantiating the packet like RERR messages because the goal is not precisely stated in these messages. The overhead for utilizing this technology is really low.

The collaboration value of each node is calculated using the Cooperation-Based Defense Mechanism (CBDM) scheme that Bhoiwala et al. (2017) [34] proposed.

The prospect model is utilized in the calculation of the worth of the partnership. The value is used to determine whether or not the node should be considered suspicious or a typical node. In this case, the node in question will be labeled as malevolent if the cooperation value of the node in question is more than the threshold value. In addition, for the purpose of accurate verification, a bait request is delivered to the node that is suspicious. It is possible to identify the whole node of mistrust based on the process. This can be accomplished by examining the response that the node provided in response to the bait request.

The prior efforts were improved by Chang et al. (2015) [33], who devised a cooperative bait detection system. In this scheme, the source node selects the collaborating neighbor as the bait destination address. Every time, this is different in a random way. The source node will then generate a bribe appeal by selecting the nearby as the destination, and it will then send the bait request for a route to the nearby to the malicious node. This will lead the malicious node in the correct direction. The recognition of malicious nodes is exactly the same as it is in CBDM.

A black hole attack was discovered by Amiri et al. (2014) [66] when they allocated two IP addresses to the node, one of which was a legal IP address and the other was an invalid IP address. Without the attacker's context, all nodes will proceed normally when they receive packets from other nodes that contain a reply to an incorrect address sent by the attacker node.

A trust-based approach was offered by Schweitzer et al. (2015) [51] to make advantage of a changed mechanism in which the data broadcast is provided via the nodes involving privileged trust value. The trust value is computed based on the number of

packets that were replaced throughout the time period of the transaction, which were used to connect the nodes.

According to Shen et al. (2015) [30], the maximum out value estimation method can be accomplished. The node that is responsible for receiving the RREP packet will now perform the computation necessary to determine a threshold value for the destination sequence number associated with each transaction. This threshold value is determined with the assistance of the three constraints; namely, the total number of RREQs and RREPs received, as well as the sequence number of the routing table. If the RREP established by the node has a higher sequence quantity than the threshold value that was determined, then that RREP packet is considered redundant, and the sender of that RREP packet is considered to be a malicious node. A malicious node is removed from the route.

A method that is based on graphs is presented in Liu et al. (2015) [79]. In this method, the nodes will adjoin to form a structure similar to a graph, and each node will investigate the transmission of control packets to the other nodes in its immediate vicinity. The nodes assign a score value to each other based on the frequency of the communication, which makes it easier to select the next hop in the chain when it comes time to figure out the path.

2.2 ATTACK DISCOVERY BASED ON ENERGY AND TRUST

According to Wang and Wang (2019) [78], a brand-new energy-efficient routing algorithm and protocol was created in order to lengthen the life of the network. This study provides the first energy-efficient routing technology, known as 3PEC-MBCR, which is based on the partial energy level. In order to lengthen the lifespan of the network, it is also important to take into account the amount of energy that is consumed by each node.

The PEC-AODV protocol's final simulation and performance evaluation are carried out on the NS-2 simulation platform, which has recently been updated to incorporate a module dedicated to the PEC-AODV protocol. The program ensures that the energy consumption of all of the nodes is equalized, which in turn maximizes the lifetime of each node. The overall performance of the PEC-AODV routing protocol in comparison to the current AODV routing protocol is superior in terms of energy efficiency, which helps to extend the life of the entire network in some way.

Selvi et al. (2019) [69] delay restriction increases end-to-end latency while lowering energy consumption by forming effective clusters. Since the other current approaches expand more effort creating clusters and figuring out the shortest way, the rule-based clustering for routing model exceeds them in terms of network lifetime. By building balanced clusters using the criteria in this recommended model, additional overhead on cluster head selection is also effectively addressed. The main benefits of the suggested approach are enhanced performance and scalability in the areas of throughput, energy efficiency and connection quality as well as a longer network life expectancy. Simulations created in MATLAB were utilized to test this strategy in an experimental setting. The same approach decreased latency times, decreased energy consumption and improved packet delivery rates and network performance.

Guleria & Verma (2019) [26] Hierarchical energy-efficient routing methods are discussed in this article. These algorithms are based on both traditional and swarm intelligence routing techniques. It is possible to characterize the routing protocols that fall into each of these two kinds of protocols based on energy efficiency, data aggregation, location awareness, Quality of Service (QoS), scalability, load balancing, and fault

tolerance, as well as query-based and multipath properties. Following an exhaustive review of the relevant literature, researchers from 2012 to 2019 investigated hierarchical approaches to energy-efficient routing algorithms. It can serve as a useful technical guide for academicians while they are developing routing protocols.

Shamsi (2019) [70] offers a discussion on energy-efficient routing methods, including the reasoning behind why the protocol is zone based and the repercussions of a black hole attack on this protocol. In this article, a brand-new energy-efficient protocol that is based on the Mobility Factor was devised to lessen the impact of black hole attacks. In comparison to existing protocols that are efficient in terms of energy use, the approach that has been developed offers a high packet delivery ratio and higher throughput. Additionally, the utilization of the protocol results in improved performance with regard to the energy consumption of the network.

Dhand and Tyagi (2019) [15], in order to improve the safety of wireless networks and the efficiency with which they use energy Elliptic Curve Cryptography and Spherical Grid Multi-Tier Routing are both utilized in Spherical Grid Multi-Tier Routing, which results in the provision of encrypted communication. These metrics are used to evaluate the performance, and they reveal that the existing standards have superior outcomes in terms of packet delivery ratio and low energy consumption, as well as communication overheads such as throughput and end-to-end delay. In other words, the present standards have a better ratio of packets delivered and a lower energy consumption. It has been established that there is an active reduction in the amount of energy that is consumed as a result of more efficient and secure data routing over the network.

Low Energy Adaptive Clustering Hierarchy (LEACH) and Genetic Algorithm (GA) are two examples of potential energy-efficient routing systems that were proposed by Bhola et al. (2020) [18]. Cluster Heads (CH) are responsible for gathering the data and compressing it before transmitting it to a destination node. A hierarchical mechanism known as LEACH is responsible for transforming sensor nodes into cluster heads. Through the use of its genetic algorithm, the fitness function of the genetic algorithm assists in locating the most optimal solution.

The purpose of the study that was conducted by Pereira and Leonardo et al. (2020) [60] was to look at how well the Dynamic Source Routing (DSR) method worked in MANETs. Extensive testing was done with a variety of settings in three different types of propagation models: free space, two-ray ground, and shadowing. The results of the study that are presented here indicate that the performance of networks changes depending on the model of propagation that is used. It shows, for instance, that the algorithm has trouble sustaining paths in conditions with really severe fading. In addition, controlling the radio strength in such a way that packet broadcasts can be tailored to only reach the target nodes looks to be an effective way to strike a compromise between coverage and interference.

The Security-Aware Energy-Efficient Routing Protocol that was developed by Kalidoss et al. (2019) [38] is an innovative routing protocol that was developed on the basis of trust and energy modeling in order to improve the safety of WSNs while also reducing their overall energy consumption. For the purpose of providing trust ratings and authenticating the trust model, a security technique based on keys is utilized. In addition, in order to increase the safety of communication, this research investigates three distinct trust ratings: total, indirect, and direct trust ratings. The study also proposes a way for

executing cluster-based secured routing, which chooses a group leader based on QoS indicators and trust ratings. This approach may be found around the end of the paper. It has been found that in order to properly carry out the secure routing operation, the final path has been chosen based on path-trust, energy, and hop count.

A novel concept for a hybrid trust metric that takes into account both social trust and quality of service has been proposed by Kumar and Shekhar (2020) [45]. In Addition, the On-Demand distance Vectors (AODVs) of the Routing Protocol have been raised, and the trust-based paradigm has been fused with a process of discovery for attack patterns in order minimize the ability of adversaries to engage in a variety of packet forwarding malpractices. This was done in order to protect the integrity of the network. The measurement of energy, mobility, and RSSI distance are the three factors that go into determining the value of trust. This protocol relies on information obtained from neighbours to provide the success and failure rates of packet transmissions.

Jhaveri et al. (2018) [36] presented a proactive secure routing technique as a potential solution. That employs the use of a linear regression in order to forecast the destination node's maximum sequence number, which may be included into the RREP packet by the nearby nodes. Through linear regression, we were able to determine the target sequence number of the RREP packet's threshold value. When the RREP was broadcast with a maximum sequence number that was higher than the threshold value, the malicious nature of the node was discovered and reported. In addition, a bait identification technique was used to confirm that an unauthorized node was removed from the routing path after it had been identified. The Packet Delivery Ratio (PDR), on the other hand, did not function properly.

Gao et al. (2018) [20] designed naive Bayes classifier that was able to protect users' privacy. To avoid the deletion of data while the substitution-then-comparison attack is in progress. An innovative double-blinding method was incorporated with oblivious transfers and additively homomorphic encryptions with the intention of preserving the confidentiality of the information. Because of the system's great processing complexity, it is incapable of detecting substitution-then-comparison attacks.

An improved trust identification approach was developed by Manoranjini et al. (2019) [48] for use in MANETs. The goal of this method is to increase the likelihood of discovering and preventing black-hole nodes. In this approach, the behaviour of each node was monitored using a variety of trust metrics. These trust metrics included the relationship between sensor nodes, social and service attribute trust, and QoS metric trusts. On the basis of the behaviour that was observed from the malicious nodes, the routing path has been completely cleansed of them. The number of false positives, on the other hand, remained relatively high.

A Hybrid Wormhole AIS (HWAIS) was studied by Tahboush and Agoyi (2021) [73] in order to identify wormholes in MANET that are both in-band and out-of-band. After determining the hop count and the Packet Delivery Ratio (PDR), the Round-Trip Time (RTT) was included. This allowed for the calculation of the in-band wormholes. In addition, K-means clustering was carried out in order to obtain the most appropriate centroid for use as the PDR threshold in in-band identification. The communication range between successive nodes was utilized in an extremely optimistic manner in order to find out-of-band wormholes.

The Hybrid Optimization-based Secure Routing Protocol (HOSRP) was presented by Vatchala and Preethi (2022) [76] as a mechanism to secure data transfers while simultaneously calculating the best route to a destination. HOSRP is offered as a technique to accomplish both of these goals. First, the network is segmented into a number of different numbers, and then the cluster head is selected using a modified version of the particle swarm optimization technique. HOSRP employs a firefly optimization strategy to locate short paths between clusters so that it can cut down on delay and boost the percentage of packets that are successfully delivered. HOSRP ensures the safety of data transfer by utilizing a message digest in conjunction with a cryptographic method. The effectiveness of HOSRP is analyzed by employing the Greencloud Simulator in conjunction with performance metrics that are used in the industry. According to the findings, HOSRP is superior to other approaches in terms of speeding up the process of saving energy and protecting data.

2.3 DISTINCT ATTACK IDENTIFICATION

The relative report of several hybrid routing protocols in WSN that Govindasamy et al. (2018) [23] designed against wormhole attacks was written by these researchers. In contrast to the wormhole attack, the suggested search for information indicates in favour of participating freely in the reactions routing protocol, descriptive of stimuli routing protocol, crossbreed reroute rules governing the format and conveyance of data. In that equivalence, the operation of the existing agreement is calculated and modelled with the help of a tool designed to reproduce the behaviour of network nodes. This is accomplished by concentrating on the relative input time and relative output time, relative input delay, relative output delay, and energy expenditure by comparing different types of

wormhole attacks. The dynamic wireless sensor networks' resistance to wormhole attacks is significantly improved as a result of the simulated routing algorithms. This research provides support for a variety of routing protocols as well as a comparison of these methods against malicious behaviours in routing.

Cai et al. (2018) [9] discussed about the self-cooperative trust approach in interaction with MANETs routing. The proposed routing algorithms made it possible to provide reliable routing while maintaining high mobility. The security, self-cooperative trust, and internal representation of the routing are all improved as a result of this trustworthy routing. In order to prevent attackers in routing, the ESCT scheme performs an evaluation of a generic trust evaluation mechanism. The security mechanism of the ESCT system determined who the known internal attackers were. The final trust level of any affected malicious nodes in the networking environment is rehabilitated through the periodic exchange of trust information. In order to minimize disruptions to the route continuity, the trust information provides additional context for neighbours' self-detection. The practice needed to overcome the security issue is provided by the study that has been proposed. The trust evaluation vs self-detection mechanism is responsible for carrying out trust analysis in accordance with cooperative detection. With the completion of the evolutionary self-detection, hostile nodes within the network are neutralized, resulting in fewer routing attacks.

Islabudeen et al. (2020) [32] investigates about attacks on network security and advocated using intelligent intrusion detection to stop system configuration in mobile ad hoc networks. The SHA-256 violation was discovered in an ad hoc networked system that was researching challenges such as immediate attacker identification, efficient packet

feature selection, dynamic intrusion detection, and low false positives. Quick and brisk impendent for violation catching and the act of preventing organization by applying the opposing team's purpose, categorisation, harmful activities mitigation, intrusion detection efficiency calculation, false-positive reduction These issues are strengthened by the Quick and brisk impendent for violation catching and the act of preventing organization. This research improves the mobility in a dynamic way by utilizing the intuitive IDPs, which include a packet analyzer, pre-processing data unit, feature extraction unit, and classification unit. Moreover, this research classifies the users more accurately. Because of this dynamic mobility, the Quality of Service (QoS) may be maintained to support quick response, particularly amongst mobile nodes.

Khanna et al. (2019) [42] conducted research on the trust-based mechanisms present in MANET. This research focuses on the protection of wormholes, black holes, and gray holes from malicious attempts to breach their security. Enhancing the trust-based detective is the goal of the trust-based multi-hop communication solution ad-hoc route security. Despite this, the trust-based method is continually evaluated with a number of different components in order to determine whether or not it is vulnerable to assaults that include dropping packets. In this research, the aforementioned components have undergone in-depth research, and the functionality of these components has been thoroughly investigated. Because of this research, we are inspired to implement a flexible use inside an open interconnected system in order to close off potentially dangerous connection points. The efficient monitoring operation encourages the development of signal detection compositions that are accountable for the scoring of goals.

Balaji et al. (2019) [7] designed the identification of rogue nodes is the key to achieving an improvement in secure routing. It is important to keep private information like the packet drop and DOS attack a secret in order to lower the number of suspicious nodes. When the collaboration and DOS attack prevention workflow is carried out in accordance with the repeated game model (SAR-RG), it improves the entire packet delivery across the wireless network. The success rate of the defense is determined by this research based on how accurately it can detect threats. With the assistance of the SAR-RG scheme, the security-based routing can be made more balanced. This research provides an opportunity to develop a method of data transmission in MANET that is both secure and reliable, with the potential to even understand suspicious nodes. This research contributes to the generation of the routing scheme that is based on the procedure of the protocol model for the repeated game model (SAR-RG). The purpose of the proposed research is to stimulate an effort to strike a balance between the ratio of packet drops and malicious attacks in MANETs.

El-Semary et al. (2019) [1] proposed the methodology to protect the AODV routing protocol from the Black hole attack. The proposed systematic inquiry aimed to establish and create a facts version of the SAODV protocol, which would cooperate with the malicious node to produce fruitful knowledge into how to tackle black hole attacks. The SAODV protocol, which is used to obtain the vulnerable to cooperative black hole attack, is responsible for correcting the vulnerability remedies. The black hole protected AODV (BP-AODV) protocol efficiently blocks coordinated black hole attacks at the early simulation stage. This allows it to prevent cooperative black hole attacks in MANETs, which are used to control the MANETs. The outcome of the simulation offers a superior

outcome in the fight against the malicious node activities. The hostile node actions as well as the black hole-protected AODV (BP-AODV) protocol are brought under control by the chaotic map design. This disordered map ensures that the MANETs will chose diverse paths to take. The BP-AODV that has been presented offers the possibility of protecting the MANETs environment against attacks and other forms of malicious node activity.

Fu et al. (2019) [18] utilizing the IOLTS automated method to review the current iteration of the AODV protocol to identify its security issues is one way to enhance the protection of Mobile Ad-Hoc Network. Once these issues have been identified, a suggestion can be made to improve the AODV algorithm in order to reduce the likelihood that it will be exploited by black hole attacks. This will help to ensure that Mobile Ad-Hoc Network is as secure as possible. The suggested way for making improvements was implemented in the NS3 simulator, and the functionality of this strategy was validated using a number of different tests. The results of the experiment revealed that the strategy that was provided can be employed to some degree to defend the MOBILE AD-HOC NETWORK from Black Hole Attacks.

Md Ibrahim Talukdar et al. (2021) [49] developed the performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature. This would-be NS2 programming has been utilized as a recreation apparatus to re-enact existing organization geographies; but it does not have any component to reenact scathing conventions independently; as a result, we have designed and carried out a D_BH_AODV steering convention. According to the findings, the PDR value can be reduced by approximately 40–50 percentage points using the suggested D_BH_AODV strategy for modifying hubs and packages. It is interesting to observe that the delay decreases from

300 milliseconds down to 100 milliseconds and from 150 milliseconds down to 50 milliseconds when the number of hubs and packages increases, respectively. In addition, the overhead varies from one to three depending on the hubs and the parcel values in question. The outcomes of this investigation indicate that the dark opening attack lowers the general's status.

The work of Asif Uddin Khan et al. (2021) [2]conducted When it comes to the identification and prevention of black hole attacks in AODV of mobile ad-hoc networks, an approach that is based on confidence has recently been devised. A calculation that is based on paired parcel grouping is used at the source hub, and this calculation is used to recognize and prevent black hole assaults. They compared the exhibition of the suggested arrangement with the existing arrangement, and they demonstrated that our solution is superior to the one that is now in place. Because of this result, a new detection solution was developed in order to find an issue with the technique that is currently in use, which makes use of the validity bit.

Detection and Avoidance Mechanism of Black Hole Attack on AODV Routing Protocol in Mobile Ad-hoc Network proposed by Nguyen Duy Tan et al. (2020) [55]. The authors estimated the effects of several dark opening attacks using Network Simulator 2 (NS2) with regard to throughput, energy efficiency, and the delivery of information packages. They suggested a fundamental solution to the problem of recognizing and avoiding dark opening assaults. Their replication results show that the more attackable hubs there are in a network at the same time, the lower the energy effectiveness of the network's performance. Furthermore, if an AODV steering convention that includes a discovery and evasion system (dam) of dark opening assault hubs is sent into the network, the

performance of the organization can be improved by about 35% in comparison to an AODV that does not include aversion.

Khushbu et al. (2021) [67] designed Black Hole Attack. In this study, presented yet another Black Hole Attack neutralization approach that is based on breaking points as a means of providing protection against such an attack. As the study of energy research on MOBILE AD-HOC NETWORKs continues to advance, obtaining MOBILE AD-HOC NETWORKs is becoming a serious worry. In a MOBILE AD-HOC NETWORK, each center point acts presumably as a switch, transmitting data bundles to other center points and exchanging controlling information with other center points. One of the most significant threats to the security of MOBILE AD-HOC NETWORKS is referred to as a Black Hole Attack.

An improved trust identification method (ITIM) was proposed by Manoranjini et al. (2019) [48] to maximize the possibility of identifying black-hole nodes in MANETs and mitigating their effects. The activities of each node were monitored using a variety of trust metrics, such as the relationship between the sensor nodes, social and service attribute trust, and quality-of-service (QoS) metric trusts, according to this strategy. Due to the suspicious nature of the activities that were witnessed, the nodes in question were identified and removed from the routing path. However, the percentage of false alarms remained rather high.

The gray wolf trust accumulation (GWTA) method has been created by Vatambeti et al. (2020) [84] in order to preserve and improve anonymity in routing. First, the black and gray-hole attacks were identified based on the characteristics of the gray wolf optimization, also known as GWO. The trust schematic approach, which

forecasts every node and promotes route stability, was then used to maintain the route stability for information sharing. This was accomplished by preserving the route stability. Despite this, the rate of detection was not particularly high because GWO had a low searching ability and a slow convergence speed.

Wadhwani et al. (2020) [85] developed a trust-based architecture in order to build a network that is resistant to malicious nodes. The RREQ and RREP counters were used to determine trust, which allowed for the identification of malicious nodes. However, it requires more measures in order to improve its detection rate. An innovative method that is both secure and dependable. Using a correlation coefficient, Thebiga et al. (2020) [86] designed a method to protect MANETs from being vulnerable to black hole assaults. However, the detection rate it offered was ineffective in any case.

Talukdar et al. (2021) [49] studied the method for detecting black-hole attacks was implemented on the basis of the AODV protocol. It recognized black-hole assaults in the MANET on the basis of the anomaly recognition methodology and digital sign-based cryptography. However, because only a select number of nodes and packets were used for analysis, the scalability of the system was insufficient for usage in real-time applications.

Accurate and Cognitive Intrusion Detection System (ACIDS) was established by Sivanesh et al. (2021) [87] to identify black-hole assaults. It was determined that the attributes such as the destination sequence number (DSN) and the RREP could be used to identify the invaders by determining whether or not there was a deviation in these attributes from the typical activity. However, throughput was less and packet loss was still high.

Indirect trust-AODV (ITAODV), which was created by Jari et al. (2021) [88], is a new trust-based routing protocol that analyzes the node's reliability during data

transmission for the purpose of detecting and separating rogue nodes from the routing channel. However, its effectiveness was negatively impacted when the node mobility speed was increased.

Malik et al. (2022) [89] was designed detection and prevention of a black hole attack (DPBHA) to protect and enhance the total confidentiality of the system by recognizing the blackhole attacks at an early phase of the path-finding task. It was depending on the determination of an adaptive threshold and the creation of the fake RREQ packet. But it needs to identify and mitigate gray-hole attacks to further increase the network performance.

Ebazadeh et al. (2021) [90] was intended a Reliable and Secure Algorithm (RSA) for gray-hole attack detection and prevention according to the probabilistic threshold. In the beginning, the authenticity of each node along a route was evaluated in order to choose a path that was legitimate. After that, the malicious nodes in the path were detected and removed from the network. But, the mean End to End Delay was still high.

Jamaesha et al. (2018) [91] suggested based on a trustworthy ECC. In addition to this, the trust value is used to determine whether or not the system has been compromised by malicious nodes. The ns2 simulation platform is used to introduce this new stable method. The packets are encoded using elliptic curve cryptography for data protection. This application's overall output is more effective.

2.4 PROTECTING MANET

Doss et al. (2018) [16] developed precise mitigation and identification of Jelly Fish AIS (JFAIS) based on the ensemble legitimate routing-based strategy to identify attacks.

The Support Vector Machine (SVM) was applied to learn the efficiency of packet transfer and identify the suspected nodes. Also, the legitimate nodes were selected to transfer data according to the hierarchical trust estimate property of nodes. But, it was not effective to identify more types of attacks in the network.

Rajendran et al. (2019) [65] explained a Cross Centric AIS (CCAIS) to enable secure routing over black hole attacks in the MANET. It depends on the route source choice, priority bit allocation and AIS attack minimization. The secure routing by PIHNSPRA routing scheme was used by the route source choice and the route from end-to-end nodes was chosen securely to mitigate the black hole attack. Also, the priority bit allocation was applied to handle the node location and network forecasting by the previous interaction history. Moreover, a secure AIS transfer efficiency was obtained to establish an effective routing path. But, the throughput was not high, which indicates that this system was not suitable to detect various attacks.

Tahboush and Agoyi (2021) [73] designed a Hybrid Wormhole AIS (HWAIS) to identify in-band and out-of-band wormholes in MANET. The in-band wormholes were identified by executing Round Trip Time (RTT) depending on its hop count and Packet Delivery Ratio (PDR). Also, K-means clustering was used to obtain the optimum centroid, which was considered as the PDR threshold in in-band identification. The out-band wormholes were identified by the communication range between successive nodes in a highly optimistic way. But, its flexibility and identification efficiency were not effective in a large topological region.

PremKumar and Manikandan (2021) [62] contributed a Distributed Hybrid Sybil AIS (DHSAIS) to detect static and dynamic Sybil attacks in ad-hoc networks. First, a specified group of nodes was chosen as monitoring nodes depending on the neighbor

density of the nodes. If the node was static, the Sybil attack was identified by using the Received Signal Strength Indicator (RSSI) and Angle of Arrival (AoA) rate of any identical position claims. If the node was traveling and if the mobility distance at successive timeslots were varied, it was termed as Sybil attack. But, it has a high computational overhead while concurrently identifying various types of attacks.

Dhanaraj et al. (2021) [14] studied a hybrid identification model for attacks by using a Proportional Coinciding Score (PCS) and an MK-means algorithm to detect the black hole and sinkhole attacks. Initially, the number of collected training data attributes was minimized by the data pre-processing in the PCS. Then, the chosen attributes were fed to the MK-means algorithm to learn the data and identify specific attack decision measures. But the records considered for the simulation were limited and so it was not apt for multiple attacks identification.

Sumathi Ganesan et al. (2019) [71] proposed a novel method for detecting and combating Jellyfish attack in MANET called the Accurate Prevention and Detection of Jellyfish Attack Detection (APD-JFAD). And AODV MANETs is surrounded by tons of different attacks, each with different behavior and aftermaths. The Jellyfish attack is regarded as one of the most difficult attacks to detect and degrades the overall network.

Shruti Thapar et al. (2020) [75] provided brief information about jellyfish attack's detection and prevention techniques. This explains the JF delay effects, reordering effects and dropping effects altogether. Each detection and prevention technique are different from one another. Future scope of JF attacks requires efficient and effective detection and prevention policies with minimum delay and reordering effects which will increase the

total achievement of the ad hoc network with changing nodes, forwarding packets and flexible pattern.

Pandey et al. (2019) [57] suggested IDS based on a multi-track routing mechanism to minimize the rate of congestion and to enhance the level of energy efficiency. The foundation of the presented system is designed based on game theory and K-means technique, which computes level reliability. The experimental analysis demonstrates that the presented approach is better in terms of PDR, energy consumption, overhead compared to the existing method, which is based on a machine learning approach. However, the efficiency and scope of the presented IDS system are limited to the homogenous network.

Ghugar et al. (2019) [22] a trust-oriented IDS is offered to secure sensor networks by detecting and eliminating attacks at the various layer of the network. The computation of each node trust values is achieved using key trust metrics on three different layers- (i.e., physical layer, MAC layer, and network layer). The obtained trust values from three different layers are then combined, and based on the pre-defined cut-off value, the node is then identified as a true node or compromised node. The authors have also implemented three different kinds of attacks on three different layers to measure the performance of the proposed system. The study outcome validates the effectiveness of the presented approach in terms of detection accuracy, false-negative rate, and false-positive rate.

Elwahsh et al. (2018) [17] introduced a hybrid approach for categorizing MANET attacks. This hybrid scheme uses characteristics of the unsupervised learning, autonomous feature map, and genetic algorithm- GA to describe the neutrosophic conditional variable of MANETs. These variables are further subjected to GA with the training data to estimate optimal rule set from sub attacks on the basis of the fitness function. The simulation

outcome exhibits that the presented approach improves the accuracy in intrusion recognition and significantly minimizes the rate of false alarm.

Zhang et al. (2018) [83] have addressed the issues related to traditional data mining and rule file-based IDS, which is not effective for identifying new kinds of security threats and attacks and also suffers from low detection rate. Here, the presented study has introduced IDS using the concept of improved principal component analysis-(PCA) for dimensionality reduction and Gaussian Naïve Classifier-(GNC) classifier for classification of observed behaviour. The experimental outcome validates the effectiveness of presented IDS in terms of detection time and detection accuracy.

Neha et al. (2019) [80] have carried a review work on MANET attacks and its mitigation schemes. Here a brief discussion is presented on various and different forms of attacks. Also, in this study, authors have discussed various security protocols against a particular form of attack and tried to establish a strong correlation among the different security solutions to provide a suitable guideline for enabling secure routing in the data transmission and node communication operation.

Chintalapalli et al. (2018) [10] contributed the research study focuses on the optimal path selection problem of secure routing, where the malicious nodes are likely to exist when transmitting data between the paths of legitimate real nodes. In order to reduce the problem of the secure path selection, the authors have used a mixed approach of the Lion and Whale Optimization technique as a hybrid optimization scheme for secure routing. The efficiency of the presented mixed approach is assessed using throughput, PDR, and energy consumption. The experimental performance reveals that the presented approach is robust to offer path selection strategy with a better approach of energy consumption, throughput, and PDR.