electronics

MDPI

Review

A Survey on Parameters Affecting MANET Performance

Ahmed M. Eltahlawy [1], Heba K. Aslan [1], Eslam G. Abdallah [2], Mahmoud Said Elsayed [3], Anca D. Jurcut [3,*] and Marianne A. Azer [1,4]

[1] Faculty of Information Technology and Computer Science, Nile University, Cairo 12677, Egypt
[2] Information Systems Security Management, Concordia University of Edmonton, Edmonton, AB T5B 4E4, Canada
[3] School of Computer Science, University College Dublin, Belfield, D04 V1W8 Dublin, Ireland
[4] National Telecommunication Institute, Nile University, Cairo 12677, Egypt
* Correspondence: anca.jurcut@ucd.ie

Abstract: A mobile ad hoc network (MANET) is an infrastructure-less network where mobile nodes can share information through wireless links without dedicated hardware that handles the network routing. MANETs' nodes create on-the-fly connections with each other to share information, and they frequently join and leave MANET during run time. Therefore, flexibility in MANETs is needed to be able to handle variations in the number of existing network nodes. An effective routing protocol should be used to be able to route data packets within this dynamic network. Lacking centralized infrastructure in MANETs makes it harder to secure communication between network nodes, and this lack of infrastructure makes network nodes vulnerable to harmful attacks. Testbeds might be used to test MANETs under specific conditions, but researchers prefer to use simulators to obtain more flexibility and less cost during MANETs' environment setup and testing. A MANET's environment is dependent on the required scenario, and an appropriate choice of the used simulator that fulfills the researcher's needs is very important. Furthermore, researchers need to define the simulation parameters and the other parameters required by the used routing protocol. In addition, if the MANET's environment handles some conditions where malicious nodes perform network attacks, the parameters affecting the MANET from the attack perspective need to be understood. This paper collects environmental parameters that might be needed to be able to set up the required environment. To be able to evaluate the network's performance under attack, different environmental parameters that evaluate the overall performance are also collected. A survey of the literature contribution is performed based on 50 recent papers. Comparison tables and statistical charts are created to show the literature contribution and the used parameters within the scope of the collected papers of our survey. Results show that the NS-2 simulator is the most popular simulator used in MANETs.

Keywords: AODV; DSR; MANET attacks; MANET configuration parameters; MANET evaluation; MANET simulators; NS-2; OLSR

Citation: Eltahlawy, A.M.; Aslan, H.K.; Abdallah, E.G.; Elsayed, M.S.; Jurcut, A.D.; Azer, M.A. A Survey on Parameters Affecting MANET Performance. *Electronics* **2023**, *12*, 1956. https://doi.org/10.3390/electronics12091956

Academic Editor: Hamed Taherdoost

Received: 6 February 2023
Revised: 29 March 2023
Accepted: 17 April 2023
Published: 22 April 2023

1. Introduction

MANETs' nodes create on-the-fly connections with other network nodes without a need for existing infrastructure. These established connections allow all nodes to exchange information and forward packets between each other [1]. Each node contributes to the network by acting as a router that forwards data packets between the source node and the destination node [2].

Before researchers proceed with the setup and testing of a MANET environment, they should be able to select a suitable simulator. Researchers need to know the simulator's key features, and the points of strength and weakness of each simulator to select the simulator which fits the required MANET environment. In this paper, a comparison between the universally used simulators in the MANET is covered.

After selecting the simulation tool, researchers need to understand the different parameters that affect the behavior of MANETs. The efficiency of the network's performance is dependent on the defined environment parameter sets. In this paper, three main categories of parameter sets are defined as follows: (1) simulation parameters are the list of parameters related to the simulation tool where these parameters control the overall network definition, for example, simulation area, simulation time, and the mobility speed of nodes; (2) routing parameters control the routing protocol mechanism; and (3) attack parameters control the effect of malicious nodes on network performance. The performance measurements of a MANET are achieved using evaluation metrics used to evaluate the network's efficiency. In this paper, evaluation metric terms are also described. Figure 1 depicts the MANET simulation environment.

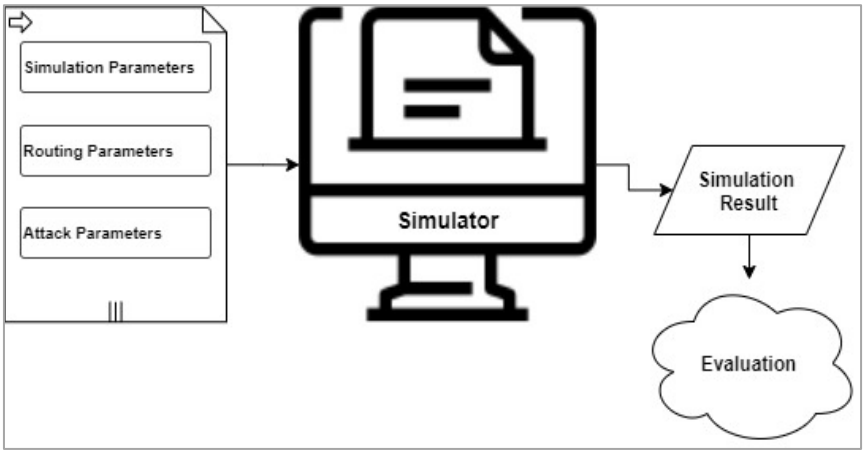

Figure 1. MANETs' simulation environment.

An abundance of the literature covered the effect of changing different environmental parameters on MANETs' performance. In this paper, a survey of 50 recent papers that cover the literature contribution is collected. The main contributions of this paper are summarized as follows:

1. The commonly used simulation tools in a MANET are described, covering the advantages and disadvantages of each. Additionally, statistics on the percentage of usage of these simulation tools are collected against 50 recent papers.
2. The list of routing protocol parameters that control the routing behavior is provided for three routing protocols. Comprehensive flowcharts for the covered routing protocols are provided. Additionally, the routing parameters' usage statistics against 50 recent papers are presented.
3. The simulation parameters used to define a MANET environment are collected, illustrating the usage of each, and statistics on the literature usage percentage of the simulation parameters are covered. The literature range of values used for each simulation parameter is also provided.
4. The main parameters that influence the MANET performance under attack are covered, a list of common attack types on a MANET is collected, and the percentage of usage is shown.
5. The evaluation metric terms used for a performance analysis of MANETs are described. Additionally, statistical tables are collected to show the used environment parameters in our survey papers.

The remainder of the paper is organized as follows. Section 2 is an introduction to different routing protocols in MANETs and their related routing parameters. In Section 3, the list of simulation tools that support MANETs is covered, as well as the simulation parameters and attack parameters that affect MANETs' performance when under attack. Section 4 covers different evaluation metrics used to analyze the network's performance.

In Section 5, the literature contribution is presented. Finally, conclusions and future work suggestions are presented in Section 6.

Table 1 summarizes the abbreviations of terminologies used in this paper.

Table 1. The list of abbreviations.

Notation	Meaning
MANETs	Mobile ad hoc networks
AODV	Ad hoc on-demand distance vector
DSR	Dynamic source routing
OLSR	Optimized link state routing protocol
RREQ	Route request
RREP	Route reply
DPC	Delete period constant
RERR	Route error
TC	Topology control
MPR	Multipoint relays
mph	Mile per hour
DB	Decibel
DDoS	Distributed denial of service
THPT	Average throughput
AETED	Average end-to-end delay time
PDR	Packet delivery ratio
PLR	Packet loss ratio
ROR	Routing overhead ratio
NRL	Normalized routing load
NL	Network load

2. Routing in MANETs

In MANETs, each node is responsible for packet forwarding on behalf of the source node, and it also initiates routing discovery mechanisms to discover its neighbors in the network, then find the best route to reach a destination node [3]. When a new node joins the network, it announces itself by broadcasting a hello message to all neighbors and starts learning about the network [4]. In addition, each node holds a routing table database to maintain a record of the current network nodes as well as the number of hops to reach each node inside the network [5]. There are a multitude of routing protocols related to MANETs' discovery and data forwarding. The three main categories for routing protocols in MANETs are as follows:

- Proactive routing protocols: For example, OLSR, each node maintains its routing table by periodically updating its information [6]; this increases network overhead. On the other hand, routes will always be available with a minimum delay. Proactive protocols provide better performance than reactive protocols as each node continuously updates its awareness of network changes. When a request is received, the packet forwarding procedure is directly handled.
- Reactive routing protocols: For example, AODV and DSR, when a source node tries to perform a packet transmission, it initiates a route discovery mechanism to know how to reach the destination. After the route is determined and updated in the routing table, the packet is forwarded [7]. Reactive protocols have minimal network overhead, but there is a delay time consumed in the route discovery.
- Hybrid routing protocols: For example, ZRP, the close local neighbors to a node are periodically updated, and the global nodes that are not direct neighbors will be updated on demand such as in reactive routing protocols [8].

This paper describes the AODV, DSR, and OLSR routing protocols and the related routing parameters for each. Figure 2 shows a simple classification of the MANETs' routing protocols.

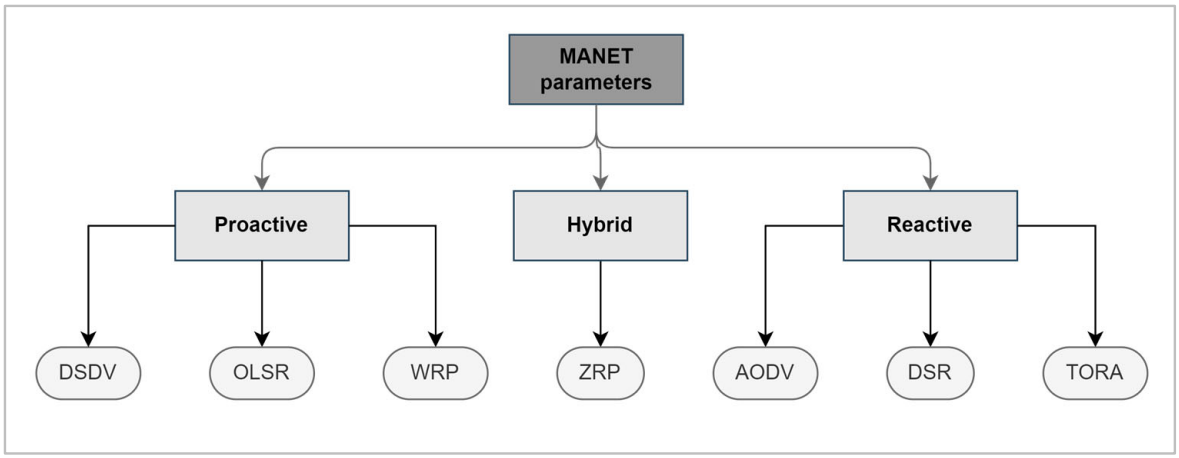

Figure 2. MANETs' routing protocols classification.

2.1. AODV Routing Protocol

AODV is a reactive routing protocol used for MANETs where mobile hosts provide a packet forwarding service acting as an intermediate node between source and destination. In AODV, each node acts as a router and their local routing tables are updated on demand when a request to forward a packet is received or the node is the packet originator [9].

To maintain connectivity between a node and its neighbors, a discovery mechanism is used. AODV discovery mechanism is used to increase the response time for new requests. The route discovery mechanism is initiated by transmitting a RREQ packet to neighbors, asking them to search for the shortest path to the destination. This mechanism increases node awareness with the smallest number of hops needed to reach the destination node. When an intermediate node receives a RREQ, it rebroadcasts the RREQ to all neighbor nodes only in case it does not have a direct connectivity link with the destination node [10].

When an intermediate node has a fresh route to the destination node and the RREQ conditions are fulfilled, the intermediate node sends a RREP in the backward direction to the source. During the forward and reverse path of RREQ and RREP packet forwarding, all intermediate nodes update their local routing table with the latest information contained in the forwarded packet [11].

Each routing table entry contains the following information fields [12]:

1. Destination node address;
2. Number of hop counts to reach the destination;
3. Intermediate nodes address;
4. Route entry expiry time;
5. Destination node sequence number.

When the source node receives the RREP packet, it can begin sending the data needed. If the source node is out of a MANET's range during the active route request, it can initiate another route discovery request with a different request identification.

To ensure that connectivity is present between neighbors, each node periodically sends a hello message. A hello message is a type of RREP packet that is used to announce the node's existence inside the network. If a node has not participated in any packet forwarding or has not sent a hello message for a specific period, the link toward this node will be considered broken. The broken node neighbors send RERR packets to their active neighbors in the network to invalidate any existing route that uses this broken node 'as an intermediate node' in data forwarding [13]. The AODV routing protocol flow chart is illustrated in Figure 3.

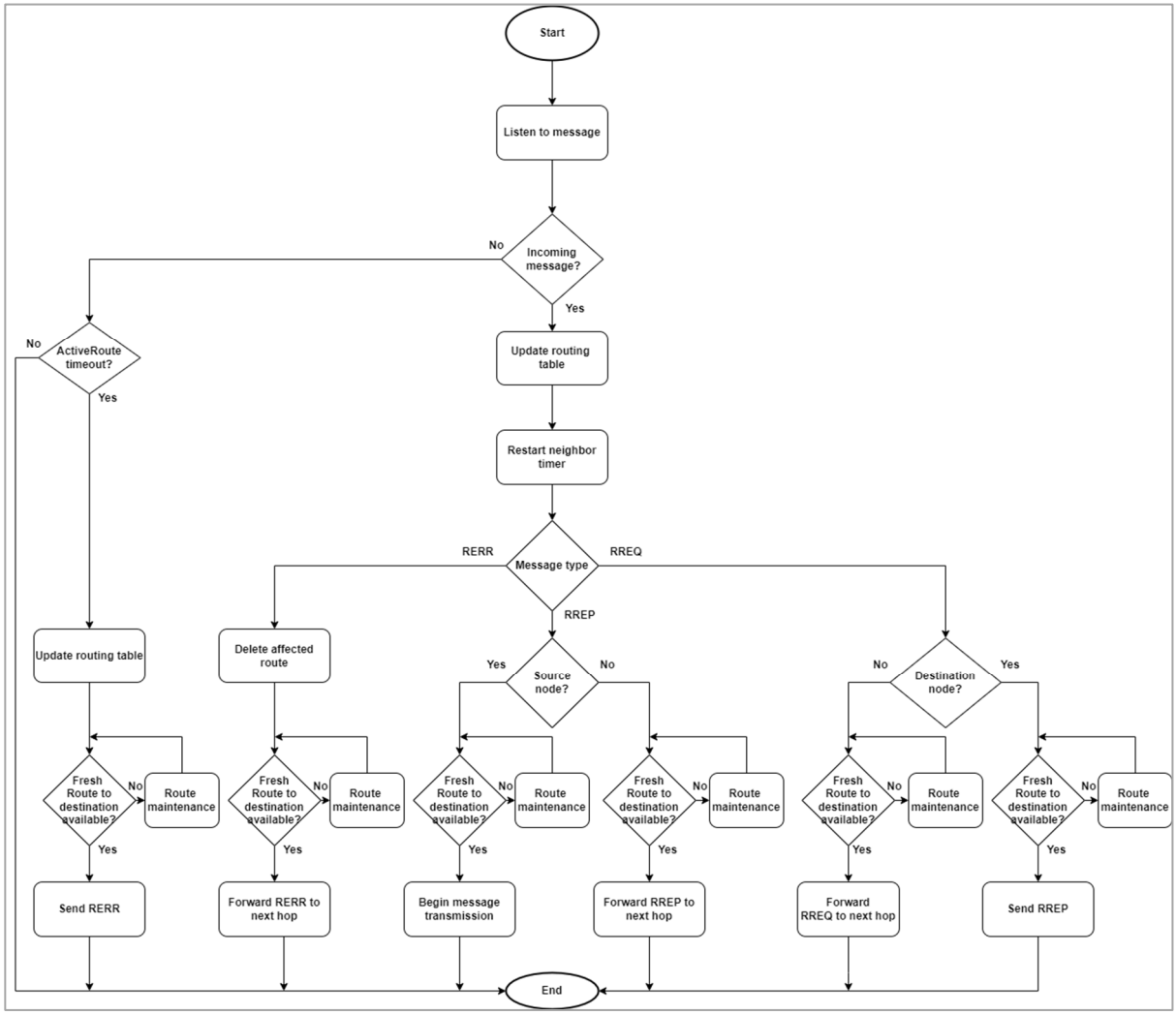

Figure 3. The AODV routing protocol flowchart.

A mobile node holds AODV configuration parameters with default values to control routing protocol operations. The main configuration parameters that affect the AODV protocol are as follows [14]:

- Network diameter: The network diameter value sets the maximum number of hop counts between two nodes in MANETs. The network diameter default value is up to thirty-five hops at most as per RFC 3561 standard.
- Node transversal time: The node transversal time is the estimation of packet transversal time between two neighbor nodes; this estimation should consider the network, processing, and transfer delay time. The default configuration time is 40 ms.
- Network transversal time: The network transversal time is the expected time between sending the RREQ packet and the reception of the RREP packet as per the equation [14]:

$$\text{NetworkTransversalTime} = 2 \times \text{NetworkDiameter} \times \text{NodeTransversalTime} \quad (1)$$

- Route request retry: If a route reply is not received by the source node within the maximum network transversal time, the source node can retry to request the route discovery again for a maximum route request retry times. If the route discovery exceeds the route request retry times, the destination node should be considered unreachable. The default value for the route request retry parameter is equal to 2 retries.
- Blacklist timeout: When the RREP transmission from node A to node B fails, node A records node B in its blacklist buffer. During this blocking time, node A discards any

RREQ from neighbor node B until the blacklist timeout is reached. After the blacklist timeout expires, node B is removed from the blacklist [14].

$$\text{BlackListTimeout} = \text{RouteRequestRetry} \times \text{NetworkTransversalTime} \quad (2)$$

- Route request rate limits: The route request rate limit is the maximum number of RREQ packets for the source node to originate per second. The route request rate limit's default value is ten packets per second.
- Active route timeout: The neighbor node is recorded in the routing table and considered an active node when the active route timeout is not exceeded. When a neighbor node is active, the recorded route to this neighbor should be used [15]. The active route timeout default value is 3000 ms.
- Hello interval: All MANET nodes should reveal their existence in the network within a hello interval time [16]. If a node does not contribute to the routing activities for a hello interval time, it should broadcast a hello message with TTL = 1. Hello interval default value is set to be 1000 ms.
- Allowed hello loss: If a node does not receive any contribution to routing activities from its direct neighbor node for more than (HelloInterval × AllowedHelloLoss), the node should assume a link failure to this neighbor [17]. The allowed hello loss default value is two link failures.
- DPC: After the delete period constant time is expired, the expired route will be deleted from the routing table [18]. The default value for DPC is 5 s.

Table 2 summarizes all AODV configuration parameters and their default values.

Table 2. AODV parameters' default values.

AODV Parameter	Default Value
NetworkDiameter	35 hops
NodeTransversalTime	40 ms
NetworkTransversalTime	1400 ms
RouteRequestRetry	2 retries
BlackListTimeout	2800 ms
RouteRequestRateLimits	10 packets/s
ActiveRouteTimeout	3000 ms
HelloInterval	1000 ms
AllowedHelloLoss	2 times
Delete Period Constant	5 s

2.2. DSR Routing Protocol

DSR is an efficient reactive routing protocol for MANETs. Each data packet contains a header that carries the IP address of all intermediate nodes between a source node and a destination node. The DSR header holds the sequence of hops to reach the destination [19].

In DSR, each node holds a cache memory to store the routing information needed for all MANET nodes; a source node can also cache multiple routes to the same destination. This mechanism allows the routing of data packets to be much more rapid in comparison to other MANETs' routing protocols. There is no need for periodic packets in DSR to minimize network overhead [20]. The DSR protocol is divided into two mechanisms: route discovery and route maintenance [21].

The route discovery mechanism is initiated when a source node does not hold the needed routing information to reach the destination node. The source node broadcasts a RREQ message to all neighbors within the source's wireless range to initiate a route discovery. The RREQ message contains the following information:

1. source node identifier;
2. destination node identifier;
3. route request identifier;
4. record listing the address of all intermediate nodes.

A route maintenance mechanism is issued when the cached route to a destination is no longer valid. When a link to the destination node is broken, the source node can try using another cached route to this destination or it can initiate a route discovery mechanism to find new routes and update the cache. Figure 4 depicts the DSR routing protocol flowchart.

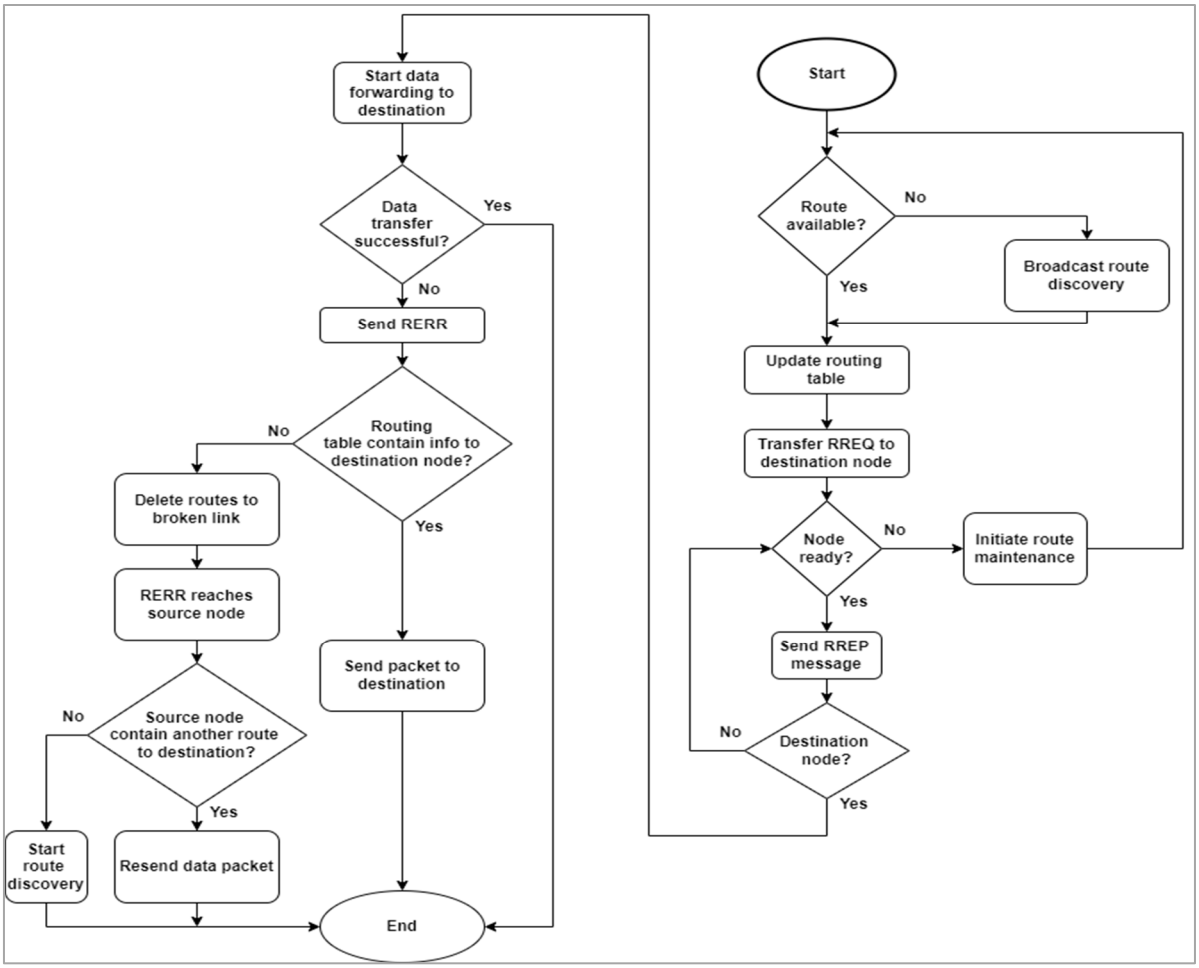

Figure 4. The DSR routing protocol flowchart.

When the destination node receives a RREQ, it examines the route back again to the source node, then it returns a RREP message that holds the accumulated record list back again to the initiator. If the examination of the reverse path to reach the source node fails, the destination node should broadcast a route discovery and then send the RREP message after updating the cached route. The DSR protocol contains a set of configuration parameters that could affect routing in MANETs as follows [22]:

- Discovery hop limit: The discovery hop limit value is defined as the limit to the route request re-broadcast. If the first attempt of RREQ does not reach the destination node, the default value of the discovery hop limit is 255 hops, and the minimum value is one hop.
- Broadcast jitter: The destination node should delay the RREP message by a random value that does not exceed the broadcast jitter's maximum delay time. The broadcast jitter default value is ten milliseconds.
- Route cache timeout: The route cache timeout is associated with each route entry in the cache [23]. When the timeout is reached, this means that the related route is not used and needs to be deleted from the node's cache. Route cache timeout default value is three hundred milliseconds.

- Send buffer timeout: When a packet cannot be transmitted to the next-hop node, this packet is queued inside a buffer to try sending it when possible. Send buffer timeout is the maximum time associated with a packet to be sent before being removed from the send buffer. The default value for send buffer timeout is 30 s.
- Max request period: After a route discovery attempt fails to find a route to the destination node, the time between successive route discovery attempts doubles until the maximum request period is reached. The default value for the maximum request period time is 10 s.
- Re-transmit buffer size: Re-transmit buffer holds the maximum number of packets waiting for the next-hop reachability confirmation. If the buffer is not sufficient to keep the new packet, this packet is discarded without notification. The re-transmit buffer size defines the buffer size with a default value of 50 packets.
- Max maintenance re-transmission: The maximum number of re-transmissions for a packet waiting for a confirmation from the next hop should be limited by the configuration value of the max maintenance re-transmission parameter. The default value is only two transmissions.

Table 3 summarizes the DSR configuration parameters with their default values.

Table 3. DSR parameters' default values.

DSR Parameter	Default Value
DiscoveryHopLimit	1 hop
BroadcastJitter	10 ms
RouteCacheTimeout	300 ms
SendBufferTimeout	30 s
MaxRequestPeriod	10 s
RetransmitBufferSize	50 packet
MaxMaintenanceRetransmit	2 times

2.3. OLSR Routing Protocol

OLSR is a proactive routing protocol that is based on the periodic exchange of control packages to maintain the network topology [24]. Routes to neighbor nodes should be available when needed. OLSR reduces the control packet data rate by only declaring a subset of the neighbors [25]. MPR nodes in most cases are neighbor nodes that are only two hops away with bidirectional links. Multipoint relays can only re-transmit the received broadcast messages, and this technique reduces the useless broadcast messages' re-transmission. Nodes that are not MPR normally process the received messages but do not re-transmit the broadcast messages in MANETs.

In OLSR, a node periodically broadcasts a hello message with all information about the node's neighbors. This hello message allows the neighbors to know the one-hop neighbors and their link state to create the neighbor's table [26]. Additionally, using the information contained in the hello messages, they learn the two hops' neighbors to form the MPR selector table.

To be able to identify the whole network topology and have better scalability, each node periodically transmits another control message (TC) along with the periodic hello messages. A TC message contains the MPR selector list of the transmitter, and this allows network nodes to create their topology table. TC messages are only sent when a node senses a change in its MPR table that needs to be advertised to other nodes with constraints on time between two consecutive TC message transmissions. After receiving a TC message, the receiver should maintain its topology table, either by creating a new entry record or by maintaining an existing node record. Figure 5 covers the OLSR routing protocol mechanism.

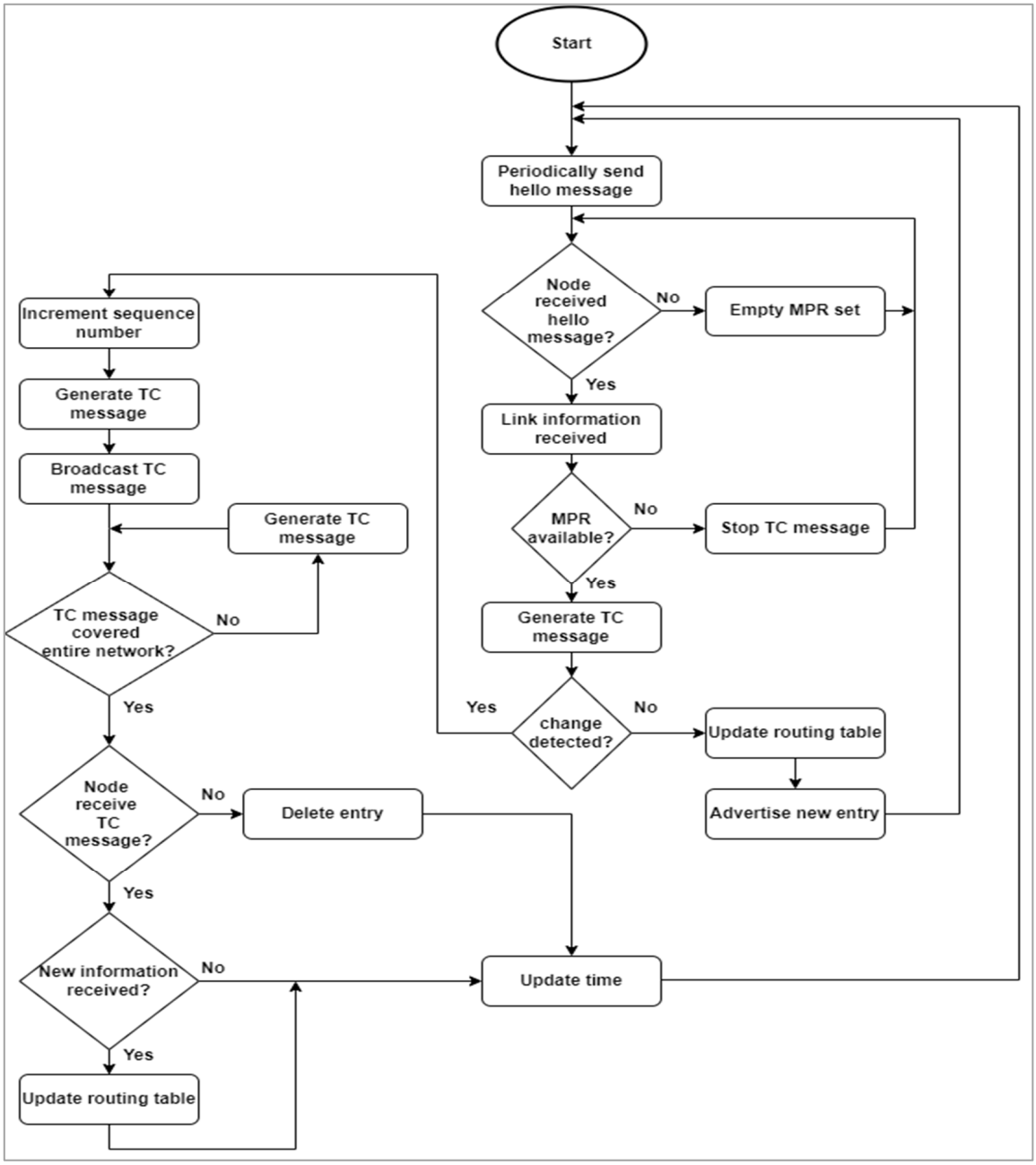

Figure 5. The OLSR routing protocol flowchart.

To be able to control the OLSR performance, some configuration parameters are used below [27]:

- Willingness: Willingness is a configuration parameter that specifies the node's willingness to forward traffic packets to other network nodes [28]. A node may change the willingness during run-time based on conditions such as resource constraints and power limitations. Willingness is an integer value with a range between 0 and 7. 'WILL_NEVER = 0' is the lowest willingness value where this node must not be selected as a MPR for any node. 'WILL_ALWAYS = 7' is the highest willingness for a node to advertise its willingness to forward traffic on behalf of other network nodes. The default willingness value for a node is 'WILL_DEFAULT = 3'.
- Hello interval: Hello interval is the set periodic time between two consecutive hello messages in seconds. The default value is 2 s.

- TC interval: This is the interval time in seconds between two consecutive topology control messages that carry the connectivity information. The TC interval default value is 5 s.
- Refresh interval: Each node must cooperate in the network by sending a periodic hello message before the refresh interval period reaches a timeout. A hello interval must be smaller than or equal to the refresh interval. The default value for the refresh interval parameter is 2 s.
- Neighbor hold time: Defines the link expiry time before declaring it as a broken link [29]. The neighbor hold time default value is 6 s.
- Topology hold time: This is the timeout for the entries in the topology table before being deleted [29]. The topology hold time default value is 15 s.

Table 4 summarizes the default values of OLSR configuration parameters.

Table 4. OLSR parameters' default values.

OLSR Parameter	Default Value
Willingness	WILL_DEFAULT (3)
TCInterval	5 s
RefreshInterval	2 s
NeighbHoldTime	6 s
TopHoldTime	15 s
HelloInterval	2 s

3. Simulation in MANETs

MANET technology is rapidly changing, and new protocols and mechanisms are continuously proposed by researchers. Evaluating a network's performance under different attacks is important to be able to propose protection mechanisms. Therefore, a cost-effective method that empowers researchers to set up and test MANETs plays an important role in research.

3.1. MANETs Simulators

Simulators are software tools used to create a virtual environment that supports researchers to set up and test a network's performance under different conditions. Simulators are GUI-driven tools used to set up a network environment and then perform different attacks on the defined network, or make comparisons between a standard routing protocol and a newly proposed protocol. Using the defined evaluation metrics, a simulator is also capable of collecting the network's results and evaluating the overall performance [30].

There is another method for developers to define and test MANETs using testbeds. Testbeds are experimentation in-lab networks that researchers can set up using dedicated hardware sets for this purpose. Testbeds lack the flexibility to define a MANET network, as MANETs are dynamic networks where nodes continuously join and leave the network. Additionally, the cost is much higher than software simulations to define a MANET using testbeds.

To be able to select a suitable simulator, the researchers need to know the simulator's key features [31]. Table 5 is a comparison between the widely used simulators in MANETs.

Table 5. Comparison between simulation tools in MANETs.

Simulator Name	Languages Supported	Platform Support	License	Advantages	Disadvantages
OPNET	C, C++	Windows, Sun Solaris, RedHat Linux	Commercial, Free Educational License	- User-friendly and easy to use. - Provides additional supportive tools.	- Limited wireless mobility. - Not open source and supported protocols are limited. - Expensive. - Lack of energy model.

Table 5. *Cont.*

Simulator Name	Languages Supported	Platform Support	License	Advantages	Disadvantages
OMNeT++	C++, NED	Windows, MacOS, and any Unix-like systems	Open source	- Used by a wide number of users. - Extensive GUI interface. - Intelligence support. - Rich C++ libraries. - Parallelly distributed simulation is supported.	- Documentation is poor. - Performance measures are weak. - Does not cover all protocols.
NS-2	C++, OTCL	Windows, MacOS, Ubuntu, Sun Solaris, Fedora Linux, and any Unix-like systems	Open source	- The most used simulator for research. - Good with complex systems' evaluation. - Provides energy model. - Supports wired and wireless networks.	- Documentation is poor. - Simulation is not real-time. - Lack of supporting tools. - Not suitable for large systems. - Difficult to use and poor GUI. - High computational overhead and memory usage.
NS-3	C++, Python	MacOS, FreeBSD, Linux	Open source	- Very fast simulator where parallel simulation is supported with real-time scheduling. - Supports emulation. - Provides debugging traces. - Organized source code with low-level abstraction. - Good documentation.	- Lacks backward compatibility with NS-2. - Virtualization support is limited. - Difficult to use.
GloMoSim	C, PERSEC	Windows XP/7, FreeBSD, Sun Solaris, Fedora Linux	Free	- Scalable and can handle very large systems with thousands of nodes. - Parallel simulation environment. - Scalable simulation library.	- Documentation is poor. - The simulator is outdated. - Does not support end devices such as simulators.
QualNet and EXATA/cyber	JAVA	Windows NT/2000/XP/Professional, macOS, Sun Solaris, and most Unix-like systems	Commercial	- Provides animation tools. - Scalable and can handle very large systems with thousands of nodes. - Support wired and wireless networks. - Realtime simulator	- Slow interfaces. - Difficult to install. - Expensive.
JIST/SWANS	JAVA, Tcl	Windows, macOS, Sun Solaris Linux	Commercial	- Powerful simulator and suitable for simulating real-world systems. - Less memory usage.	- Features not competing with other simulators.
J-SIM	JAVA	Windows, Sun Solaris Linux	Open source	- Supports wired and wireless networks. - Reusable models with good flexibility.	- Worst execution time.

3.2. Attacks on MANETs' Routing Protocols

The MANET's environment is dynamic and nodes continuously join and leave. An attacker could easily take a critical location in the network to block data packets from being delivered to the destination node. Moreover, a malicious node might produce a high-power signal that covers a wide range of network nodes to introduce itself as the best routing path to forward the packet between the source node and the destination node [32]. This malicious node would then block the data packets from being forwarded to the destination node. Such malicious activity leads to increasing the loss of important data packets, and it is reducing the network's overall throughput.

MANETs suffer from malicious activities where malicious nodes tend to impact the routing protocol mechanism. The direct impact of the attacks on routing protocols is to degrade the MANET's performance. To disrupt the MANET routing protocol, attackers tend to use several techniques such as follows:

1. Routing table overflow attack: In this attack, the attacking node tends to crowd the network by advertising several non-existing nodes to overflow the routing table [33].

This prevents legitimate nodes from being aware of network nodes and routing their packets normally.

2. Flooding attack: In a flooding attack, malicious nodes tend to waste network resources such as memory, bandwidth, and battery by flooding the network with bogus packets [34]. For example, flooding RREQ packets prevents the MANET from functioning normally.
3. DDoS attack: In a DDoS attack, attackers tend to keep the targeted legitimate node busy by continuously requesting RREQ messages from collaborative attackers at the same time without respecting the TTL time [35].
4. False removal of working route: In this attack, the malicious node advertises a false state of the link with the destination node as if the link is broken. This enforces the source node to re-initiate route discovery protocol to find another path to reach the destination. Additionally, it slows down packet transmission. False removal of working route attack could be used with another collaborative attack to isolate the targeted legitimate node from MANET.
5. Node isolation attack: Attackers isolate an innocent node by blocking routing information about this targeted node from the entire network [36]. This leads to an ignorance of the presence of this innocent node.
6. Routing table poisoning: In this attack, the attacker sends false RREQ packets with a higher sequence number to force all nodes to delete the old genuine route to a destination and update this route with a corrupted one.
7. Blackhole attack: The attacker tends to change the routing protocol packets to be the best route known for a targeted destination, and when it is requested to forward data packets to the destination node, it starts discarding the received packets to slow down the network performance [37].
8. Grayhole attack: Grayhole attack is an instance of a blackhole attack where an attacker selectively drops some data packets and normally forwards others [38], or drops all packets but only at a certain time. This makes the attack difficult to detect.
9. Wormhole attack: In a wormhole attack, two attacking nodes cooperate where one attacker at a specific location encapsulates some packets and tunnels them to the second attacker, bypassing all intermediate nodes to introduce itself as the fastest route to a destination and then drop the data packets later [39]. It can also be used to replay the received data packets in the other side of the network to disrupt the routing protocol.
10. Rushing attack: In a rushing attack, the malicious node sends RREQ messages with high-power transmission to introduce itself as the shortest path to any destination with only one hop count [40], this manipulates all network nodes to use this routing path. The rushing attack is most likely used alongside another attack such as dropping the network packets that need forwarding.

3.3. Simulation and Attack Parameters

Researchers need to understand the different parameters used to control the MANET simulation environment, as well as the parameters that affect the network's behavior under attack. The list of simulation and attack parameters is described as follows:

- Maximum simulation time (s): While running any simulator, a simulation time parameter is set to stop the simulation after this timeout is reached [41]; for more accurate results it is preferred to increase the simulation time.
- Medium packet rate (packet/s): To avoid interference and packet loss between nodes due to the wireless medium limitation, a packet rate ratio should be pre-set between all MANET nodes. This parameter depends on the road capacity (number of nodes/mile), the available frequency used for packet transfer, and the used wireless protocol (ex. IEEE 802.11) [42].
- Mobility speed of nodes (m/s): MANET nodes do not have a fixed location, which means that they are moving from one place to another at varying speeds. The speed of nodes affects the result of the simulation.

- Nodes' mobility movement pattern: The mobility pattern of mobile nodes in a MANET comprises one of the following patterns: (1) random way mobility, (2) linear mobility in a straight line, (3) circle mobility, and (4) stationary mobility for fixed nodes across the network.
- Number of intermediate nodes: Increasing the number of intermediate nodes that forward packets between source nodes and destination decreases the routing protocol performance.
- Number of source nodes: In MANETs, source nodes initiate packet transmission procedures; increasing the number of source nodes in MANET will overload the channel with more packets overhead.
- Number of malicious nodes: Increasing the number of malicious nodes in MANETs decreases overall network performance.
- Position of intermediate nodes: The position of intermediate nodes inside MANETs affects the performance. As the number of intermediate nodes between the source node and the destination node increases, network performance increases.
- Position of malicious nodes: Attackers tend to take a good physical position between source and destination nodes to be able to perform the planned attack and drop the network packets.
- Data packet payload (byte/packet): Data packet payload is the percentage of real data bytes (excluding the control and header data bytes) divided by the overall packet size in bytes. The data packet payload is an indication of the actual gain from packet transmission.
- Simulation area: Simulates the MANETs' network coverage area in m^2. The simulation area reflects on the density of nodes inside the network, which impacts the routing protocol mechanisms.
- Antenna type: The following are the antenna types and properties used for wireless communication: (1) the isotropic antenna transmits equal signal power in all directions; (2) the omnidirectional antenna transmits equal power in all horizontal directions, decreasing to zero along the vertical axis; and (3) the directional antenna transmits only in one direction at a specified angle.
- Transportation protocol type: Transport protocol is based on two types: (1) the TCP protocol is a connection-oriented protocol that requires a connection establishment between the sender and the receiver first before sending data packets. This leads to a more secure and guaranteed delivery of data packets. On the other hand, the TCP protocol slows down packet delivery due to the needed overhead of handshaking. (2) UDP is a connectionless protocol that needs no connection establishment, which is faster but less reliable for packet delivery.
- Transmission power: Each node needs to configure the transmission power that defines the range that this node could reach in one hop. Increasing transmission power leads to more coverage, but also means more energy consumption and quick battery drain.
- Mobility speed of malicious nodes: MANETs have a dynamic network structure, which means that at certain times the network consists of some nodes that could leave the network after a while. Malicious node mobility speed is a key factor in affecting network performance. The attacker could use its speed to target an innocent node and isolate it from the network by simply taking a position between this innocent node and the destination node while traveling.
- Transmission power of malicious nodes: The power of transmission for a malicious node could be valuable when the attacker aims to introduce itself as the shortest path between source and destination nodes. This malicious node can then drop the network packets later.

Figure 6 summarizes the different types of MANETs' parameters.

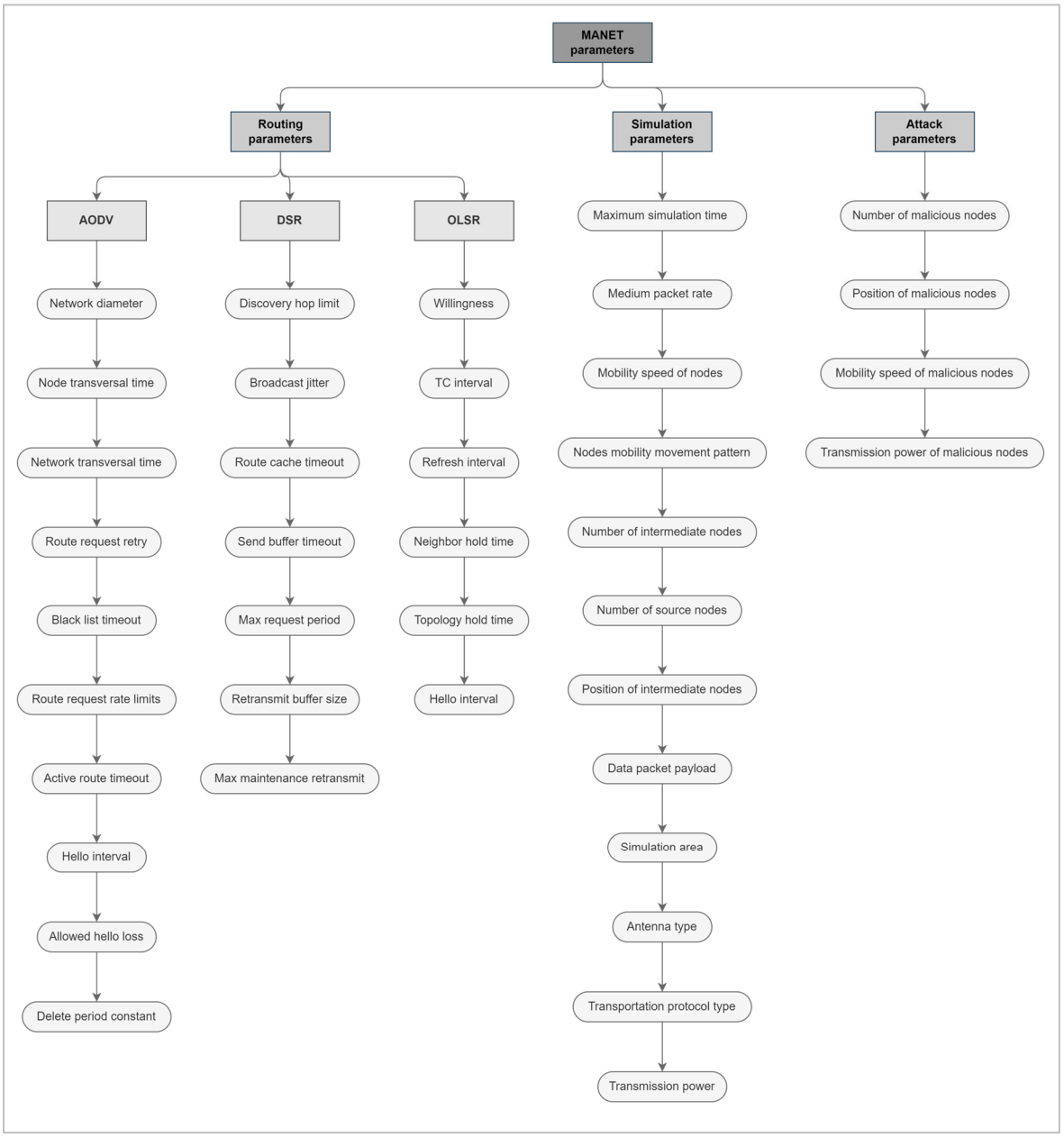

Figure 6. The different types of MANETs' parameters.

4. Evaluation Metrics and Performance Analysis in MANETs

Different evaluation metrics are used to define the characteristics of the MANET performance under certain conditions. After researchers set up the simulation environment and define the parameters needed to control the MANET environment, the results of the simulation tool need to be evaluated. To analyze the network performance, some metrics are used as follows:

- THPT: Throughput is the rate of successfully delivered packets that reached the receiver node per time slot [43]. Throughput is affected by topology changes, noise on communication links, the power of transmission from the source node, and the existence of malicious nodes affecting the throughput ratio.
- AETED: Average end-to-end delay is the average time taken to send a packet to the destination node [44]. This delay is due to many reasons such as route discovery queuing and process latency, delays caused by wireless links, and processing delays at both the sender and the receiver sides.

- PDR: Packet delivery ratio is the ratio of packets that are received by the destination across the overall transmitted packets from the source node [45]. The packet delivery ratio represents the maximum throughput that can be achieved by the MANET network.
- PLR: Packet loss ratio is the opposite of PDR; PLR measures the total lost packets that did not reach the destination node across the overall transmitted packets [46].
- ROR: Routing overhead ratio is the size of control and header packets needed by the protocol for route discovery and maintenance over the total data packets received by the destination node [47].
- NRL: Normalized routing load is the ratio between the total number of control packets sent by a source node over the total number of data packets received by a destination node [48]. An increase in normalized routing load metric indicates the efficiency of the used routing protocol.
- NL: The network load is the average amount of data packets that are being carried by the entire network over time [49]. Increasing the network load ratio increases the possibility of data collision in the wireless medium.

Figure 7 is a conclusion of the evaluation metric terms used in MANETs.

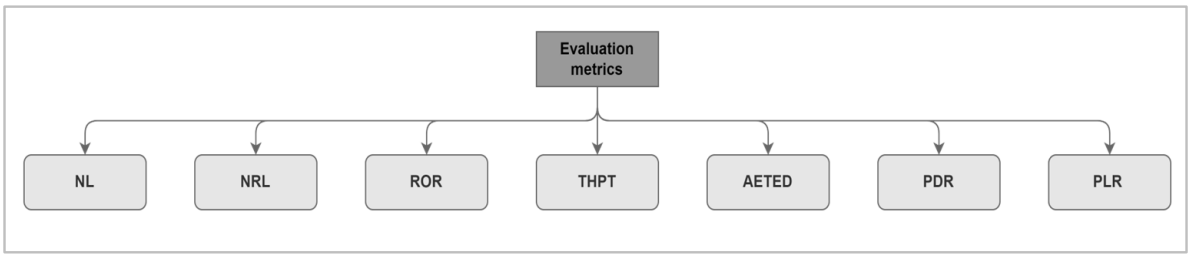

Figure 7. The different evaluation metrics used in MANETs.

5. Related Work

An abundance of the literature covered the effect of changing different environmental parameters on MANETs' performance. Statistical analyses regarding the topics covered by the researchers and the areas which require more attention in the future are performed. All selected references share in common the AODV routing protocol. AODV protocol is one of the widely used routing protocols in MANETs [49] as it has a wide range of advantages compared with other protocols. AODV is loop-free and scales to a large number of nodes, is adaptable to topology changes and responds to changes quickly, supports both unicast and multicast transmissions, has a minimal routing overhead, and has lower setup delay [50]. Some researchers conduct a performance analysis comparison between the AODV routing protocol and other routing protocols such as OLSR and DSR protocols, while other researchers focus on the performance of the AODV protocol under attack. A part of the literature contribution focuses on analyzing the effect of changing some parameters, such as mobility speed or network density, to analyze the effect of changing such parameters on the AODV protocol. Furthermore, other researchers propose enhancements to existing protocols while others propose new mechanisms for routing.

The current survey is based on 50 recent papers that share in common the AODV routing protocol. Table 6 summarizes the used routing protocol parameters within the scope of collected papers.

Out of 50 papers, only five references covered the effect of changing routing protocol parameters on the overall performance. As shown in Table 7, the percentage of the usage of routing protocols in MANETs does not exceed 6% of the literature contribution. Other routing parameters that are not mentioned in Table 6 were not used in the current survey papers. More focus and contributions are needed from the literature to address the effect of changing the routing parameters.

Table 6. Survey on routing parameter usage in MANETs.

Reference Name	Routing Protocol	Network Diameter	Node Transversal Time	RREQ Retries	Max RREQ Timeout	Active Route Timeout	Delete Period Timeout
Observation of AODV Routing Protocol's Performance at Variation in ART Value for Various Node's Mobility [15]	AODV	x	x	x	-	x	x
Impact of Active Route Time Out and Delete Period Constant on AODV Performance [18]	AODV, DSR	-	-	-	-	x	x
Comparative Performance Analysis of AODV for CBR and VBR Traffic under Influence of ART and DPC [23]	AODV	-	-	-	-	x	x
Performance Optimization of MANET Networks through Routing Protocol Analysis [51]	AODV, OLSR	-	-	x	x	-	-

(x) parameter is used, (-) parameter is not used.

Table 7. Percentage of routing parameter usage in MANETs.

Routing Parameter	Papers	Percentage of Usage
Network diameter	1 of 50	2%
Node transversal time	1 of 50	2%
RREQ retries	2 of 50	4%
Max RREQ timeout	1 of 50	2%
Active route timeout	3 of 50	6%
Delete period	3 of 50	6%
Other parameters	0 of 50	0%

Some researchers analyzed the effect of attacking the MANET routing protocol under different environments and attack scenarios. As shown in Table 8, the literature has placed more focus on blackhole and grayhole attacks. Based on a study of the most common attacks on the MANET network layer [52], the study shows that blackhole and grayhole attacks are globally introduced to affect MANETs and they also have a high impact on MANET performance. Table 8 compares the simulation and attack parameters used in the collected papers.

Table 8. Survey on simulation and attack parameters usage in MANETs.

Reference Name	Simulator	Network Area	Simulation Time	Mobility Speed (m/s)	Number of Network Nodes	Number of Malicious Nodes	Attack Type	Packet Rate (Packet/s)	Mobility Model
Performance Analysis of MANET under Grayhole Attack Using AODV Protocol [1]	NS-2	1000 m × 850 m	1200 s	-	10	1	Grayhole	-	Random waypoint
A Comparative Study of Reactive, Proactive, and Hybrid Routing Protocol in Wireless Sensor Network Under Wormhole Attack [7]	QualNet 5.0	400 m × 400 m	17 min	10	50	1, 8	Wormhole	-	Random waypoint
Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol [10]	NS-2	500 m × 500 m	100 s	-	[10–50]	[1–10]	Blackhole	-	Random waypoint
Simulation-Based Study of Blackhole Attack under AODV Protocol [12]	NS-2	500 m × 500 m	[20–100] s	0, 50	[20–100]	0–1	Blackhole	[5–25]	Random waypoint

Table 8. *Cont.*

Reference Name	Simulator	Network Area	Simulation Time	Mobility Speed (m/s)	Number of Network Nodes	Number of Malicious Nodes	Attack Type	Packet Rate (Packet/s)	Mobility Model
Blackhole Attack Detection in Vehicular Ad Hoc Network Using Secure AODV Routing Algorithm [32]	NS-2	650 m × 1000 m	100 s	-	100	1	Blackhole	-	-
Identifying the Impacts of Active and Passive Attacks on Network Layer in a Mobile Ad Hoc Network: A Simulation Perspective [33]	NS-2	-	5 s	-	10, 15, 20, 25, 30	1, 2	Blackhole, Wormhole, Grayhole	-	-
An Effective Approach to Detect and Prevent Collaborative Grayhole Attack by Malicious Node in MANET [38]	NS-3	300 m × 1500 m	200 s	-	50	0, 10	Grayhole	-	Random waypoint
Comparative Analysis of Blackhole and Rushing Attack in MANET [40]	NS-2	1000 m × 1000 m	200 s	-	50	5, 10, 15, 20	Blackhole, Rushing	-	-
VRA-AODV: Routing Protocol Detects Blackhole and Grayhole Attacks in Mobile Ad Hoc Network [43]	NS-2	3200 m × 1000 m	200 s	-	100	1	Blackhole, Grayhole	2 packets/s	Random waypoint
A Dynamic Threshold-based Algorithm for Improving Security and Performance of AODV Under Black-hole Attack in MANET [45]	NS-2	750 m × 750 m	500 s	20	10, 60	0, 1	Blackhole, Grayhole	-	Random waypoint
Defending Against Smart Grayhole Attack Within MANETs: A Reputation Based Ant Colony Optimization Approach for Secure Route Discovery in DSR Protocol [46]	NS-2	200 m × 200 m	300 s	-	-	1	Grayhole	-	Random waypoint
A Novel Approach for Mitigating Gray hole Attack in MANET [47]	NS-2	750 m × 750 m	500 s	5, 15, 25, 35	48	0, 1, 2	Grayhole	-	Random waypoint
Evaluation of Blackhole Attack with Avoidance Scheme using AODV Protocol in VANET [53]	NS-2	650 m × 650 m	1000 s	-	20	0, 1	Blackhole	-	Random waypoint, Highway, City
Entity-Centric Combined Trust (ECT) Algorithm to Detect Packet Dropping Attack in Vehicular Ad Hoc Networks (VANETs) [54]	NS-2	3000 m × 3000 m	500 s	30	[100–600]	10, 20, 30, 40, 50, 60	Blackhole	-	Highway
Blackhole Attack Prevention in MANET Using Enhanced AODV Protocol [55]	GloMoSim 2.03	1600 m × 1600 m	1 h	1, 5, 10, 20, 50	20	1	Blackhole	1, 2, 4, 6, 8 packet/s	Random waypoint
Design and Analysis of an Improved AODV Protocol for Black hole and Flooding Attack in Vehicular Ad Hoc Network (VANET) [56]	NS-2	-	-	-	3, 5, 10	1	Blackhole, Flooding	-	-
Detection and Prevention of Black Hole Attacks in Mobile Ad Hoc Networks [57]	NS-2	1000 m × 1000 m	500 s	[0–20]	50	0, 1, 2	Blackhole	-	Random waypoint
Gray Hole Attack Analysis in AODV Based Mobile Adhoc Network with Reliability Metric [58]	NS-2	7000 m × 500 m	100 s	5, 10, 15, 20, 25	50, 100, 150, 500	0, 5, 10	Grayhole	-	Random waypoint
Effect of Wormhole Attacks on MANET [59]	NS-2	1000 m × 850 m	1200 s		5, 30	0, 2	Wormhole	-	Random waypoint
An Approach to Detect Wormhole Attack in AODV based MANET [60]	NS-2	750 m × 750 m	-	-	10, 20, 50	0,1	Wormhole	-	Random waypoint
An Approach to Prevent Gray-hole Attacks on Mobile Ad Hoc Networks [61]	NS-2	750 m × 550 m	500 s	-	20, 30, 40	-	Grayhole	-	-

Table 8. *Cont.*

Reference Name	Simulator	Network Area	Simulation Time	Mobility Speed (m/s)	Number of Network Nodes	Number of Malicious Nodes	Attack Type	Packet Rate (Packet/s)	Mobility Model
A Novel Solution for Grayhole Attack in AODV Based MANETs [62]	NS-2	800 m × 800 m	50 s	20	5, 30	1, 7	Grayhole	-	-
BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map [63]	NS-2	1000 m × 500 m	200 s	20, 25	25	1	Blackhole	-	-
Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles [64]	NS-2	1000 m × 1000 m	500 s	30	50, 60, 70, 80	0, 4	Blackhole	-	-
Impact Analysis of Blackhole, Flooding, and Grayhole Attacks and Security Enhancements in Mobile Ad Hoc Networks Using SHA3 Algorithm [65]	NS-2	1200 m × 1200 m	-	30	10, 100	1, 5	Blackhole, Grayhole, Flooding	-	-
Comparative Performance Analysis of AODV and DSR Routing Protocols under Wormhole Attack in Mobile Ad Hoc Network on Different Node's Speeds [66]	QualNet 5.0	1500 m × 1500 m	300 s	10, 15, 20, 25, 30	20	2	Wormhole	-	Random waypoint
Performance Evaluation of AODV and AOMDV Routing Protocols under Collaborative Blackhole and Wormhole Attacks [67]	NS-2	1200 m × 800 m	-	-	50, 80, 100, 120	0, 1, 2	Blackhole, Wormhole	-	-
Black Hole Attacks Analysis for AODV and AOMDV Routing Performance in VANETs [68]	NS-2	1000 m × 1000 m	100 s	11, 16, 22	10	1	Blackhole	-	-
Performance Analysis of AODV and DSR Routing Protocols of MANET under Wormhole Attack and a Suggested Trust-Based Routing Algorithm for DSR [69]	EXata/Cyber 1.2	2500 m × 2500 m	300 s	-	20, 40, 60, 80, 100, 120, 140, 160, 180, 200	2, 3, 4	Wormhole	-	Random waypoint

(-) parameter is not used.

Table 8 shows a wide variety in the simulation and attack parameters used to set up the MANET environment. All research papers share in common the random waypoint mobility model. The network area for small networks was found to be 200 m × 200 m, while for extensive networks, the network area does not exceed 2500 m × 2500 m. The range of simulation time was found to be from 5 s up to 1 h, and the mobility speed range is between 0 for static nodes up to 50 m per second. Additionally, from Table 8, the number of network nodes for small networks is between 3 and 50 nodes, and for very large networks, the number of nodes reaches 600 nodes with a varying number of malicious nodes inside—the number of malicious nodes varies between 0 and 60 malicious nodes. Table 9 presents a conclusion of the ranges used in the literature for simulation and attack parameters.

Table 9. Simulation and attack parameters' range of used values in MANETs.

Parameter	Range of Used Values
Network area (m^2)	[200 × 200, 2500 × 2500]
Simulation time (s)	[5, 3600]
Mobility speed (m/s)	[0, 50]
Number of network nodes	[3, 600]
Number of malicious nodes	[0, 60]
Packet rate (packet/s)	[1, 25]

In Table 8, only 29 papers out of the 50 collected papers cover scenarios where MANETs are under attack where each researcher uses a different simulation tool and parameters to deploy the MANET environment. From Table 8, the NS-2 simulation tool is the most used tool, followed by both NS-3 and OPNET simulators. Figure 8 shows the percentage of simulation tool usage in MANETs.

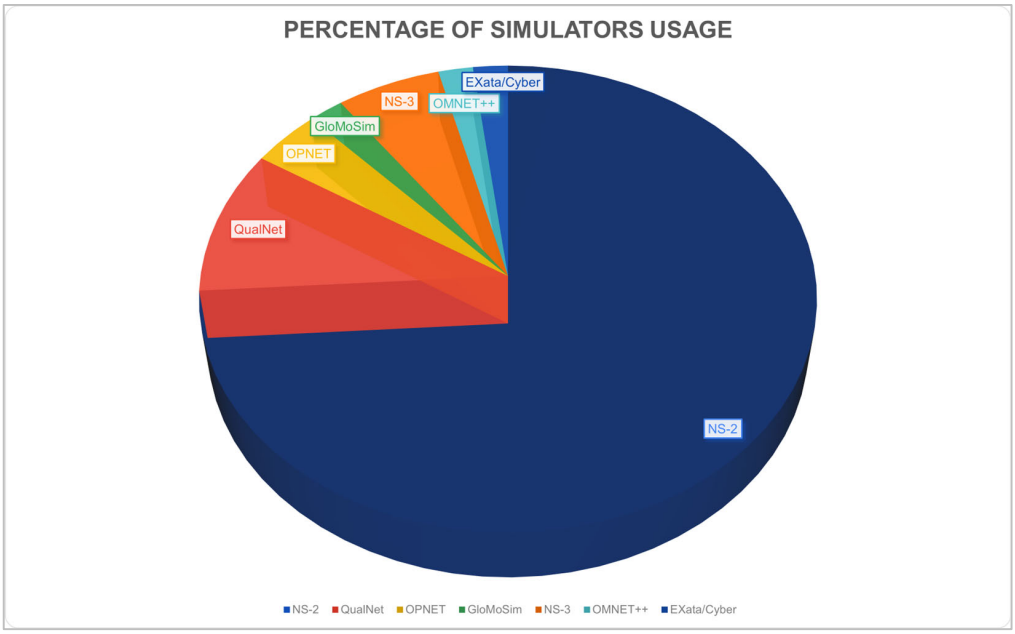

Figure 8. Percentage of simulation tool usage in MANETs.

Table 10 shows the use of evaluation metrics according to the collected papers of this survey.

Table 10. Survey on evaluation metrics use in MANETs.

Reference Name	Throughput	Average End-to-End Delay	Packet Delivery Ratio	Packet Loss Ratio	Routing Overhead Ratio	Normalized Routing Load	Network Load
Performance Analysis of MANET under Grayhole Attack Using AODV Protocol [1]	x	-	-	-	-	-	-
Performance Evaluation of AODV, OLSR, and GRP for Transmitting Video Conferencing over MANETs [2]	x	x	x	-	-	-	x
Performance Analysis of Routing Protocols AODV, OLSR, and DSDV on MANET using NS3 [3]	x	x	x	x	-	-	-
Performance Evaluation and Analysis of Proactive and Reactive MANET Protocols at Varied Speeds [4]	-	x	x	-	-	-	-
A Comparative Study of Reactive, Proactive, and Hybrid Routing Protocol in Wireless Sensor Network Under Wormhole Attack [6]	x	x	-	-	-	-	-
Performance Comparison and Evaluation of the Proactive and Reactive Routing Protocols for MANETs [7]	x	x	x	-	-	-	-
Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol [10]	x	-	x	-	-	-	-

Table 10. *Cont.*

Reference Name	Throughput	Average End-to-End Delay	Packet Delivery Ratio	Packet Loss Ratio	Routing Overhead Ratio	Normalized Routing Load	Network Load
Simulation-Based Study of Blackhole Attack under AODV Protocol [12]	x	x	x	x	x	-	-
Observation of AODV Routing Protocol's Performance at Variation in ART Value for Various Node's Mobility [15]	x	x	-	-	-	-	-
Impact of Active Route Time Out and Delete Period Constant on AODV Performance [18]	x	x	x	-	-	-	-
Survey on Performance Analysis of AODV, DSR, and DSDV in MANET [19]	x	x	x	x	-	-	-
Analysis of Routing Protocols for Ad Hoc Networks [20]	x	x	x	-	x	-	-
Comparative Performance Analysis of AODV for CBR and VBR Traffic under Influence of ART and DPC [23]	x	x	-	-	-	-	-
Performance Evaluation of OLSR and AODV Routing Protocols over Mobile Ad Hoc Networks [24]	x	x	x	x	x	-	-
Investigating the Impact of Mobility Models on MANET Routing Protocols [25]	x	x	-	-	-	-	x
Blackhole Attack Detection in Vehicular Ad Hoc Network Using Secure AODV Routing Algorithm [32]	x	-	x	-	-	-	-
Identifying the Impacts of Active and Passive Attacks on Network Layer in a Mobile Ad Hoc Network: A Simulation Perspective [33]	x	x	x	x	-	-	-
Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad Hoc Network) [34]	x	x	-	-	-	-	-
An Effective Approach to Detect and Prevent Collaborative Grayhole Attack by Malicious Node in MANET [38]	x	-	x	x	x	-	-
Comparative Analysis of Blackhole and Rushing Attack in MANET [40]	x	x	x	x	-	-	-
VRA-AODV: Routing Protocol Detects Blackhole and Grayhole Attacks in Mobile Ad Hoc Network [43]	x	-	x	-	x	-	-
A Dynamic Threshold-based Algorithm for Improving Security and Performance of AODV Under Black-hole Attack in MANET [45]	x	-	x	x	x	x	-
Defending Against Smart Grayhole Attack Within MANETs: A Reputation Based Ant Colony Optimization Approach for Secure Route Discovery in DSR Protocol [46]	x	x	x	x	-	-	-
A Novel Approach for Mitigating Grayhole Attack in MANET [47]	x	x	x	x	x	x	-
Comparative Study of Routing Protocols for Mobile Ad Hoc Networks [49]	x	x	x	x	x	x	-

Table 10. *Cont.*

Reference Name	Throughput	Average End-to-End Delay	Packet Delivery Ratio	Packet Loss Ratio	Routing Overhead Ratio	Normalized Routing Load	Network Load
Performance Optimization of MANET Networks through Routing Protocol Analysis [51]	x	x	x	x	x	-	-
Evaluation of Black Hole Attack with Avoidance Scheme Using AODV Protocol in VANET [53]	x	x	x	x	-	-	-
Entity-Centric Combined Trust (ECT) Algorithm to Detect Packet Dropping Attack in Vehicular Ad Hoc Networks (VANETs) [54]	x	x	x	x	x	-	-
Blackhole Attack Prevention in MANET Using Enhanced AODV Protocol [55]	-	x	x	-	x	-	-
Design and Analysis of an Improved AODV Protocol for Black Hole and Flooding Attack in Vehicular Ad Hoc Network (VANET) [56]	-	x	x	x	x	-	-
Detection and Prevention of Black Hole Attacks in Mobile Ad Hoc Networks [57]	x	-	-	x	x	-	-
Grayhole Attack Analysis in AODV Based Mobile Adhoc Network with Reliability Metric [58]	x	-	-	-	-	-	-
Effect of Wormhole Attacks on MANET [59]	x	-	-	-	-	-	-
An Approach to Detect Wormhole Attack in AODV based MANET [60]	-	-	x	-	-	-	-
An Approach to Prevent Gray-hole Attacks on Mobile Ad Hoc Networks [61]	x	x	x	-	-	-	-
A Novel Solution for Grayhole Attack in AODV Based MANETs [62]	-	x	x	-	-	x	-
BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map [63]	x	x	x	-	-	-	-
Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles [64]	x	x	x	x	x	-	-
Impact Analysis of Blackhole, Flooding, and Grayhole Attacks and Security Enhancements in Mobile Ad Hoc Networks Using SHA3 Algorithm [65]	x	x	x	-	-	-	-
Comparative Performance Analysis of AODV and DSR Routing Protocols under Wormhole Attack in Mobile Ad Hoc Network on Different Node's Speeds [66]	x	x	-	-	-	-	-
Performance Evaluation of AODV and AOMDV Routing Protocols under Collaborative Blackhole and Wormhole Attacks [67]	x	x	x	-	-	-	-
Black Hole Attacks Analysis for AODV and AOMDV Routing Performance in VANETs [68]	x	-	-	x	-	-	-
Performance Analysis of AODV and DSR Routing Protocols of MANET Under Wormhole Attack and a Suggested Trust-Based Routing Algorithm for DSR [69]	x	x	-	-	-	-	-

Table 10. *Cont.*

Reference Name	Throughput	Average End-to-End Delay	Packet Delivery Ratio	Packet Loss Ratio	Routing Overhead Ratio	Normalized Routing Load	Network Load
Analyzing the Impact of the Number of Nodes on the Performance of the Routing Protocols in a MANET Environment [70]	x	x	x	-	-	-	-
A Performance Study of Various Mobility Speed on AODV Routing Protocol in Homogeneous and Heterogeneous MANET [71]	x	-	x	-	-	-	-
Logistic Regression Based Reliability Analysis for Mobile Ad Hoc Network with Fixed Maximum Speed and Varying Pause Times [72]	x	-	-	-	-	-	-
A Performance Review of Intra and Inter-Group MANET Routing Protocols under Varying Speed of Nodes [73]	x	x	x	-	x	-	-
Energy Analysis of AODV Routing Protocol in MANET [74]	x	-	x	-	-	-	-
Performance Comparison of Modified AODV-ETX with AODV and AODV-ETX Routing Protocol in a MANET [75]	x	x	x	-	-	-	-

(x) parameter is used, (-) parameter is not used.

For the 50 surveyed references, throughput is the most used evaluation metric, and average end-to-end delay and packet delivery ratio are also widely used in the evaluation. Figure 9 shows the usage statistics of evaluation metrics.

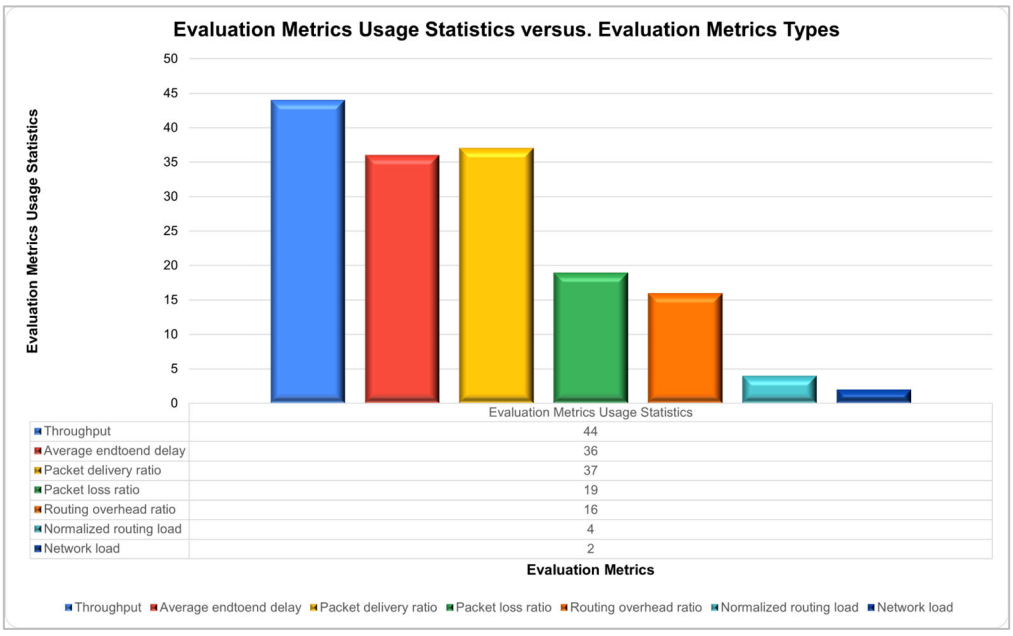

Figure 9. Percentage of evaluation metrics usage in MANETs.

Based on Table 11, a comparison is performed to show the progress made in the current survey compared to another recent survey paper [76]. After reviewing the literature contribution, in [76] is the only paper we found that covers the area of interest of the current paper. Another one of the literature contribution was found to be either outdated or partially covered the current area of interest.

Table 11. Comparison of current contribution with the literature.

	Our Survey Paper	**A Review on Parameters of Internet Gateway Discovery in MANETS [76]**
Number of papers used in the survey	50	72
Covered simulation tools	Provide simulation tool key features + Cover statistics of the following simulators: - NS-2 - NS-3 - OMNET++ - OPNET - GloMoSim - QualNet and EXATA/cyber - JIST/SWANS - J-SIM	Cover statistics of the following simulators: - NS-2 - MATLAB - OMNET++ - OPNET
Covered simulation parameters	Cover statistics of the following simulation parameters: - Simulation time - Packet rate - Mobility speed - Movement pattern/model - Number of intermediate nodes - Number of source nodes - Position of nodes - Packet payload/size - Simulation area - Antenna type - Transport protocol - Transmission power	Cover statistics of the following simulation parameters: - Mobility model - Speed of the nodes - Pause time - Packet size - Packet rate - Topology size - Number of nodes - Transmission range - Simulation time - Traffic type
Covered routing parameters	Cover the following routing protocols + All related routing parameters: - AODV - DSR - OLSR	-
Covered attack parameters	Cover attack types in MANETs + Cover the following attack parameters: - Number of malicious nodes - Position of malicious nodes - Speed of malicious nodes - Transmission power of malicious nodes	-
Covered evaluation metrics	Cover statistics of the following evaluation metrics: - THPT - PDR - PLR - AE2ED - ROR - NRL - NL	Cover statistics of the following evaluation metrics: - THPT - PDR - PDF - AE2ED - ROR - NRL

(-) parameter is not covered.

6. Conclusions and Future Work

The efficiency of packet forwarding between nodes depends on the network environment. To set up the MANET environment, researchers need to select a suitable simulator that fits the needed environment. Researchers use MANET simulation tools for different purposes, some of them conduct a performance analysis comparison between different routing protocols, whereas others check the performance of specific protocols under attack. Moreover, a part of the literature contribution analyzes the effect of changing the environment parameters on performance, and others use simulation tools to evaluate the performance of a newly introduced protocol. To be able to control MANET behavior and set up the needed environment for evaluation, researchers should be familiar with different parameters that affect the MANET environment. The efficiency of the MANET's performance is controlled by different parameters that are clustered into three group sets: (1) simulation parameters, (2) routing parameters, and (3) attack parameters.

In this paper, the key features of different simulation tools in MANETs are provided. A survey is performed against 50 recent papers to summarize the literature contribution. The list of simulation parameter values used in the surveyed papers is mentioned. Additionally, the performed statistics show that NS-2 is the most popular simulator used in the MANET. In addition, the results of this survey show that the minimum defined network area for small networks was found to be 200 m $\times$ 200 m, and for extensive networks, the network area does not exceed 2500 m $\times$ 2500 m. The range of simulation time was found to be from 5 s up to 1 h, and the mobility speed range is between 0 for static nodes up to 50 m per second. Furthermore, the number of network nodes for small networks is between 3 and 50 nodes, and for extremely large networks, the number of nodes reaches 600 nodes with a varying number of malicious nodes inside. Additionally, the statistics show that the number of malicious nodes varies between 0 and 60 malicious nodes. All parameters that control the MANET behavior are described along with a list of commonly used evaluation metrics that are used to evaluate network performance. Furthermore, the literature contribution is collected for all parameters. It is noticed that checking the effect of changing routing parameters on the network's performance is not particularly focused on in the literature.

Future work is recommended to focus on evaluating the effect of changing routing parameters on a MANET's performance. Additionally, an analysis of malicious activities on MANETs under different environments is needed. Finally, the detection and prevention of MANET attacks is an active research area of great interest to many researchers that warrants further exploration.

Author Contributions: Conceptualization, A.M.E., H.K.A., E.G.A. and M.A.A.; methodology, A.M.E., H.K.A., E.G.A. and M.A.A.; software, A.M.E.; validation, H.K.A., E.G.A. and M.A.A.; formal analysis, A.M.E.; investigation, A.M.E.; resources, A.M.E.; data curation, A.M.E., H.K.A., E.G.A., M.S.E., A.D.J. and M.A.A.; writing—original draft preparation, A.M.E.; writing—review and editing, A.M.E., H.K.A., E.G.A., M.S.E., A.D.J. and M.A.A.; visualization, A.M.E. and M.A.A.; supervision, H.K.A., E.G.A., M.S.E., A.D.J. and M.A.A.; project administration, H.K.A. and M.A.A.; funding acquisition, A.D.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not Applicable.

Conflicts of Interest: The authors declare that they have no known competing financial interest or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Reddy, B.; Dhananjaya, B. The AODV routing protocol with built-in security to counter blackhole attack in MANET. *Mater. Today Proc.* **2022**, *50*, 1152–1158. [CrossRef]
2. Ahmed, D.E.; Ibrahim, H.; Khalifa, O. Performance Evaluation of AODV, OLSR, and GRP for Transmitting Video Conferencing over MANETs. *Int. J. Comput. Sci. Inf. Secur.* **2020**, *18*, 45–51.

3. Kurniawan, A.; Kristalina, P.; Hadi, M.Z.S. Performance Analysis of Routing Protocols AODV, OLSR and DSDV on MANET using NS3. In Proceedings of the 2020 International Electronics Symposium (IES), Surabaya, Indonesia, 29–30 September 2020; pp. 199–206. [CrossRef]
4. Skaggs-Schellenberg, R.; Wang, N.; Wright, D. Performance Evaluation and Analysis of Proactive and Reactive MANET Protocols at Varied Speeds. In Proceedings of the 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0981–0985. [CrossRef]
5. Ferdous, R.; Muthukkumarasamy, V. A Comparative Performance Analysis of MANETs Routing Protocols in Trust-Based Models. In Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 15–17 December 2016; pp. 880–885. [CrossRef]
6. Govindasamy, J.; Punniakody, S. A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. *J. Electr. Syst. Inf. Technol.* **2018**, *5*, 735–744. [CrossRef]
7. Bai, Y.; Mai, Y.; Wang, N. Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs. In Proceedings of the Wireless Telecommunications Symposium (WTS), Chicago, IL, USA, 26–28 April 2017; pp. 1–5. [CrossRef]
8. Panda, N.; Patra, B.; Hota, S. Manet Routing Attacks and Their Countermeasures: A Survey. *J. Crit. Rev.* **2020**, *7*, 2777–2792. [CrossRef]
9. Saudi, N.A.M.; Arshad, M.A.; Buja, A.G.; Fadzil, A.F.A.; Saidi, R. Mobile Ad-Hoc Network (MANET) Routing Protocols: A Performance Assessment. In Proceedings of the Third International Conference on Computing, Mathematics and Statistics, Singapore, 27 March 2019; pp. 53–59. [CrossRef]
10. Shrestha, S.; Baidya, R.; Giri, B.; Thapa, A. Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol. In Proceedings of the 8th International Electrical Engineering Congress (iEECON), Chiang Mai, Thailand, 4–6 March 2020; pp. 1–4. [CrossRef]
11. Kumari, A.; Krishnan, S. Simulation-Based Study of Blackhole Attack Under AODV Protocol. In Proceedings of the Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 16–18 August 2018; pp. 1–6. [CrossRef]
12. Jubair, M.A.; Muniyandi, R.C. NS2 Simulator to Evaluate the Effective of Nodes Number and Simulation Time on the Reactive Routing Protocols in MANET. *Int. J. Appl. Eng. Res.* **2016**, *11*, 11394–11399.
13. Agrawal, R.; Tripathi, R.; Tiwari, S. Performance Evaluation and Comparison of AODV and DSR Under Adversarial Envi-ronment. In Proceedings of the International Conference on Computational Intelligence and Communication Networks, Gwalior, India, 7–9 October 2011; pp. 596–600. [CrossRef]
14. Perkins, C.; Belding-Royer, E.; Das, S. *RFC3561: Ad Hoc On-Demand Distance Vector (AODV) Routing*; IETF: Santa Barbara, CA, USA, 2003. [CrossRef]
15. Gupta, S.K.; Saket, R.K. Observation of AODV Routing Protocol's Performance at Variation in ART Value for Various Node's Mobility. In Proceedings of the First International Conference on Information and Communication Technology for Intelligent Systems: Volume 1. Smart Innovation, Systems and Technologies, Maghreb, Tunisia, 18–20 December 2018; Springer: Cham, Switzerland, 2016; Volume 50. [CrossRef]
16. Sharma, Y.; Sharma, A.; Sengupta, J. Performance evaluation of Mobile Ad hoc Network routing protocols under various se-curity attacks. In Proceedings of the International Conference on Methods and Models in Computer Science, New Delhi, India, 13–14 December 2010; pp. 117–124. [CrossRef]
17. Gupta, S.K.; Alsamhi, S.; Saket, R.K. Optimal Relation between ART and Mobility & Transmission Range at Default QualNet & Calculated Transmission Powers. In Proceedings of the 6th International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM-2016), Kuala Lumpur, Malaysia, 21–22 December 2016. [CrossRef]
18. Agrawal, N.; Fatima, M. Impact of Active Route Time Out and Delete Period Constant on AODV Performance. *Int. J. Comput. Appl.* **2016**, *147*, 19–25. [CrossRef]
19. Aggarwal, A.; Gandhi, S.; Chaubey, N. Performance analysis of aodv, dsdv and dsr in manets. *Int. J. Distrib. Parallel Syst.* **2014**, *2*, 167–177. [CrossRef]
20. Desai, R.; Patil, B.P. Analysis of routing protocols for Ad Hoc Networks. In Proceedings of the 2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), Mumbai, India, 4–5 April 2014; pp. 111–115. [CrossRef]
21. Bobade, N.P.; Mhala, N.N. Performance Evaluation of AODV and DSR On-Demand Routing Protocols with Varying MANET Size. *Int. J. Wirel. Mob. Netw.* **2012**, *4*, 183–196. [CrossRef]
22. Johnson, D.; Hu, Y. *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4*; Rice University: Houston, TX, USA, 2007; Available online: https://tools.ietf.org/html/rfc4728 (accessed on 5 February 2023).
23. Gupta, S.K.; Alsamhi, S.H.; Saket, R.K. Comparative performance analysis of AODV for CBR & VBR traffic under influence of ART & DPC. In Proceedings of the 11th International Conference on Industrial and Information Systems, Roorkee, India, 3–4 December 2016; pp. 112–117. [CrossRef]
24. Hashim, A.-A.; Farhan, M.M.; Alshybani, S. Performance Evaluation of OLSR and AODV Routing Protocols over Mobile Ad-hoc Networks. In Proceedings of the First International Conference of Intelligent Computing and Engineering, Hadhramout, Yemen, 15–16 December 2019; pp. 1–8. [CrossRef]

25. Abdullah, A.M.; Ozen, E.; Bayramoglu, H. Investigating the Impact of Mobility Models on MANET Routing Protocols. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 25–35. [CrossRef]
26. Jacquet, P.; Muhlethaler, P.; Clausen, T.; Laouiti, A.; Qayyum, A.; Viennot, L. Optimized link state routing protocol for ad hoc networks. In Proceedings of the IEEE International Multi Topic Conference: Technology for the 21st Century, IEEE INMIC 2001, Lahore, Pakistan, 30 December 2001; pp. 62–68. [CrossRef]
27. Clausen, T.; Jacquet, P.; Adjih, C.; Laouiti, A.; Minet, P.; Muhlethaler, P.; Qayyum, A.; Viennot, L. Optimized link state routing protocol (OLSR). RFC3626. *Technol. Rep.* **2003**, *1*, 1–75.
28. Boushaba, A.; Benabbou, A.; Benabbou, R.; Zahi, A.; Oumsis, M. Optimization on OLSR protocol for reducing topology control packets. In Proceedings of the International Conference on Multimedia Computing and Systems, Tangiers, Morocco, 10–12 May 2012; pp. 539–544. [CrossRef]
29. Kumar, M.; Sharma, C.; Dhiman, A.; Rangra, A.K. Performance Variation of Routing Protocols with Mobility and Scalability in MANET. In *Advances in Intelligent Systems and Computing*; Springer: Singapore, 2018; Volume 638, pp. 9–21. [CrossRef]
30. Malhotra, J. A survey on MANET simulation tools. In Proceedings of the 2014 Innovative Applications of Computational In-telligence on Power, Energy and Controls with their impact on Humanity (CIPECH), Ghaziabad, India, 28–29 November 2014; pp. 495–498. [CrossRef]
31. Dorathy, I.; Chandrasekaran, M. Simulation tools for mobile ad hoc networks: A survey. *J. Appl. Res. Technol.* **2018**, *16*, 437–445. [CrossRef]
32. Kumar, A.; Varadarajan, V.; Kumar, A.; Dadheech, P.; Choudhary, S.S.; Kumar, V.A.; Panigrahi, B.; Veluvolu, K.C. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocess. Microsyst.* **2020**, *80*, 103352. [CrossRef]
33. Ahamed, U.; Fernando, S. Identifying the Impacts of Active and Passive Attacks on Network Layer in a Mobile Ad-hoc Network: A Simulation Perspective. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 600–605. [CrossRef]
34. Fiade, A.; Triadi, A.Y.; Sulhi, A.; Masruroh, S.U.; Handayani, V.; Suseno, H.B. Performance Analysis of Black Hole Attack and Flooding Attack AODV Routing Protocol on VANET (Vehicular Ad-Hoc Network). In Proceedings of the 8th International Conference on Cyber and IT Service Management, Pangkal Pinang, Indonesia, 23–24 October 2020; pp. 1–5. [CrossRef]
35. Kaur, T.; Kumar, R. Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol. In Proceedings of the IEEE International Conference on Smart Energy Grid Engineering, Oshawa, ON, Canada, 12–15 August 2018; pp. 288–292. [CrossRef]
36. Poongodi, T.; Khan, M.S.; Patan, R.; Gandomi, A.H.; Balusamy, B. Robust Defense Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks. *IEEE Access* **2019**, *7*, 18409–18419. [CrossRef]
37. Hameed, A.; Al-Omary, A. Survey of Blackhole attack on MANET. In Proceedings of the 2nd Smart Cities Symposium, Bahrain, Bahrain, 24–26 March 2019; pp. 1–4. [CrossRef]
38. Yadav, S.; Kumar, R.; Tiwari, N.; Bajpai, A. An Effective Approach to Detect and Prevent Collaborative Grayhole Attack by Malicious Node in MANET. In *Intelligent Systems Design and Applications, Advances in Intelligent Systems and Computing*; Springer: Cham, Switzerland, 2021; Volume 1181. [CrossRef]
39. Dash, S.P. Study of Blackhole Attack and Wormhole Attack in Vanet Environment and Their Countermeasure. Master's Thesis, Michigan Technological University, Houghton, MI, USA, 2019.
40. Sivanesh, S.; Dhulipala, V.S. Comparaitive Analysis of Blackhole and Rushing Attack in MANET. In Proceedings of the In-ternational Conference on Microwave Integrated Circuits, Photonics and Wireless Networks, Tiruchirappalli, India, 22–24 May 2019; pp. 495–499. [CrossRef]
41. Chavan, A.; Kurule, D.; Dere, P. Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack. *Procedia Comput. Sci.* **2016**, *79*, 835–844. [CrossRef]
42. Cali, F.; Conti, M.; Gregori, E. IEEE 802.11 protocol: Design and performance evaluation of an adaptive backoff mechanism. *IEEE J. Sel. Areas Commun.* **2000**, *18*, 1774–1786. [CrossRef]
43. Vo, T.T.; Luong, T.N. Vra-Aodv: Routing Protocol Detects Blackhole and Grayhole Attacks in Mobile Ad hoc Network. *J. Comput.* **2018**, *13*, 222–235. [CrossRef]
44. Mai, Y.; Bai, Y.; Wang, N. Performance Comparison and Evaluation of the Routing Protocols for MANETs Using NS3. *J. Electr. Eng.* **2017**, *5*, 187–195. [CrossRef]
45. Gurung, S.; Chauhan, S. A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. *Wirel. Netw.* **2019**, *25*, 1685–1695. [CrossRef]
46. Ourouss, K.; Naja, N.; Jamali, A. Defending Against Smart Grayhole Attack Within MANETs: A Reputation-Based Ant Colony Optimization Approach for Secure Route Discovery in DSR Protocol. *Wirel. Pers. Commun.* **2021**, *116*, 207–222. [CrossRef]
47. Gurung, S.; Chauhan, S. A novel approach for mitigating gray hole attack in MANET. *Wirel. Netw.* **2018**, *24*, 565–579. [CrossRef]
48. Husieen, N.A.; Kadhum, A.N. The Effect of Pause Time on the Performance of Mobile Ad-hoc Network Routing Protocols. In Proceedings of the 4th International Conference on Intelligent Information Technology Application, Qinghuangdao, China, 5–7 November 2010.
49. El-Kabbany, A.F.; Ali, H.M.; Hussein, A.; Tawfeek, B. Comparative study of routing protocols for mobile ad hoc networks. *Int. J. Intell. Comput. Inf. Sci.* **2017**, *17*, 31–43. [CrossRef]

50. Hassnawi, L.A.; Ahmad, R.B.; Yahya, A.; Aljunid, S.A.; Elshaikh, M. Performance Analysis of Various Routing Protocols for Motorway Surveillance System Cameras' Network. *Int. J. Comput. Sci. Issues (IJCSI)* **2012**, *9*, 7.
51. Priyambodo, T.K.; Wijayanto, D.; Gitakarma, M.S. Performance Optimization of MANET Networks through Routing Protocol Analysis. *Computers* **2021**, *10*, 2. [CrossRef]
52. Mohammad, S.N. Security Attacks in MANETS (Survey Prospective). *Int. J. Eng. Adv. Technol.* **2017**, *6*, 93–96.
53. Kumar, M.; Jain, V.; Jain, A.; Bisht, U.S.; Gupta, N. Evaluation of black hole attack with avoidance scheme using AODV protocol in VANET. *J. Discret. Math. Sci. Cryptogr.* **2019**, *22*, 277–291. [CrossRef]
54. Tripathi, K.N.; Jain, G.; Yadav, A.M.; Sharma, S.C. Entity-Centric Combined Trust (ECT) Algorithm to Detect Packet Dropping Attack in Vehicular Ad Hoc Networks (VANETs). In *Next Generation Information Processing System. Advances in Intelligent Systems and Computing*; Springer: Singapore, 2021; Volume 1162. [CrossRef]
55. Alsmady, A.; Alazzam, H.; Al-Shorman, A. Blackhole attack prevention in MANET using enhanced AODV protocol. In Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems. Association for Computing Machinery, Seoul, Republic of Korea, 19–21 July 2019; pp. 1–5. [CrossRef]
56. Kumar, A.; Sinha, M. Design and analysis of an improved AODV protocol for black hole and flooding attack in vehicular ad-hoc network (VANET). *J. Discret. Math. Sci. Cryptogr.* **2019**, *22*, 453–463. [CrossRef]
57. Imran, M.; Khan, F.A.; Abbas, H.; Iftikhar, M. Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks. In *Ad-Hoc Networks and Wireless, Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 8629. [CrossRef]
58. Singh, M.M.; Mandal, J.K. Gray Hole Attack Analysis in AODV Based Mobile Adhoc Network with Reliability Metric. In Proceedings of the IEEE 4th International Conference on Computer and Communication Systems, Singapore, 23–25 February 2019; pp. 565–569. [CrossRef]
59. Jha, H.N.; Gupta, S.; Maity, D. Effect of Wormhole Attacks on MANET. In *Design Frameworks for Wireless Networks*; Lecture Notes in Networks and Systems; Springer: Singapore, 2020; Volume 82. [CrossRef]
60. Dubey, N.; Joshi, K.K. An Approach to Detect Wormhole Attack in AODV based MANET. *Int. J. Comput. Appl.* **2015**, *114*, 32–39. [CrossRef]
61. Sachan, K.; Lokhande, M. An approach to prevent Gray-hole attacks on Mobile Ad-Hoc Networks. In Proceedings of the International Conference on ICT in Business Industry & Government, Qingdao, China, 10–11 July 2017; pp. 1–6. [CrossRef]
62. Jhaveri, R.H.; Patel, S.J.; Jinwala, D.C. A Novel Solution for Grayhole Attack in AODV Based MANETs. In *Advances in Communication, Network, and Computing*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Berlin, Heidelberg, 2012; Volume 108. [CrossRef]
63. El-Semary, A.M.; Diab, H. BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map. *IEEE Access* **2019**, *7*, 95197–95211. [CrossRef]
64. Hassan, Z.; Mehmood, A.; Maple, C.; Khan, M.A.; Aldegheishem, A. Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles. *IEEE Access* **2020**, *8*, 199618–199628. [CrossRef]
65. Ramya, P.; SairamVamsi, T. Impact Analysis of Blackhole, Flooding, and Grayhole Attacks and Security Enhancements in Mobile Ad Hoc Networks Using SHA3 Algorithm. In *Microelectronics, Electromagnetics, and Telecommunications*; Lecture Notes in Electrical Engineering; Springer: Singapore, 2018; Volume 471. [CrossRef]
66. Ali, S.; Nand, P. Comparative performance analysis of AODV and DSR routing protocols under wormhole attack in mobile ad hoc network on different node's speeds. In Proceedings of the International Conference on Computing, Communication, and Automation, Greater Noida, India, 29–30 April 2016; pp. 641–644. [CrossRef]
67. Hai, T.H.; Toi, N.D.; Huh, E.N. Performance Evaluation of AODV and AOMDV Routing Protocols Under Collaborative Blackhole and Wormhole Attacks. In *Advances in Computer Science and Ubiquitous Computing*; Lecture Notes in Electrical Engineering; Springer: Singapore, 2021; Volume 715. [CrossRef]
68. Afdhal, A.; Muchallil, S.; Walidainy, H.; Yuhardian, Q. Black hole attacks analysis for AODV and AOMDV routing performance in VANETs. In Proceedings of the International Conference on Electrical Engineering and Informatics, Banda Aceh, Indonesia, 18–20 October 2017; pp. 29–34. [CrossRef]
69. Tripathi, S. Performance Analysis of AODV and DSR Routing Protocols of MANET under Wormhole Attack and a Suggested Trust Based Routing Algorithm for DSR. In Proceedings of the IEEE International WIE Conference on Electrical and Computer Engineering, Bangalore, India, 15–16 November 2019; pp. 1–5. [CrossRef]
70. Haglan, H.M.; Mostafa, S.A.; Safar, N.Z.M.; Mustapha, A.; Saringatb, M.Z.; AlHakami, H.; AlHakami, W. Analyzing the impact of the number of nodes on the performance of the routing protocols in manet environment. *Bull. Electr. Eng. Inform.* **2021**, *10*, 434–440. [CrossRef]
71. Ismail, Z.; Hassan, R. A performance study of various mobility speed on AODV routing protocol in homogeneous and heterogeneous MANET. In Proceedings of the 17th Asia Pacific Conference on Communications, Sabah, Malaysia, 2–5 October 2011; pp. 637–642. [CrossRef]
72. Singh, M.M.; Mandal, J.K. Logistic Regression Based Reliability Analysis for Mobile Ad Hoc Network with Fixed Maximum Speed and Varying Pause Times. *J. Sci. Ind. Res.* **2017**, *76*, 81–84.
73. Sisodia, D.S.; Singhal, R.; Khandal, V. A Performance Review of Intra and Inter-Group MANET Routing Protocols under Varying Speed of Nodes. *Int. J. Electr. Comput. Eng.* **2017**, *7*, 2721–2730. [CrossRef]

74. Mafirabadza, C.; Khatri, P. Energy analysis of AODV routing protocol in MANET. In Proceedings of the International Con-ference on Communication and Signal Processing, Tamilnadu, India, 6–8 April 2016; pp. 1125–1129. [CrossRef]
75. Purnomo, A.; Najib, W.; Hartono, R. Performance Comparison of Modified AODV-ETX with AODV and AODV-ETX Routing Protocol in an MANET. *IOP Conf. Ser. Mater. Sci. Eng.* **2019**, *578*, 012082. [CrossRef]
76. Osman, H.; Ebedon, M.M.; Saad, A. A Review on Parameters of Internet Gateway Discovery in MANETS. *Int. J. Online Biomed. Eng. (iJOE)* **2021**, *17*, 38–59. [CrossRef]