https://doi.org/10.48047/AFJBS.6.15.2024.6434-6649

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Enhanced Security Measures for AODV Routing in MANETs Using DRL Against Wormhole Attacks

Jim Mathew Philip[1], Kavitha N S[2]

[1]Associate Professor, Department of Computer Science and Engineering,Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India
[2]Associate Professor, Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India

Volume 6, Issue 15, Sep 2024

Received: 15 July 2024

Accepted: 25 Aug 2024

Published: 05 Sep 2024

doi: 10.48047/AFJBS.6.15.2024.6434-6649

Abstract— An Adhoc network is a mix of mobile nodes that functions without centralized infrastructure. Every mobile node works as host and routers. In addition, it also transmit packets to additional mobile nodes in the network that are not within the direct broadcasting range. Mobile ad-hoc networks are readily subject to different network layer assaults such as black hole, wormhole, as well as DOS attack. Wormhole attack is one of the serious assaults in MANET. Wormhole attacker gets the packets at any given site in the network and interrupts the flow of packet through tunneling them to a different location. In this research, enhanced method is described against these wormhole assaults in a MANET. Particularly, due to their incapacity to maintain node dependability, MANETs are susceptible to routing assaults like wormhole attacks. Since wormhole attacks generally do not immediately destroy networks, discovering them may be tricky. In response, we offer a unique multiple verification-based wormhole identification approach that harnesses the peculiarities of such assaults. The suggested technique assesses the credit of all nodes based on a trust mechanism. The trust levels for suspicious nodes are decreased throughout routing; those having trust levels below a specific threshold are deemed malevolent. This trust system was created utilizing AODV inspired Deep reinforcement learning, which enhances the accuracy of the algorithm over time. Simulation studies in which the suggested technique was applied to current routing algorithms in a highly populated environment were undertaken; the rate of traffic going via pathways containing malevolent nodes was dramatically decreased. Existing solutions employ Quality of Service (QoS) for whole network to identify attacks. Our technique takes utilize of the packet delivery rate and round trip duration for each node, and it also identifies active and passive assaults. Thus, the entire detection of a wormhole attack is attainable using the provided approach.

Keywords— *ad hoc on-demand distance vector, high speed link, packet forward ratio, round trip time, wormhole attack*

INTRODUCTION

One well-liked network architecture that doesn't need any fixed infrastructure is the mobile ad hoc network, or MANET. This allows for the dynamic exchange of data between mobile nodes. Unfortunately, unlike their infrastructure-based counterparts, MANETs are vulnerable to a wide range of security vulnerabilities since there is no central regulating authority [1]. The ability of MANETs to self-configure is well-known; these networks

are constructed by amassing an enormous amount of mobile devices. These mobile nodes are able to talk with one another and set up transmission lines using wireless technology; no infrastructure is required for this [2]. The MANET's nodes communicate with one another using a MANET that is structurally unpredictable. Due to the mobility of nodes in a MANET network, the node-to-node connection cannot be guaranteed when a node's vicinity with other nodes can be maintained periodically by reliant nodes. It is possible for a node to behave selfishly or maliciously, the untrusted selfish or malicious node in the network, if it ever uses its own resources [3]. The most important and challenging part of any future wireless communication system or network will be Some of the many uses for MANETs include healthcare, the cloud, internet networks, reconfigurable networks, and routing across domains. Nevertheless, despite several security measures and choices, MANET's specific security vulnerabilities remain unresolved. In order for MANET algorithms to adapt to new technologies, its routing systems can handle any danger and allow security technologies to change based on the environment where mobile nodes are operating [4]. Stations in robotics MANETs are mobile and not subject to any kind of central control or authority. In Robotics MANETs, mobile stations double as routers and hosts. Multiple security threats may target Robotics MANETs because of their distinct nature. One kind of routing protocol used in Robotics MANETs is the reactive AODV [5]. Many different types of security breaches may occur in wireless networks due to their inherent characteristics and the media they utilize. A node can't send data without depending on other nodes, which other nodes it doesn't know much about. A wireless network is not a good fit for AODV since the nodes are mobile and powered by batteries. To improve the dependability of routes when routing and to identify malicious behavior on nodes, trust based routing is a solution that could perform well in mobile ad hoc networks. [6]. In MANETs, nodes are free to roam and operate as both hosts and routers due to the absence of a permanent infrastructure. These nodes use routing protocols including DSDV, AODV, and DSR to create connections and set up virtual linkages. Still, safety is paramount; one major risk is the Blackhole attack, in which an evil node discards data packets rather than transmitting them [7]. The term MANET refers to a kind of wireless network in which nodes are free to roam and perform dual roles as hosts and routers. To communicate with one another, nodes set up virtual links while employing routing protocols such as DSDV, AODV, and DSR. In the Blackhole attack, an adversarial node deliberately discards packets rather than forwarding them, posing a serious security risk [8].

Ad hoc networks, or mobile ad hoc networks, are networks of wireless devices that are able to communicate with one another without any preexisting infrastructure. Routing protocols are susceptible to a variety of security attacks, as Jellyfish attacks, because of the unsecured wireless communication channel, the multi-hop routing communication method, and the dynamic behavior of the nodes in MANETs. One way in which a Jellyfish node might hinder the performance of a TCP-based MANET is by taking advantage of its inner workings [9]. MANET is an entirely new kind of wireless communication network that can function independently. It doesn't need any infrastructure support to be established when needed. There are a lot of nodes in MANETs that can communicate well with each other. Due to their inherent self-organization, multi-hop wireless networks present unique challenges when it comes to real-time systems and the safe transport of data [10]. The wireless nodes that make up a mobile ad hoc network are movable. It is not possible to centrally supervise the communication among such mobile nodes. Mobile nodes are free to move around in a MANET, which is a self-organizing and self-configuring network. By accepting and transmitting packets, the mobile nodes may function as a router [11]. The lack of an infrastructure makes MANET gadgets vulnerable to power outages and raises serious issues about their energy consumption and security. It has been widely believed by researchers that Cluster Head nodes are harmless and that their frequent cluster re-elections reduce the lifespan of the network. The S2-AODV technique, which stands for Smart & Secure Ad Hoc On-Demand Distance Vector, is suggested to work with main CH, secondary CH (S-CH), and a super cluster head node, among others [12]. Due to the fact that MANETs do not need any explicit configuration, such as a base station or access point, and instead rely on wireless connections between individual nodes, these networks are able to self-organize. If a mobile node is within transmission range, it may connect with other mobile nodes directly; relay nodes are nodes that transfer packets to recipients [13]. The highly adaptable and appealing properties of MANETs are a result of its open architecture. Security concerns must be addressed in light of the openness. The black-hole attack is the most common kind of assault in mobile ad hoc networks. It promotes a fictitious route to the destination node as the fastest and most recent one. Data packets will be dropped and not sent to their destination while they are being collected [14]. Recent developments in wireless communication technology have led to MANETs becoming the preferred networks for a range of applications. From the wireless channel's perspective, in particular, MANETs may be susceptible to collaborating wormhole attacks, such as packet dropping as well as message manipulation assaults [15], which is a major drawback of this benefit. Communications on MANETs are secure by default using symmetric key encryption methods. In many ways, the current schemes' performance isn't giving full security.

Network topology, routing method, existence of hostile nodes, etc., are some of the elements that might affect their degree of security [16]. In a MANET, no established framework is in place; instead, the network is self-configuring and supported by distant mobile devices. Data packets in MANETs go from source to destination using a store-and-forward technique; the network is peer-to-peer and has several distant hops. Methods that draw inspiration from biology are known as "bio-inspired" [17].

Below is a summary of the key points made in this paper:

- To identify wormhole assaults in MANETs, this study suggests a new trust system that uses reinforcement learning with an incentive mechanism. We use the wormhole attack's traits and the Deep Reinforcement Learning framework to determine a node's trustworthiness. A node's exclusion from the network occurs when its trust value falls below a certain threshold, guaranteeing network security. Also, the AODV protocol is used for packet routing.
- To start, we provide a deep reinforcement learning (DRL) instance of constructing the best possible link quality values, or costvalues, which aid in the routing process and allow it to choose the QoS route with the least amount of queuing time, all while keeping the number of hops in mind.
- Secondly, we provide a DQR protocol that uses the DRL model for reactive deep reinforcement learning-based quality of service (QoS) routing. In order to locate the quality of service path that avoids harmful nodes in the environment, the suggested DQR protocol is used.
- Even in highly dynamic network settings, like MANETs, the suggested technique may adapt successfully. In addition, it is capable of identifying malicious nodes of any sort, including those that operate on an isolated channel.
- Current routing protocols including Secure AODV, Dynamic Source Routing (DSR), and Ad hoc On-demand Distance Vectors routing (AODV) may be implemented using the suggested way without specialized auxiliary devices. This allows for its versatile use in MANETs using any routing protocol.

This paper is organized as follows for the rest of it. Part II discusses relevant research on the topic, including defenses against wormhole assaults. Section III explains the study's network and attack models, and Section IV presents the suggested key technique, breaks it down into its architecture, and explains how it detects wormhole attacks. Section V then shows the results of the simulations run to see how well the suggested technique works in contrast to previous wormhole detection algorithms in different routing protocols. Section VI wraps up the report and delves into the study's shortcomings.

I. Related Work

An algorithm was suggested in [18] that use a technique to modify the sequence number in control packets, specifically the Route Reply Packets in the popular AODV routing protocol. That technique can detect blackhole nodes and eliminate them from the route, reducing data loss. When compared to the old Intrusion Detection System that was installed for AODV, the suggested approach performs better in the simulations. To strengthen the safety of 150-node MANETs via the use of trust-based procedures, an improved AODV protocols for routing called Proposed_TAODV is presented in [19]. Under situations involving growing malicious node presence, the Proposed TAODV is tested in a thorough simulation against both current AODV along with Dynamic Source Routing protocols. In comparison to the benchmarks, Proposed_TAODV exhibits better performance and resilience, as seen by a greater Packet Delivery ratio, lower Average End-to-End delay and larger Throughput. To get around the security problems of the SAODV protocol, which cause transmission delays due to each node's energy consumption, BP-AODV is introduced as a secured manet routing system in [20]. Several potential dangers might compromise the functioning and accessibility of MANETs. One kind of attack that actively lowers network performance by discarding packets on purpose is called a blackhole attack. To protect MANETs against SMCBA, or secure multipath blackhole attacks, they provide a secure multipath strategy in that article. To identify and remove the bad node, the SMCBA strategy uses a timer-based chaotic map and luring technique. Experiments are conducted on NS2 using simulation by investigating various circumstances. Hopefully, a new attribute of a wireless node, the amount of routing error messages sent by a node, will be developed based on the results of the research [21]. That recently added feature of a wireless node may be employed to establish trustworthiness and may affect network performance. By using that trust value, the black hole route may be located, and the route will subsequently be removed from the routing database. In order to simulate the effects of Blackhole nodes and evaluate the efficacy of AODV and DSR rules, the researchers used the NS-2.35 ns-allinone2.35 version in [22]. The average efficiency, packet delivery proportion, and residual energy were some of the measures that were the focus of the research. According to the results, DSR had higher throughput than AODV, but AODV had superior energy usage and packet delivery. In addition, the research took environmental conditions and data sizes into consideration. In order to construct AODV and DSR protocols and simulate the influence of black hole nodes, the NS-2.35 ns-allinone-2.35 version was used in [23]. Using residual energy, average throughput, and packet delivery ratio as measures, the research found that DSR outperformed AODV in throughput while AODV outperformed DSR in energy efficiency and delivery. The investigation also took environmental conditions and data quantities into account. The AODV, Dynamic routing of sources, Geographic routing protocols, and optimized link state routing are some of the routing protocols that are tested in [24] while TCP-based MANETs are subjected to Jellyfish delay variance attacks. In addition, they compare the TCP protocols known as TAHOE, RENO, and SACK. The OPNET simulator is used to replicate certain routing technologies and assess their performance based on

particular network characteristics. When tested against the jellyfish delay variation attack, the AODV protocol outperformed the others, including DSR, TORA, OLSR, and GRP. Both online and offline modes of operation are supported by the suggested method in [25]. Each CH node in the network collects a variety of Wi-Fi statistics while it is not online, including the Received Signal Strength Indicator, transmitter power, battery level, distance, and number of transmission retries. In order for the CH nodes to establish the transmission power, ML techniques find a look-up table. Each SCH node in the system shares that table with all the other CH nodes. That procedure avoids the P-CH and S-CH nodes' occasional reelection, which increases the lifespan of the network. When running in online mode, SCH uses H-AODV to detect and eliminate any CH nodes that are malicious (ns-2.34). With an emphasis on security, the most popular routing protocol, AODV, is examined and improved in [26]. Particularly, they are focusing on making Blackhole Attacks more secure. The Secure AODV routing protocol is an adaptation of the AODV protocol that they developed using the Hash function validation method. Through the use of execution and simulation utilizing the network simulator (NS-2.35), the solution to both the single- and cooperative-blackhole attacks has been validated. Shown below are two possible outcomes of black hole assaults. 1) think about the one network node that is completely unconnected. 2) Scenarios in which black holes work together. Using the NS3 simulator and the parameters relating to routing overhead and packet delivery ratio, the authors of the paper [27] optimized the AODV routing protocol for usage on mobile ad hoc networks by analyzing Sybil attacks and then using the Bacteria Foraging Optimization algorithm. Bio-inspired algorithms, such as BFO, effectively mimic the behavior of bacteria and have applications in many fields. At the end, they compared the network nodes before and after the attack's compensation with BFO. The findings show that BFO is effective in awarding against Sybil attacks. The goal of that study is to address energy consumption and environmental sustainability in MANETs via the creation and assessment of defense mechanisms based on AODV. The goal is to successfully mitigate blackhole assaults. Because of its minimal overhead and on-demand nature, AODV is a popular MANET routing technology. But it's vulnerable to assaults since it doesn't have built-in security features. Green routing optimization, energy-efficient intrusion detection, collaborative energy sharing, solar-powered routing, energy-aware route selection, and energy harvesting from environmental causes are all part of their system. Their defensive mechanism works to improve network security while simultaneously reducing consumption of energy and environmental impact via route selection that takes these aspects into account. Numerous simulations and performance studies are carried out utilizing network simulation tools to test the efficiency of the suggested defense measures. The innovative hybrid secure routing method S-DSR is the subject of attention in [29], which ensures the delivery and efficiency of packets across the network's nodes. In order to determine the safest path for transferring files, that protocol makes use of neighbor trust information. It is OMNET++ that makes use of that protocol. When compared to competing protocols like AODV and AOMDV, it provides a better combination of speed and latency. In the future, industrial wireless networks will employ MANETs, which stand for mobile ad hoc networks, as its communication protocols. The interconnection of smart gadgets will be decentralized via these protocols. Digital data is one-dimensional, making indirect use of encryption technologies impossible. These magazines exist only in digital form. They need a secure, lightweight keyframe extraction method to make e-healthcare MANETs more private. The goal of that work is to provide a safe protocol that wireless MANET networks may use. To test how well MANET routing protocols like AODV, TORA, GRP, and OLSSR fare against Distributed Denial of Service assaults, see [30]. In order to evaluate the performance of these routing protocols using specified network metrics, they are simulated using the OPNET simulator. The experimental findings demonstrate that when subjected to a DDOS assault, the TORA protocol outperforms the AODV, OLSR, and GRP protocols. A research analyzing the performance of multicast technology in VANETs utilizing the Multicast On-demand Distance Vector Routing Protocol—a protocol that is frequently used in MANETs—was conducted in [31]. Similar wireless devices that are combined with sensors and made expressly for purposes related to safety, privacy, and security are also used as wireless nodes in networks of wireless vehicles. Improving and expanding the set of service quality metrics (received packets, latency, productivity, node energy use, etc.) is a focus of research. That paper's objective is to provide and enhance VANETS multi-cast transmission method in order to lessen packet loss, delay, and boost throughput. In [32] technique for detecting black hole attacks grounded on statistical theory is presented in that study. Black hole attack detection and prevention is made possible by BDA's real-time data collection capabilities. To identify a black hole attack, the suggested method uses a statistically-based balance threshold value. In the event of an attack, every node that responds to the route using a SN value higher than the threshold is promptly isolated. The paper goes on to provide an improved version of the AODV protocol that uses a BDA solution: BDAODV, which stands for black hole attack identification and routing protocol. A network model to randomly movable nodes is used to assess and compare the BDAODV protocol's performance with comparable solutions. According to the simulation findings, the suggested protocol performs admirably in the network situation when subjected to a black hole assault with varying numbers of hostile nodes.

II. WORMHOLE ATTACKS IN MANET

Here, we outline the groundwork that was necessary to carry out this investigation.

In a MANET, an external assault and an interior attack are two distinct types of threats. (a) Attack from Outside the Network: Nodes outside the network are the ones responsible for these assaults. It leads to delays and

inaccurate routeing data transmissions. The inaccessibility of services is another consequence. (b) An assault that started within the network itself, initiated by individual nodes. In this kind of attack, the bad node impersonates a legitimate one in order to get unauthorized access. Various forms of attacks may disrupt MANET architecture, which in turn affects applications running at higher layers. These include wormhole, blackhole, greyhole, flooding, replay, DoS (Denial of Service), man-in-the-middle, and evasive assaults. In a wormhole attack, at least two malicious nodes work together to create a tunnel that takes the quickest route from the starting node to the ending node in the network. The tunnel is used by the malicious nodes to send packets to each other. A result of this assault is that the network's usual packet flow is disrupted.

You may see the wormhole assault in Figure 1. A hostile node intercepts a control packet at one end of the tunnel and relays it to a cooperating node at the other end over a private channel; the receiving node then rebroadcasts the packet locally. When dealing with a wormhole assault, there are essentially two stages. The first stage involves the wormhole nodes engaging in many pathways. Finally, these bad nodes begin taking advantage of the packets they've received. Colluding nodes may drain the power of other intermediary nodes by repeatedly sending data packets through and across a virtual tunnel, or these nodes might muddle protocols that rely on the physical position or closeness of nodes. Malicious wormhole nodes may delete, alter, or transmit data to an outside source.

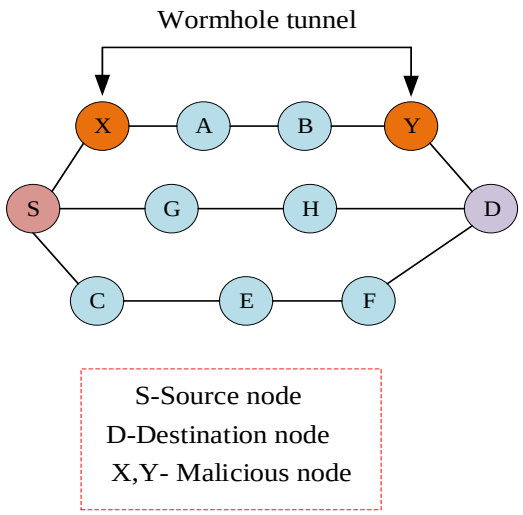

Fig.1. Wormhole Attacks Scenario

Whenever it's needed, the AODV protocol calculates the route data to the destination. Part one of the AODV protocol is Route Discovery, and Part two is Route Maintenance. In an ad hoc network, an RTERQS packet is broadcast to determine the path, and an RTERPL packet is unicasted to the source to confirm receipt. Two concepts used by the DSR protocol are source-routing and route-caching. According to source-routing, all of the route information is carried by the sender as it travels through the network. The intended node will get routing-related information from each node's route cache. If no reserved route is found in the cache at that point, the route discovery stage operates similarly to the AODV protocol.

Using MANET characteristics such as position, duration, hop count, neighborhood, packets of data, route reply, as well as route request, wormhole attacks may be detected. In this part, we will quickly go over these aspects.

4.1 Distance

For instance, in the event of an attack, the precise position of the invader node is crucial. With its aid, we can pinpoint the location of the malicious node in our network. So, pinpointing the exact position of the node will be a breeze. The system's price goes up when every node is linked to the global positioning system. One solution is to equip the receiver node with a GPS so it can always know where its neighboring node is.

Information on the relative nodes is collected using the specialized antenna. Finding the source of the data transmission is made possible with the aid of the related node. Using a specialized antenna or GPS will raise the price of the system, which is the biggest drawback. The system's battery life will be reduced when using a worldwide positioning system or a specific antenna. Since nodes in mobile ad hoc networks are always moving around, relying on their detected locations could lead to an inflated false positive rate.

4.2 Time

You may also use the time feature to identify the wormhole assault. When an attacker node is present, the per-hop time of the route is higher than that of the regular route. The network's synchronized clock allows for precise monitoring of the time difference between the node's transmissions from source to destination. An alternative way to determine the time difference that does not involve a synchronized clock is as follows: starting at the first node, send a hello message. When the last node reaches its destination, it replies with another hello message to the source. The time it takes for the hello message to travel from the source to the destination is then monitored. After subtracting the timestamps from the source, destination, and intermediary nodes, and then dividing by 2, the time difference between the sender and the recipient may be determined. This approach calculates the average time required by each hop, which is useful since synchronized clock implementation is difficult and costly.

4.3 Hop count

Because worm whole nodes directly attack network traffic by displaying the erroneous route—that is, the shortest path—the hop count technique is employed to identify worm whole assaults. Since the hop count does not rise while the node travel in the attacked private route, the attacker's path will have less hops than the usual way. Hop count using location or tie approach may be used to identify the full attacker node of the worm. If you divide the total time or distance traveled by the total number of hops, you'll get the average time it takes for each hop. The presence of a malicious node in a hop is indicated by its greater average tie of hop. A synchronized clock or specialized antenna is

necessary for the network to function for models that rely on time or distance mechanisms.

4.4 Neighborhood

The attacker node's primary role is to pose as a neighbor node to non-neighbor nodes. This statement provides enough information to identify the attacker node, including details about its neighbors. A number of methods exist for discovering worm attacks; one of them involves sending a hello message to both of your close neighbors in order to compile and store information about your local neighborhood nodes. Because every node in a dense network has numerous neighbors, this method won't work there. Because nodes are inherently dynamic and constantly changing positions, analyzing only two neighboring nodes increases the amount of time, energy, and storage needed for the analysis. Additionally, sending out a welcome message increases network traffic, which in turn decreases overall network efficiency and raises the false positive rate.

4.5 Data packets

Using data packets, one may identify a wormhole assault by comparing the total number of nodes that transmit and receive data in the network. In this paradigm, each node is configured to listen to the function of its neighbor. The number of nodes transmitted by a neighboring node is recorded by those nodes. Using this, they may check whether the node has been dropped, updated, reached its target, or sent to another node other than its destination. Using this data, they can determine the trustworthiness of every node in the network, pinpoint the malicious node, and apply it to dense networks. Table 2 displays a comparison of characteristics used to identify wormhole attacks.

4.6 Route reply

Figure 1 shows the RREP message that may be used to identify the wormhole assault. Any node in the network that receives a request for a new route will immediately transmit an RREP message to its neighbors or the destination node. This is not an attack strategy that the malicious node will use. Since route requests are received in a unicast fashion, they must be put in a valuable node in order to evaluate and keep the node's record. The network's efficiency will be reduced if the node is set to valuable node.

III. PROPOSED WORK

The study's network along with attack models are described in full here. These models provide the groundwork for comprehending how the suggested technique for wormhole attack detection and defense works. This wormhole attack technique is shown in Fig. 1.

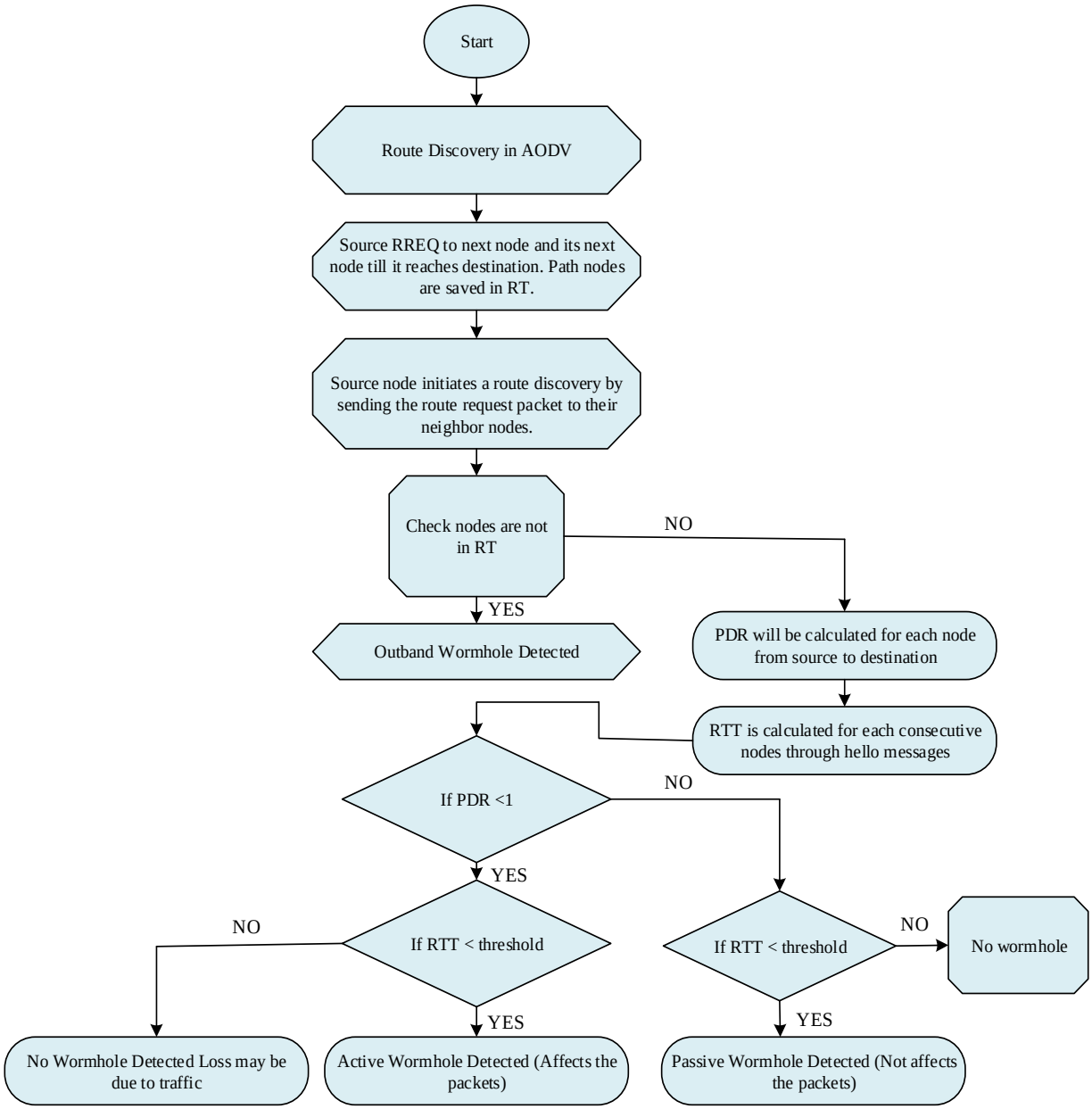

Fig.2. Flowchart for Wormhole Attacks

A. Network Model

The research presupposed that all MANETs consisted of static, non-switching nodes. Provided that the nodes traveled at rates ranging from 0 to 5 m/s, the random-walk 2D paradigm was used to initialize the nodes' locations and govern their movement. Furthermore, all of the nodes could communicate with one another, and the range of every node was same, allowing for two-way communication. A MANET was presumed to use reactive routing (also known as on-demand routing) with OR in the research. When a request is made, or a requirement to deliver a packet arises, reactive routing discovers a routing route. In MANETs and other dynamic network situations where node connection changes often, this routing strategy is commonly utilized. In order to address the shortcomings of current approaches, we provide a strategy that may be easily adjusted to meet the needs of MANET security. In terms of how it functions, it learns the trust levels between nodes using reinforcement learning. Multiple verifications are used to calculate the award under this procedure. The network will identify a node as potentially harmful and remove it from the network in order to provide a secure communication environment if its learnt trust level drops below a certain threshold.

This method chooses the best node to transmit a packet from a pool of candidates, unlike DSR and AODV. A node's location, energy state, and communication status are among the many aspects taken into account throughout this selection process. Reducing the likelihood of repeated transmissions and enhancing communication efficiency, a signal is delivered to the other candidate nodes to terminate packet transmission when one of them successfully receives the packet.

B. Adversary Model

The enemies are present in the hostile environment where the network is formed. The ability to intercept, record, and replay messages—including routing protocol messages—is assumed to be in the hands of the enemies. Additionally, the attacker may get access to the communications containing cryptographic secrets by compromising the legal nodes. Because of this, the enemy may set up and manage a malicious node. The enemy node having the ability to conspire with other hostile nodes. The wormhole is one kind of assault that involves collaboration.

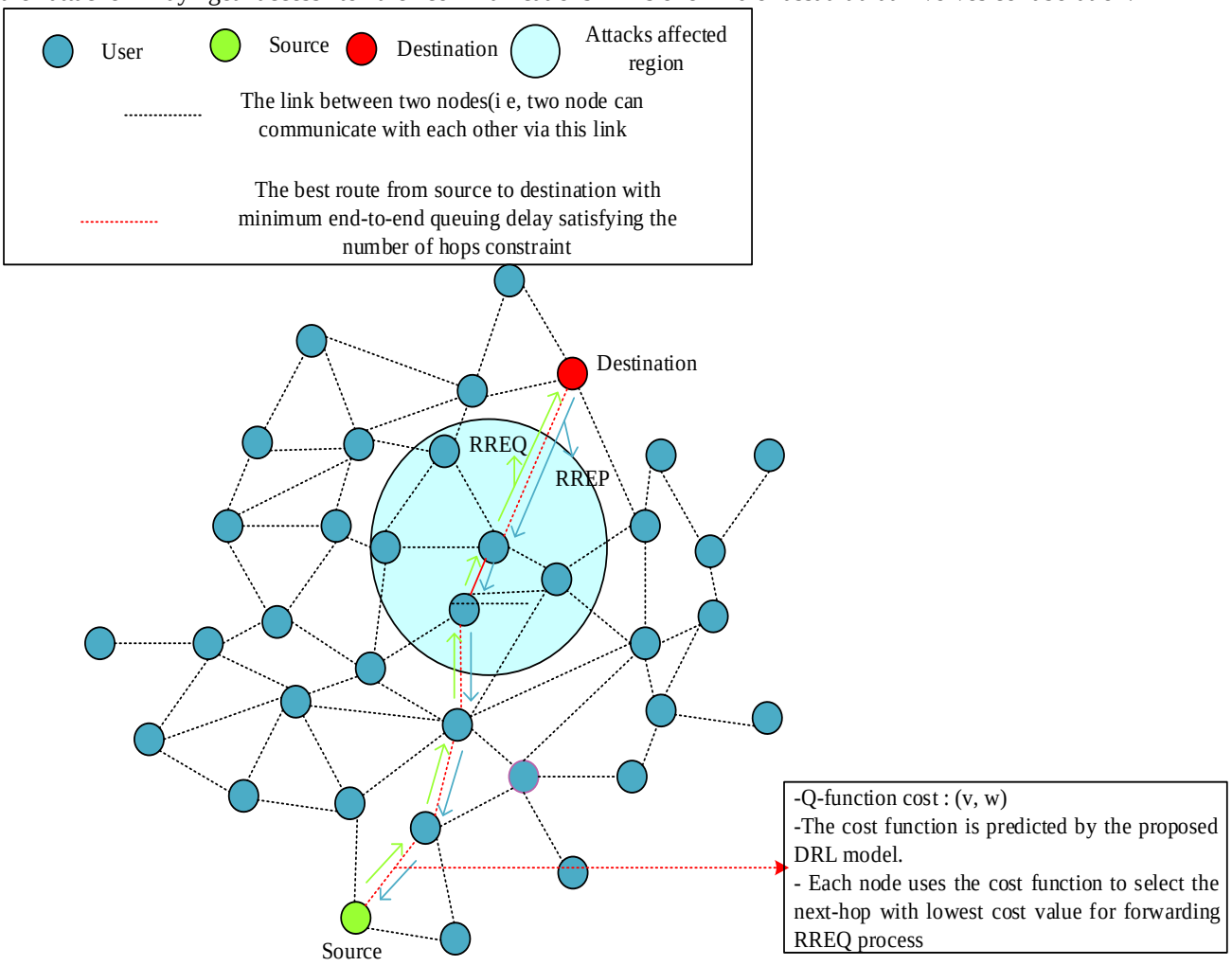

Fig.3. MANET for Wormhole Attack Detection

C. DRL for Wormhole Attacks Detection

With the number of hops limitation in mind, the suggested DRL model is made to construct cost-values of connections that aid the DQR protocol in determining the optimal route with the smallest end-to-end queuing time. As seen in Figure 1, the suggested DQR protocol is executed in sessions at every node. The two main parts of each session, data transmission and routing, are shown in the following order:

Routing phase:

- During the forwarding RREQ process, neighbors are contacted by means of hello packets whenever a source wants to transmit data to a destination. The source then uses the DRL model to create an RREQ packet, which it then transmits to the closest neighbor that is outside the main user's impacted area and has the lowest cost-value. After receiving the RREQ, the node will update its routing table to reflect the previous hop as the sender. It will then route the RREQ to the next best neighbor, who is chosen using the same procedure as before. This continues until either the destination gets the RREQ or the procedure times out.
- The receiving end will respond to the RREQ by sending an RREP back to the sending end via the prior hop. After receiving the RREP, the node will update its routing table to show the next hop as the sender. It will then proceed to deliver the RREP back to the source through the previous hop. Until the RREP gets to its origin, this procedure is repeated. The information transmission phase will begin as soon as the source gets the RREP.

Phase of data transmission: information is sent from the source to the destination along the predetermined path. A Poisson arrival mechanism and an exponentially dispersed

service interval form the basis of the queuing delay paradigm M/M/1 for each node, which is examined in this work. Because of the arrival rate λ with the server time frequency μ packets per second. One thing we can deduce from the Markov chain model of the M/M/1 system is that (i) on average, a packet spends $\mathrm{Tq} = 1/(\mu - \lambda)$ This include both the waiting time and the amount of time spent providing the service, (ii) the time a packet takes to get through the queue is $\mathrm{Wq} = \mathrm{Tq}/\mu$ Nq=λWq is the average amount of packets in the queue.

Statement 1. There comes a point when a node's queuing latency drops as its connection and queue size both go down. Consequently, the reward component for the suggested DRL model will be designed using this property.

The Minimum End-to-end Queuing Delay: MQD Problem

Assuming a starting point (src), an endpoint (dst), and a path $\mathrm{P}(\mathrm{src}, \mathrm{dst}) = \{\mathrm{src} = n_m \to n_{m-1} \to \cdots \to n_1 \to n_0 = \mathrm{dst}\}$. One way to represent the total amount of hops in route P is as #hops (P)=m. This is the way the end-to-end queuing duration for route P is stated:

$$\mathrm{Tq(P)} = \sum_{v=0}^{m} \mathrm{Tq}_{\mathrm{r\_pkt}}(v) \qquad (1)$$

where $\mathrm{Tq}_{\mathrm{r\_pkt}}(v)$ is the typical amount of time that a packet of routing data spends in node v. Finding the optimal path via (1) with the smallest possible end-to-end queuing time while keeping the number of hops limitation in mind is the MQD issue. Our proposed DRL model for calculating connection cost-values—inputs to the DQR protocol's route establishment process—will address this issue.

The following schema represents the proposed DRL model as a model-free Markov decision process (MDP).

- A robot is presumed to be beginning at the source node, according to the agent. It will solve the MQD issue by finding the optimal path to the destination. The agent here is this robot.
- Robot state: There is a set of states S that correspond to a set of nodes V. When the robot reaches a certain point in time, it is said to be in state v if it is at node v ∈V.
- Step: When the robot is in state v, it has a set of actions A_v that include moving to any of its neighbors in the changing set of neighbors of node v (NB_v). At state v, we represent a node w∈A_v as an action performed by the robot.
- At a given instant in time, the robot in state v is presented with an environment that comprises the location, queue size, and connection details of every node in the network.
- Reward function: If the robot chooses an action w that is in the set A_v at state v, the reward function has been set as

$$\mathcal{R}(v,w) = \begin{cases} \alpha_q \dfrac{\mathrm{Conn}_w \mathrm{Qsize}_w}{\mathrm{Conn}_{\max} \mathrm{Qsize}_{\max}} + \alpha_h \mathrm{W}_{\mathrm{hop}} & \\ & \text{if } w \in \mathcal{A}_v, \\ +\infty \qquad \text{otherwise,} & \end{cases} \qquad (2)$$

where Conn_w and Qsize_w and the size of the queue at node w, accordingly, $\mathrm{W}_{\mathrm{hop}}$ is a constant value in $(0,1)$, α_q and α_h find the values of the weights between zero and one such that $\alpha_q + \alpha_h = 1$.

- The robot performs an action at state v according to the quality function (Q-function) $w \in \mathcal{A}_v$ with the Q - function as follows:

$$Q(v,w) = (1-\alpha)Q(v,w) + \alpha\left(\mathcal{R}(v,w) + \gamma \min_{a \in \mathcal{A}_w} Q(w,a)\right) \qquad (3)$$

where α represents the discount factor and α stands for the learning rate.

At the beginning time, we assign $\alpha_q = 1$ and $\alpha_h = 0$ within the incentive function (2). In order to update Q-values, the DRL is run through several iterations, or epochs. Once the source determines a path to the destination using the revised Q-values, it determines how many hops this path will take. The weights α_q as well as α_h of the reward function are modified if the number of hops exceeds the constraint hop _"thres " $\alpha_q = \alpha_q - 0.1$ and $\alpha_h = \alpha_h + 0.1$

The DRL model gives Q^* - values, which represent the link cost-values, for every environment $(\mathrm{cost}\,(v,w), \forall v,w \in \mathcal{V})$. In order to determine the optimal path to their destination, every node v in the network may choose a neighbor was their next-hop if their cost(v,w) is the lowest. The process of upgrading cost-values will take a considerable amount of time. The DRL model circumvents this problem by making real-time cost-value predictions for any environment using a deep neural network (DNN) in the following way:

- Use the suggested DRL model to produce a random set of settings, and then calculate the cost-values.
- Take environmental factors into account as input parameters; they include location, connection, and queue size.
- Think of the cost-values as a vector representing the output of each environment.
- A system that can forecast the cost-value for the routing process is developed by training the DNN model with the provided data set.

In order to determine the optimal path with the smallest end-to-end queuing time while still meeting the hop count restriction, the suggested DQR protocol makes use of the anticipated cost-values from the suggested DRL model.

Here is how the suggested DQR protocol might be shown at each node:

Assuming node v is the origin, go to Step 1.1. If not, continue to Step 2.

Step 1.1. In order to find out where its neighbors are, how connected they are, and how big their queue is, a source node (src) will broadcast a request information (RNI) packet. Then it will go on to Step 1.2. In any case, continue to Step 3.

Step 1.2. The cost-values of neighbor linkages are computed by node src using the DRL model. Next, the source node will create an RREQ packet and deliver it to the neighbor with the lowest cost-value. After that, it will proceed to Step 3.

Step 2. Repeat Step 2.1 in the absence of dst at node v, and Step 2.3 in its place.

Step 2.1. In the event that node v gets an RREQ packet from source, it will add the sender's id to its routing database as the previous-hop, then broadcast an RNI packet to find out where its neighbors are located and proceed to Step 2.2. In any case, continue to Step 3.

Step 2.2. To determine the value of neighboring connections' costs, node v use the DRL model. Step 3 is then initiated when node v transmits the RREQ packet to its nearest neighbor with the lowest cost-value.

Step 2.3. In response to an RREQ packet, dst will send an RREP packet to the source and proceed to step 4.

Step 3. In the event that node v gets an RREP packet from dst, go to step 3.1. If not, continue to Step 4. 3.

Step 3.1. In the absence of a source address, node v will return the RREP packet to the preceding node while adding the sender's ID to its routing database as its next-hop. Continue to step 4. Proceed to step 3.2 if not.

Step 3.2. Next in the routing table is the sender's ID, which is recorded by the src. Continue to the fourth stage.

Step 4. We have finished the routing procedure. Proceed to Step 5 if node v is the source.

Step 5. Using the predetermined path, the source transmits data packets to the destination.

D. Secure AODV for Routing

By sending messages across the high-speed channel, a wormhole attack may make the Route Request packet get to its destination more quickly than it would using the conventional route. The identification of wormhole nodes is accomplished by locating the high speed channel. Data transport across a wormhole connection is faster. Every node along the route from origin to destination has its PFR and RTT determined. From origin to destination, the Packet Forward Ratio (PFR) is determined for every node. Consider two nodes A and B that are next to each other. A node's packet forwarding ratio (PFR) is the proportion of data packets sent and received by that node. One way to express PFR mathematically is as

$$\mathrm{PFR} = \mathrm{S}/\mathrm{R} \qquad (4)$$

In this context, S represents the data packets that node B transferred to the next node and R represents the data packets that node B received from the one before it. Whether or not packet loss is occurring may be determined from this.

In order to discover a route, the source node sends an RREQ packet to its surrounding mode. As soon as the RREQ message reaches a node in the network, it is verified to be a destination node. Upon confirmation that it is a destination node, the node is redirected to its origin. Alternatively, the network neighboring the node receives the request message. This will continue until the packet containing the route request reaches the node that it is intended to reach. For each node, we calculate the packet forward proportion and the round trip time. We can identify a wormhole-affected connection and identify two nodes as malicious if the packet forward proportion is less than 1 and the round-trip time (RTT) is less than the threshold value of one second. If the round-trip duration is less than the threshold and the packet forward proportion is less than 1, it may be concluded that packet loss occurs due to network traffic. Checking round trip time will be done if the packet forward rate is less than 1. Passive wormholes are identified when the round trip duration is less than a certain threshold. This is because wormhole nodes exploit the high speed network to intercept data without changing the packets. If the RTT is greater than or equal to the threshold, then the route is real. The following is the suggested updated secure AODV routing protocol.

Algorithm 1 Modified secure AODV
routing protocol
Step 1. Begin
Step 2. Discovering routes across the AODV protocol
Step 3. The routing table verifies the traversed nodes as soon as the source node begins sending the packet.
It is possible to identify an out-of-band wormhole if it is not in the routing table.
Then go to step 4.
Step 4. Each succeeding node has its PFR and RTT determined. From beginning to end
Step 5. If PFR < 1, Checked for RTT

(i) If RTT < threshold, (ii) Found an active wormhole Otherwise, the wormhole does not exist (traffic loss might be the cause).
Step 6. If not, verify the RTT.
(i) RTT < threshold, passive wormhole is identified
(ii) Else there is no wormhole
Step 7. End

Analysis of Round Trip Time and Hop Count

The round-trip time (RTT) of a packet is related to the total amount of hops in its path and measures how long it takes for a packet to get from its source to its destination and back again. The wormhole attack may be detected by looking at the hop count, which will be much lower when an attack is there but much higher when there isn't. Its round trip time (RTT) is calculated as the interval between when it sent its neighbor a hello packet and when it got an acknowledgment. Here is how we will calculate the round-trip time from node A to node B:

$$\text{Round trip time}_{A,B} = T_{RA} - T_{SA}, \quad (5)$$

where TRA is the period between the time node A receives confirmation that it sent hello packets and node B receives them, and TSA is the period between the two.

With an increasing number of hops, the associated route's RTT also rises. Because of the existence of the wormhole connection, the total amount of hops for the identical source-destination pair will be much lower in a wormhole assault than in the real path. The round-trip time (RTT) of a wormhole-linked route will be longer than that of a conventional route with the identical amount of hops since the packets will have to travel farther. Based on the theoretical calculations of the maximum RTT, it is clear from Table 2 that the RTT of the usual route will be either below or equal to the threshold.

$$\text{Packet Transmission Delay, } T_{\text{trans}} = \frac{\text{Packet Size}}{\text{Bit Rate}} \quad (6)$$

$$\text{Propagation Delay, } T_{\text{prop}} = \frac{\text{Distance}}{\text{Propagation Speed}} \quad (7)$$

$$\text{Packet Delivery Time, } T_{\text{del}} = T_{\text{trans}} + T_{\text{prop}} + \text{Queue}_{\text{delay}} \quad (8)$$

$$\text{Round Trip Time} = (2 * T_{\text{del}}) + \text{Processing Time (4)} \quad (9)$$

With a small amount of hop counts in a path, the likelihood of pollution increases since the wormhole attack indicates a hop count considerably lower than the real quantity. This holds true when the total energy of the current route nodes increases and the round trip duration is short. From the standpoint of route efficiency, it is also desirable to increase route security from the standpoint of wormhole attacks. Thus, the best course of action is the one that maximizes Fr's indicator, as determined by Equation (10).

$$\text{Fr (Energy Hop Count. RTT)} = \left(\frac{\text{Max RTT}}{\text{RTT Route } i}\right) + \left(\frac{\text{Hop Count Route } i}{\text{Max Hop Count}}\right) + \left(\frac{\text{Energy Route } i}{\text{Max Energy}}\right) \quad (10)$$

Equation (11) is used to derive the general route selection indicator, which takes into account metric safety and effectiveness and combines findings from both the first and second phases.

$$\text{AODV\_ Route} = (1 - Pwh(r)) * \text{Fr (Energy. Hop Count. RTT)} \quad (11)$$

Once harmful nodes have been located, an alarm message is delivered to all of the nodes in the network. Every node gets rid of the bad ones. Upon receipt of the alert message, any neighboring node will respond with an RERR (Route error) message to the sender. It will find a new way to the receiver, free of harmful nodes, and start the route discovery process afresh. This prevents wormhole attacks from compromising the network.
Figure 7 depicts flow chart.

IV. Results & Discussion

In this part, we describe the simulation tests that were run using different routing protocols to ensure that the wormhole detection approach that was suggested really worked. The purpose of these tests was to determine how well the suggested solution protected against wormhole assaults. Important insights into the proposed algorithm's behavior and defenses against wormhole assaults in real-world network settings were gleaned from the trials.

This project makes use of the open-source and cost-free NS3.24 Network Simulator. When comparing to other Network Simulators, Ns-3 produces more efficient results. You can see the simulation parameters in Table II. A wormhole attack is simulated in the proposed architecture, where two attacked nodes are linked over a high-speed wired connection that spans a distance that is roughly 8 or 9 hops. By comparing the specified route's RTT with the threshold, wormhole attacks along a route may be identified. The suggested clustering technique is used to confirm and pinpoint the malicious nodes after an attack is detected. Here we show how well the suggested DQR protocol works with varying maximum speeds for mobile nodes (20, 40, 60, and 80 km/h). The simulation takes place over a 1 × 1 km2 area and follows a random mobility model with 50 mobile nodes that can move around. The nodes have a transmission range of 250m, a coverage range of 250m, a queue arrival rate of 10 packets/second, a queue service utilization rate of 20 packets/second, as well as the simulation lasts for 1000s.The NS3 simulation framework is used to implement the suggested DQR protocol in a Python environment.

Table. I. Simulation Parameters

Network Parameters	Values
Simulator	NS-3
Platform	Ubuntu 16.04
Simulation Time	100 sec
Number of Nodes	7,15

Number of Wormhole Nodes	3
Traffic	CBR (Constant Bit Rate)
Transmission Speed	250 Kbps
Transmission Rang	250 m X 250m
Packet Size	512 bytes
Routing Protocol	AODV
Transport Protocol	UDP
Physical Layer	DLT IEEE802_11
MAC Layer	802.11 b

TABLE II. Parameters set for proposed algorithm.

Description	Parameter	value
Total episodes	total-episodes	5000
Total test episodes	total-test-episodes	100
Max steps per episode	max-steps	99
Exploration rate	epsilon	1
Exploration probability at start	max-epsilon	1
Minimum exploration proba-bility	min -epsilon	0.01
Exponential decay rate for ex-ploration prob	decay-rate	0.01

Performance Parameters

We used the Performance Parameters described below to simulate and compare the network performance of AODV both with and without an attack (Blackhole and Wormhole):

- **Packet Delivery Ratio:** PDR is calculated by multiplying the number of packets received by the destination node by the number of packets sent by the destination node, and then multiplying the result by 100%.
- **Throughput:** The throughput of a network is defined as the number of bits per packet that a destination node is able to receive, divided by the time between the first packet sent and the last packet received.
- **End to End Delay (EED):** The sum of all delays—queuing, transmission, processing, and propagation—that occur throughout the transmission of packets from their point of origin to their final destination.
- **Routing Overhead:** Even if the paths taken by packets in the same flow from source to target are identical, the delays experienced by them will be different. Routing overhead is the fluctuation in packet delays.

Figure 4 compares the network throughput under wormhole attack using regular AODV and the suggested technique. Here, traffic load is represented on the X-axis in kbps while throughput is shown on the Y-axis in bps. Unless there is a huge data rate or a very large distance between two nodes, throughput typically grows proportionately with traffic load. With wormhole attacks present, throughput will be very poor since fewer packets will reach their destinations because of packet dropping. Since the route with the wormhole connection is chosen for packet forwarding in normal AODV, there is a noticeable decrease in throughput. After the attackers have been located and detected, the suggested clustering approach re-initiates route discovery to locate a safe path that is not under assault. The network's throughput will rise as a result of packet delivery over an attack-free path.

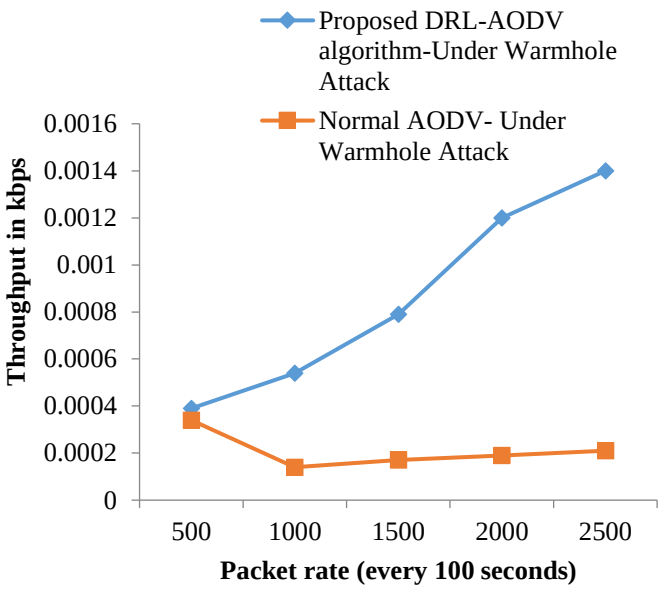

Fig. 4. Throughput in Kbps

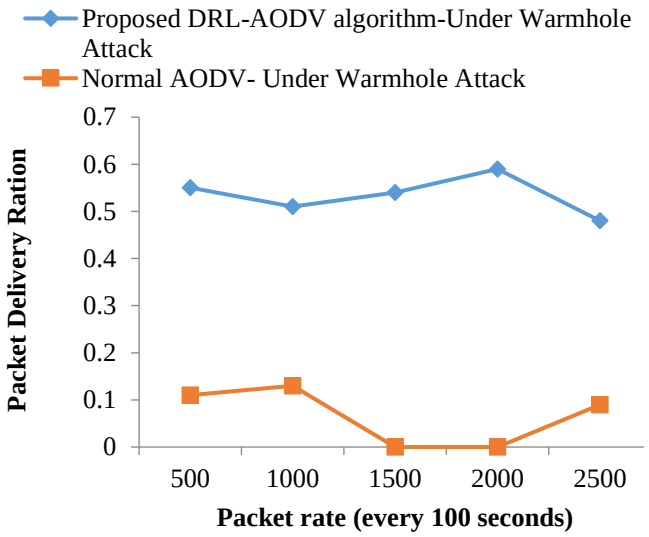

Fig. 5. Packet Delivery Ratio

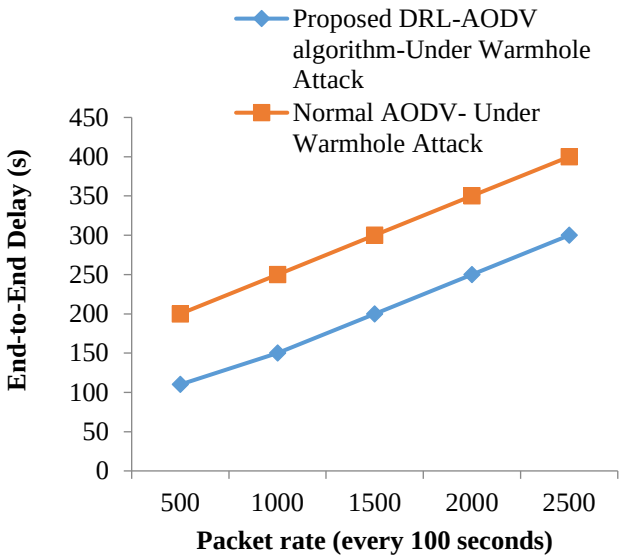

Fig. End to End Delay Analysis

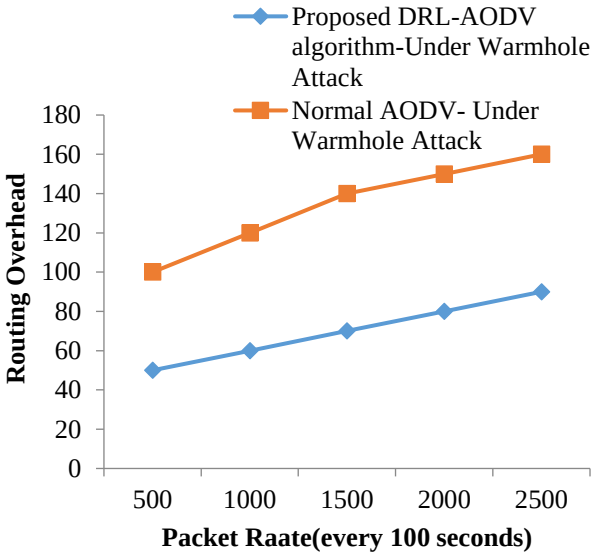

Fig. Routing Overhead Analysis

Under wormhole attack, the Packet Delivery Rate (PDR) of regular AODV and the suggested clustering technique are shown in Figure 5. Here, PDR is represented by the Y axis and traffic load in Kbps is shown by the X axis. Typically, the amount of packets transmitted over a network and, by extension, the amount of packets that make it to their destination, grows in direct proportion to the data rate. Typical AODV employs a malicious and lossy method for packet forwarding since it is unable to detect wormhole attacks along the route. The poor packet delivery ratio is caused by the wormhole connection purposefully dropping all data packets. Because it can identify wormhole attacks along the path and locate a safe way to the destination, the suggested clustering approach has a high packet delivery ratio.

With varying node speeds subjected to wormhole assaults, we display the end-to-end routing delays in Fig. 2 for the suggested DQR and AODV-based routing protocols. In most speed instances, the suggested DQR protocol uses less time than the AODV. The suggested DQR protocol uses a DRL model to determine the optimal next hop with the lowest possible end-to-end latency, which is why it is the best option. Conversely, the normal flooding RREQ method, upon which the AODV-based routing system is built, is a time-consuming way to reach the target.

A relationship between the node's speed and the control overheads of the DQR protocol for route formation is seen in Figure 3. The DRL method has advantages, such as lower overheads compared to the ADOV-based routing rules, as is shown by the DQR protocol. When sending an RREQ packet, the AODV-based routing system incurs several unnecessary overheads; in contrast, the DQR protocol uses the DRL model to simply unicast the packet to the nearest neighbor.

TABLE III. Result analysis of traditional algorithms

Sr.No	Algorithm	Throughput (Kbps)	Delay (ms)	Packet Delivery Ratio	Routing Overhead

1	AODV	723.13	343.73	71.25	120
2	DSDV	259.11	496.76	6725	114
3	OLSR	752.81	466.23	74.67	145
4	Proposed	743.56	428.58	92.65	55

TABLE IV. COMPARISON OF RTT OF NORMAL ROUTE AND WORMHOLE LINK WITH THEORETICAL RTT

No. of Hops	Theoretical RTT (ms)	RTT-Without Worm hole Attack (**ms**)	RTT- With Worm hole Attack (ms)
2	0.01092	0.0044	-
3	0.01638	0.0062	0.019
4	0.02184	0.0108	0.030
5	0.02730	0.0270	0.030
6	0.03340	0.0329	0.040
7	0.03822	0.0332	0.050

The suggested method's enhanced performance was due in large part to the fact that it made use of communication between nearby nodes to choose the best possible candidates for packet transmission. In order for the suggested strategy to make educated judgments and to reduce the effect of wormhole assaults, this routing information sharing and identification of possible harmful nodes were crucial. We did several simulations with varying random node motions to be sure the findings were legitimate. When compared to both the traditional and AODV-based routing protocols, the results consistently showed that the suggested technique was better. Because of how MANETs work, neither the suggested nor the wormhole detection methods were able to get the packet-to-wormhole ratio to zero. The absence of a central infrastructure or communication tool in MANETs makes it necessary to rely on the information sent between nodes in order to identify rogue nodes. Since this information is only sent via broadcasts, nodes who do not receive this signal will not know that a malicious node is there, even if it is discovered. In addition, because the nodes' locations are dynamic, the routing algorithm will direct packets to a malicious node if a node that does not receive the broadcast signal but comes into communication range with it nonetheless sends them. Put simply, packets delivered to a wormhole tunnel cannot be entirely stopped, no matter how much time passes, because of the rigid structure of the network.

The suggested system's key benefit is that it verifies the existence of wormhole attacks along the suspected path in addition to detecting attacks. Clustering adds cost to our suggested technique, which might make it slower on large-scale MANETs. No built-in protection mechanism protects AODV against denial-of-service assaults such as wormhole attacks or black hole attacks. This is because it is unacceptable to anticipate new security modules to result in substantial routing overhead. Secure and attack-free communication is guaranteed, notwithstanding an increase in routing and processing cost due to additional security modules.

V. Conclusion

In order to identify wormhole attacks in MANETs, this research presents a method based on Deep-Q-learning that uses a trust structure. The suggested technique takes wormhole attack features into account and, upon routing suspicion, dynamically changes the Q-value according to nodes' trust levels. During the process of validation, nodes that have Q-values below a certain level are flagged as potentially malicious and removed from the system in order to maintain reliable routing. Importantly, this approach is general enough to work with opportunistic and reactive (e.g., AODV and DSR) routing protocols. Therefore, it works well for both standard MANETs and more delicate wireless networks, such as those used by underwater sensor networks and vehicle ad hoc networks. Our suggested solution outperforms both AISs and traditional routing-based wormhole detection techniques in simulation trials when it comes to avoiding wormhole tunnels. But even with this victory, it is still not easy to alert every device of a discovered malicious node at the same time in MANETs because to their inherent characteristics, which are moving nodes that are autonomous and only capable of transferring limited amounts of data. Nodes flowing through the tunnel could not be contained to fewer than 10% using the suggested strategy in our simulations. Our future work will focus on finding a way to more effectively communicate information about harmful nodes to a wider portion of the network in order to circumvent this constraint. Establishing intermediary nodes as data relays and using broadcast techniques or clustering methods are two possible ways to efficiently propagate information about discovered malicious nodes and to achieve wider dispersion of threat data. Our goal in taking on this issue is to make the suggested approach even better at protecting MANETs against wormhole assaults.

References

[1] Ogundoyin, I.K., Omotosho, L.O., Jimoh, K.O., & Yusuf, A.G. (2020). Design and Simulation of a Secured Routing Protocol for Mobile Ad-Hoc Network.

[2] Sagar, P.V., Ushasree, D., & Reddy, G.K. (2020). PREDICTIVE APPROACH FOR TRUST MODEL SECURE ROUTING IN MOBILE ADHOC NETWORKS.

[3] Chopra, K. (2020). Mobile Ad Hoc Network Security using Mean Field Game Theoretic Threshold-Based Scheme.

[4] Bharanidharan, C., Malathi, S., & Manoharan, H. (2024). Detection of black hole attacks in vehicle-to-vehicle communications using ad hoc networks and on demand protocols. International Journal of Intelligent Unmanned Systems.

[5] PrabhakarReddy, B., Bhaskarreddy, B., & Dhananjaya, B. (2021). The AODV routing protocol with built-in security to counter blackhole attack in MANET. Materials Today: Proceedings.

[6] B, P.R., B, B.R., & B, D. (2021). The AODV routing protocol with built-in security to counter blackhole attack in MANET. Materials Today: Proceedings.

[7] Patel, B.B., & Patel, D.R. (2023). Study of Denial of Service Attack On AODV Routing Protocol in Mobile Ad-hoc Network. 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), 66-77.

[8] Sathyaraj, P., Devi, S.R., & Kannan, K. (2021). Host-based Detection and Prevention of Black Hole Attacks by AODV-ICCSO Algorithm for Security in MANETs. Ad Hoc Sens. Wirel. Networks, 55, 45-73.

[9] Minh, L.Q. (2021). AODV-MSA: A Security Routing Protocol on Mobile Ad Hoc Network. J. Commun., 16, 143-149.

[10] Nausheen, I., & Upadhyay, A.R. (2023). Performance Analysis of Efficiently trusted AODV serving Security in MANET under Blackhole Attack Using Genetic Algorithm. 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), 1127-1131.

[11] Kumari, A., Singhal, M., & Yadav, N. (2020). Blackhole Attack Implementation and Its Performance Evaluation Using AODV Routing in MANET.

[12] Priyanka, M., Prakash, O., Balaji, D.K., Shukla, D.S., Osd, D.M., & Singh-6th, J. (2022). MANET: IMPROVED SECURED ROUTING FOR AODV. 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), 747-751.

[13] Kannimuthu, P. (2021). Authenticated and Trusted AODV (ATAODV) Routing Protocol to Detect Blackhole Attack in MANET-Based Military Environments. Int. J. Interdiscip. Telecommun. Netw., 13, 51-71.

[14] Haoussi, F.E., Fezazi, N.E., Idrissi, S., Akchioui, N.E., & Fezazi, Y.E. (2023). Detecting black hole attacks in MANET using baiting and timer technique with AODV protocol. 2023 9th International Conference on Optimization and Applications (ICOA), 1-5.

[15] J., D., L, R., & S., J. (2021). A DCM Algorithm for AODV to Implement Energy Efficient Routing in MANET with Capacity Maximization. International Journal of Computer Networks and Applications.

[16] Rao, T.V., Swamy, V.K., Karthigeyan, K.A., Gopalakrishnan, S., Kalaichelvi, T., & Koteswari, S. (2023). Energy Efficient Trust Based Data Communication using AODV Protocol in MANET. Journal of Advanced Research in Applied Sciences and Engineering Technology.

[17] S M, U.S., D, D., C, C.D., & M, R. (2022). Safe Routing Approach by Identifying and Subsequently Eliminating the Attacks in MANET. ArXiv, abs/2304.10838.

[18] Shrestha, S., Baidya, R., Giri, B., & Thapa, A. (2020). Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol. 2020 8th International Electrical Engineering Congress (iEECON), 1-4.

[19] Versha Matre, E.A. (2023). Trust-Based Routing Selection Policy on Mobile Ad-Hoc Network Using Aodv Routing Protocol. International Journal on Recent and Innovation Trends in Computing and Communication.

[20] Ramesh, R., & Seshikala, G. (2023). Link Aware Multipath Routing to Defend Against Black Hole Attacks for MANETs. 2023 3rd International Conference on Intelligent Technologies (CONIT), 1-6.

[21] Chaitanya, M.P., Chowdary, B.S., Prasanna, P.L., Priyanka, M., & Tejaswi, K. (2023). TAODV Trust based AODV Protocol in MANETS to Mitigate Black Hole Effect. 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), 1348-1355.

[22] Alifo, F., Yakubu, M.A., Doe, M., & Asante, M. (2023). Analyzing the Impact of Blackhole Attacks on AODV and DSR Routing Protocols' Performance in NS-2. International Journal of Computer Science, Engineering and Applications.

[23] Alifo, F., Yakubu, M.A., Doe, M., & Asante, M. (2023). Performance Analysis of AODV and DSR Routing Protocols Under Blackhole Attack Using NS-2. Advanced Computer Science and Information Technology Trends.

[24] Omer, K.A. (2023). Impact of Jellyfish attack on routing protocols in TCP-based MANETs. University of Aden Journal of Natural and Applied Sciences.

[25] H. K., S., & K R, S. (2024). Co-Ordinated Blackhole and Grayhole Attack Detection Using Smart & Secure Ad Hoc On-Demand Distance Vector Routing Protocol in MANETs. International Journal of Computer Networks and Applications.

[26] Meena, D.K. (2020). Detection and Prevention of Black Hole Attack in Secure-AODV Network Using RSA SECURITY in MANET.

[27] Swathi, S. (2020). Bio-Inspired Approach Sybil Attack in AODV based MANET using BFO Algorithm. International Journal of Engineering Research and.

[28] Moumen, I., Rafalia, N., Abouchabaka, J., & Chatoui, Y. (2023). AODV-based Defense Mechanism for Mitigating Blackhole Attacks in MANET. E3S Web of Conferences.

[29] Tej, D.N., & Ramana, K.V. (2022). MSA-SFO-based Secure and Optimal Energy Routing Protocol for MANET. International Journal of Advanced Computer Science and Applications.

[30] Abood, K.A. (2022). Performance evaluation of MANET routing protocols under DDOS attacks. University of Aden Journal of Natural and Applied Sciences.

[31] Al-Shabi, M. (2020). Evaluation The Performance of MAODV and AODV Protocols In VANETs Models.

[32] Huy, L.D., Ha, T.T., & Tam, N.V. (2022). BDAODV: A Security Routing Protocol to detect the Black hole Attacks in Mobile Ad Hoc Networks. J. Commun., 17, 803-811