ISSN: 0974-5823 Vol. 7 No. 2 February, 2022

International Journal of Mechanical Engineering

MANET Routing Protocols, Attacks and Mitigation Techniques: A Review

Tawseef Ahmad Teli[1], Rameez Yousuf[2], Dawood Ashraf Khan[3]

[1]Department of Computer Applications, Cluster University Srinagar

[2,3]Department of Computer Sciences, University of Kashmir, J&K India

Abstract **–** In Mobile Ad-hoc Networks (MANETs) the nodes move around freely in any possible direction and as such, the reorganization of the network structure happens on the fly. MANETs have applications in many areas such as emergency, search and rescue operations, battlefields, and video conferencing. In MANETs there is no central authority that will control the operations such as adding a node to the network or checking its behaviour; rather these operations are performed by the peer nodes in a decentralized manner in the MANETs. Routing within MANETs is an important activity performed by the mobile nodes. Routing in MANETs is difficult since the nodes can leave or join the network at will; the routing protocols need to adapt to the changes that occur in the network because of the topological changes. In this research work, we discuss different MANET routing protocols, then several possible routing protocol attacks, and finally the techniques to mitigate these attacks. Comparison based on Route Structure, Multiple Routes, Routes maintained, Loop Freedom, Number of tables required, and Hello messages are also given for the different routing protocols in MANETs.

Index Terms - Mobile ad hoc network, routing attacks, routing protocol, route structure.

1. Introduction:

Wireless networks use wireless links to connect the communicating devices and eliminate the need for wired connections. Wireless networks are of two types namely infrastructure-based wireless networks and infrastructure-less wireless networks. In the infrastructure-based wireless networks, dedicated gateways and routers are employed to route the packets from the source to the destination. An example of this type of network is the cellular phone network. The infrastructure-less networks, Mobile Ad hoc Networks (MANETs) are decentralized and self-organized networks created on the fly and the nodes use wireless connections to connect. The nodes can join or leave the network as and when they want, thereby making the network topology dynamic. Without central control, the communication is governed by peer nodes, unlike the cellular networks. Each node in a MANET has the responsibility of being a host as well as a router to forward the packets. The packets are routed from the source to the destination in a multi-hop fashion. Due to the movement of the nodes in the network, the routing path changes frequently causing packet drops which finally result in low packet delivery. MANETs have vast applications because they come with the advantages of easy deployment and being cost-effective. As wireless communication has gained popularity over the years, portable devices like laptops, cellular phones, PDAs, and other wireless devices with Ad-hoc networking capability are used in various areas such as emergency and rescue operations, tactical operations, gaming and entertainment, patient monitoring, sensor networks, intelligent transport systems, smart cars, smart homes, video conferencing, radar systems and other applications. In MANETs, nodes have limited capabilities such as processing power and speed, battery, transmission power, storage and are characterized by unreliable links [1,38]. Further, the MANETs are characterized by a lack of centralized control, insecure and unreliable transmission links, and dynamic topology.

This paper presents an overview of different routing protocols such as AODV, DSR, DSDV, ZRP, and other protocols in MANETs and highlights their advantages, disadvantages, and their scope of utilization. Further, the various attacks to which MANETs are susceptible are discussed. Lastly, this paper highlights the mitigation techniques employed to mitigate such attacks and addresses the research gaps which need to be addressed in MANETs.

The rest of this paper is organized as follows: Section 2 discusses routing protocols for MANETs. Section 3 discusses popular routing attacks in MANETs. Lastly, the mitigation of the attacks is covered in section 4. The conclusion of this paper is presented in section 5.

2. Routing Protocols

A protocol is a set of rules that govern the transmission of data between two or more entities in a network. Designing protocols in MANETs is one of the most challenging tasks due to the limited resources in MANETs and dynamically changing topology and has gained attention from researchers from the last decade [1-3]. Since MANETs lack dedicated routers, the whole process of routing is done by peer nodes that form the network. While designing the routing protocols for MANETs, the augmentation of throughput and the reduction in losing packets is of significant consideration [5]. The protocols for MANETs are broadly divided into three main categories as shown in Figure 1.

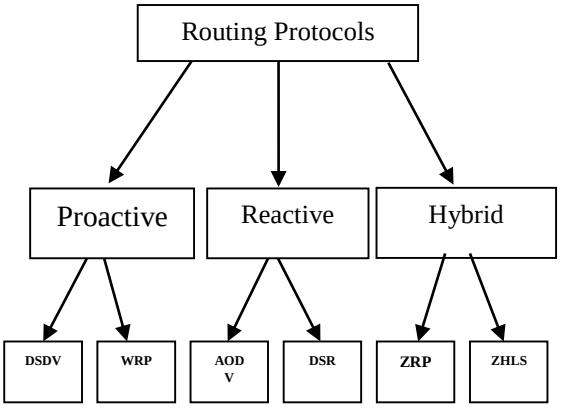

Figure 1. Routing Protocols in MANETs

2.1 Proactive protocols

Proactive protocols, for example, Destination Sequenced Distance Vector (DSDV) and Wireless Routing Protocol (WRP), are also referred to as table-driven protocols that are based on link-state algorithms [39], maintain routing information by a periodic update of topology information or trigger from the neighbouring nodes as the configuration of tables. Different types of proactive protocols are differentiated on the total count of routing tables, the specific type of routing information these maintain, and how the updates take place in these protocols [1,2,4,6]. The advantage of these protocols is in the sense that the path to the destination is readily available which results in less routing overhead and less resource consumption is also less.

Further, these protocols are fit to guarantee better QoS and real-time communications. However, these protocols underutilize bandwidth and the routing overhead is overwhelming [6]. The network is flooded when periodic updates take place to maintain the information in the routing tables.

2.1.1 Destination Sequenced Distance Vector

Bellman-Ford routing mechanism is implemented in Destination Sequenced Distance Vector(DSDV) proactive routing protocol [29] with flat routing structure requiring only two routing tables and guarantees loop freedom which would otherwise make the packets move along the same path in a repeated fashion and thereby will consume the resources in the network. The overheads in terms of memory or control are both O(N) [1, 7]. It maintains routing information containing next hop fields and target sequence numbers originated by the target node. Routes are assigned target sequence numbers while the next hop determines the final target or in-between nodes. In case there are multiple paths found to the target node, the route having assigned the highest target sequence number is selected as the path to be the carrier of the data packets. The nature of these protocols calls for route updates which are in the form of “full dump” and “incremental” packets. With the full dump update mechanism, it updates the new routing information as well as the information that is already available. It requires several network protocol data units (NPDUs). With the incremental update, the only information about routing that has been modified since the last update is updated and this approach is used more often. However, there is a scalability issue with this routing protocol when applied to large networks as a huge amount of bandwidth is used for updating purposes and also because there is a large overhead due to the periodic update requirements [7,8].

2.1.2 Wireless Routing Protocol

Wireless Routing Protocol (WRP) is another proactive type of routing protocol with a flat routing structure and is free from loops. This protocol makes use of four routing tables; a table for distances, a routing table, the cost of links table, and the list of the messages that are retransmitted also known as Message Retransmission List (MRL). The memory overhead and control overhead are $O(N^2) and\ O(N)$ respectively. It ensures the existence of neighbouring nodes by receiving the acknowledgements and other messages. Upon the failure to receive an acknowledgement within a stipulated time frame from its neighbour, it is established that the node retired from the network or the node is dead. The hello messages are required to discover new nodes. When a new node broadcasts this message and is received by the other nodes, these nodes share their routing tables and the routing tables are updated. It is also important to mention that this particular protocol ignores the count-to-infinity problem [7]. Moreover, the hello messages increase the power and bandwidth consumption in the protocol.

2.2 Source initiated protocols

Whenever there is a need for the start node to communicate with the target node, reactive types of protocols which are also referred to as on-demand protocols initiate the route discovery phase. This kind of routing reduces the overall overhead which occurs in the case of proactive routing protocols. Two control packets; a route request (RREQ) packet and a route reply (RREP) packet are required for the route discovery and the establishment of the link between start and target. During the communication between the source and target nodes, the source sends RREQ packets by flooding the network, and the reply from the intermediary nodes is sent back in the form of an RREP packet. The transmission of the data begins when there is the establishment of the path containing the

start and the target nodes. These types of routing protocols offer the advantage of not storing the information about the whole network; instead, the nodes store only the information of active routes [7, 8]. Examples include AODV, DSR.

2.2.1 Ad hoc On-demand Distance Vector

AODV is reactive with a flat structure and is an amalgam of two protocols; DSDV and DSR. It makes the use of the target's sequence number, hop-by-hop routing, and periodic beaconing in the form of *hello* messages which are employed in DSDV, and the route discovery and maintenance scheme used in DSR [7, 8].

During the communication between the start and target node, the start node broadcasts *route-request-packet* (RREQ) in the whole network to discover the path to the target node. When an intermediary node has a path to the target it creates a reply containing the *route-reply-packet* (RREP) which contains a path to the target node. The transmission of the data then begins from the start node to the target node via the intermediary nodes that come along the path to the destination node.

The maintenance of route is employed with the help of *hello* messages which are transmitted by nodes ensuring the neighbouring nodes that are still active. The failure to broadcast these messages makes the neighbouring nodes believe that the nodes are down or are unreachable. The adaptation of AODV to highly dynamic networks come as an advantage. However, the use of beacon messages and reroute discovery in case of link failures waste high bandwidth and power usage.

2.2.2 Dynamic Source Routing

Another reactive protocol is DSR with a flat structure and requires source routing that makes every packet maintain the complete address of intermediate nodes through which it must travel to be able to reach from the start to the target. The route caches are first checked to examine whether there exists a valid route to the target, if one such route is found then the route discovery is not initiated; otherwise like in the case of AODV, the route discovery mechanism begins. Unlike AODV, DSR stores multiple paths in route cache and chooses the alternate one in case of failure of a route [1,7,8].

The advantage of DSR is that it does not use beacon messages to discover neighbours so a fair amount of bandwidth is saved and also the energy is conserved. However, DSR has a scalability problem with larger mesh networks with the increase in overhead per packet.

2.3 Hybrid Protocols

Combining the precedence of proactive with on-demand protocols, hybrid protocols are more popular and have gained a lot of attention from researchers. Examples include ZRP and ZHLS.

2.3.1 Zone Routing Protocol

This hybrid routing protocol, ZRP, is flat structured and uses beacon messages in the neighbour discovery process. It uses the concept of zones that overlap each other. Inside a zone, it uses an intra zone routing mechanism. which is proactive. Outside the zone, it employs an inter-zone routing mechanism that uses a reactive approach. The zones in ZRP [30] are expressed by zone radius Ƥ which defines the number of nodes to which a node can directly communicate and is set by the transmission range of a node.

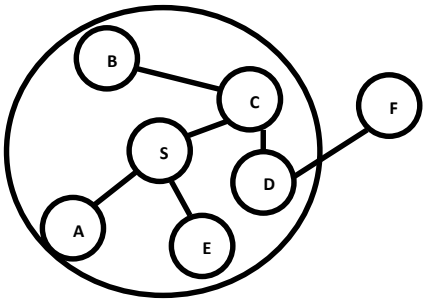

Figure 2. ZRP

The nodes which are within the zone radius are termed interior nodes and the peripheral nodes lie at a hop count of zone radius. Consider the node S in Figure 2. Suppose the zone radius is 2. Then the nodes A, E, and C are interior nodes, and nodes B and D are peripheral nodes. Whenever node S begins the communication with nodes that are inside its zone it uses the information that is already available proactively. For the nodes which are lying beyond the zone radius, the protocol switches to the reactive approach. The node S will forward an RREQ packet to the end nodes or peripheral nodes denoted by B and D. These nodes will in turn lookup

their routing tables and in this case node D finds node F in its routing tables node D replies with RREP and now node S communicate directly with node F through node D. The advantage of ZRP is that it reduces control overhead during route discovery as it sends the RREQ packets only to the peripheral nodes. Further, it employs the concept of border casting rather than flooding in which the nodes that are already queried previously are not queried again. However, the disadvantage of ZRP is that if the zone radius is increased it will behave proactively and as a result, more bandwidth and energy will be utilized. If the zone radius is decreased, ZRP will behave like a reactive protocol and will need to send RREQ packets more often [1, 9].

2.3.2 ZHLS (Zone-based Hierarchical Link State)

ZHLS employs a hierarchical strategy as compared to ZRP which uses a flat routing structure. Unlike ZRP, ZHLS does not use beacon messages to discover neighbours. There are non-overlapping zones in ZHLS in which nodes are identified by node IDs and zone by zone IDs by using GPS. Whenever a node in one zone has to communicate with a node that is in another zone, it sends a request for a route to other zones rather than flooding and thereby reducing the network traffic. Table 1 compares the routing protocols discussed above.

2.4 Comparative analysis

The comparison of the different routing protocols in MANETs is given in table 1. Protocols such as DSDV, WRP, AODV, DSR, ZRP, and ZHLS are compared based on their routing table structure, several tables required for each protocol, loop freedom, how routing information is stored, and the use of *Hello* messages. DSDV uses a flat routing structure and uses sequence numbers to identify whether a given route is stale or fresh. It uses 2 routing tables to maintain the routing information. It uses Hello messages to discover its neighbours. The use of sequence numbers further avoids the creation of routing loops. The packets are transferred through only one path; so there are no multiple paths for transferring the data from the source to the destination. WRP uses a flat route structure and uses 4 routing tables to maintain the routing information. There is only one path from the source to the destination which is a problem in case the only one selected path becomes congested which can result in high latency. It further uses Hello messages to discover its neighbours periodically. This protocol is free from loops and avoids the “count-to-infinity” problem.

Table 1. Comparison of different routing protocols

Protocol	Route Structure	Multiple Routes	Routes maintained	Loop Freedom	Number of tables required	Hello messages
DSDV	Flat	No	Routing table	Yes	2	Yes
WRP	Flat	No	Routing table	Yes	4	
AODV	Flat	No	Routing table	Yes	-	Yes
DSR	Flat	Yes	Route Cache	Yes	-	Yes
ZRP	Flat	No	Intra and inter zone tables	Yes	-	Yes
ZHLS	Hierarchical	Yes	Intra and inter zone tables	Yes	-	No

AODV maintains routing tables only as far as they are needed by the source node to reach the destination and uses a flat routing structure. It guarantees loop freedom and avoids the “count-to-infinity” problem. It also uses Hello messages to discover neighbours and detect link failures and breaks. The source node uses the route reply packet with the highest destination sequence number to select the path and avoids the rest of the replies; so, there is only one path in use for sending the packets from the source to the destination.

DSR uses a route cache to maintain the routing information and uses a flat structure for storing routing information. Multiple paths are available from the source to the destination node which reduces the network congestion. This routing protocol does not create any loops and further reduces the control overhead in the network. ZRP has also employed a flat routing structure in maintaining the routing information in the form of routing tables. It uses two routing tables: Intra routing and inter routing.

The routing information that is within the zone of a node is stored in the intra routing table while the inter routing table stores the information about the nodes which are outside the zone of a node. There are no multiple paths available for the nodes. İt uses *hello* messages to discover its neighbours.

ZHLS uses a hierarchical routing structure to store the routing information in the form of inter and intra zone tables. There are multiple paths available from the source to the destination node. It does not use *hello* messages for the discovery of neighbour nodes and rather uses Node L SPs and Zone L SPs packets for discovering the nodes. This protocol is free from loops.

3. MANETs Routing Attacks

MANETs are prone to several attacks, Figure. 3, such as external and internal attacks because of the absenteeism of a central authority and also the links are susceptible to attacks. Internal attacks are more destructive as these can drop and modify data packets and are carried out by the nodes which are a segment of the network; therefore, these are subtle in comparison with external attacks

which eavesdrop on the communication [11]. In this paper, we explain several attacks in MANETs such as:

- Blackhole Attack (Sinkhole)
- Wormhole Attack
- Greyhole Attack
- Byzantine Attack

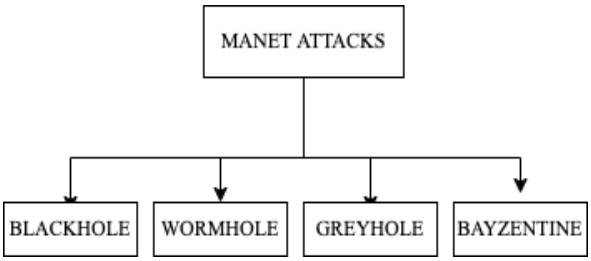

Figure 3. Types of Attacks in MANETs

3.1 Blackhole Attack

Blackhole is the most prominent type of attack in MANETs and is carried out by either one malicious node or a combination of cooperating malicious nodes [31]. During the exchange of packets between the start and target node, a *route-request-packet* is forwarded by the start node to its vicinity nodes. These nodes then forward the *RREQ packets* to all the nodes in their vicinity; the whole procedure is looped till the target node is discovered [32]. Once the target node is found, a *route-reply-packet* that has the complete route information from the start to the target is sent to the start node. If more than one *route-reply-packets* arrive at the start node, the start node selects the *route-reply-packet* which arrived at it first and discards the other *route-reply-packets* [33]. The start node then initiates the process of forwarding the data packets along with the nodes that are contained in the *route-reply packet*.

In a blackhole attack, a malicious node forwards a fake *route-reply-packet* claiming the shortest path (fewer hops) to the target node whenever the start node forwards an *RREQ packet***.** The malicious node can also generate a fake destination sequence number [14] which represents the freshness of a path and makes the start node believe that a path goes through it to reach the target node. The start node selects this node as an intermediary node and initiates the process of forwarding data packets to this node; this node being malicious then drops these data packets or sends these to another malicious node [12-14].

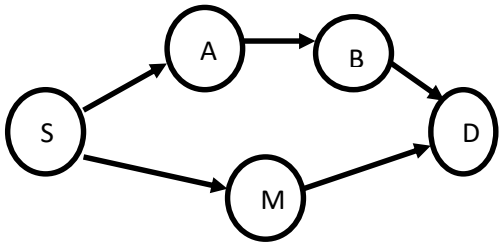

Figure 4. Blackhole attack

The blackhole attack is illustrated in Figure. 4. Node S wished to communicate with node D. So, a *route-request-packet is sent* to both the nodes A and M. Node A sends the *route-request-packet* to node B which in turn finds that it has the path to node D. So, node B creates a *route-reply-packet* that contains the route to the target with the information that the hop count is 3 and the higher destination sequence number. However, before this reply could reach the start node S, node M being malicious sends the *route-reply-packet* containing the information that through this node the hop count is 2 and any random sequence number that is larger than the previous sequence number. Node S in turn selects this node M and starts to forward data packets along with this. Node M begins to show its malicious behaviour and drops the data packets. In this way, the black hole attack is executed.

3.2 Wormhole Attack

In a wormhole attack, the malicious nodes use a private high-speed network to get a chance to be included in the path as an intermediary node from the start to the target. The use of a private high-speed network makes the *route-request-packets* reach the destination quicker [34]; also, the *route-reply-packets* are sent to the start node in a shorter period as compared to the other paths. Once the path on which these malicious nodes lie is selected, these nodes launch the attack by dropping the data packets and also compromising the security and confidentiality of the data [15]. An example is given in Figure. 5, below.

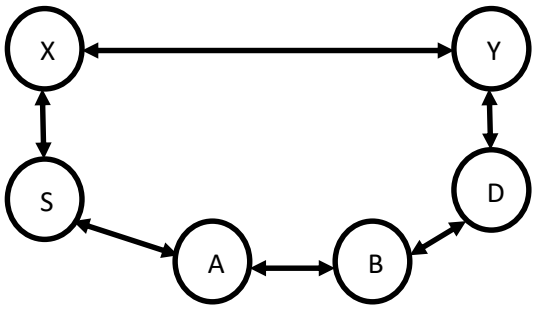

Figure 5. Wormhole attack

In Figure. 5, the start node S wished to communicate with the target node D and sends a *route-request-packet* to all the nodes in its vicinity; nodes A and X. Node A forwards this request to node B and node B has a path to the target node. So, node B forwards a *route-reply-packet* on a backward path to node S. But before it could reach node S, a *route-reply-packet is* forwarded by node Y via node X using the high-speed network reaches the start node. So, node S will select this reply which contains the path S-X-Y-D instead of S-A-B-D. Once the path S-X-Y-D is selected, nodes X and Y will drop the data packets thereby significantly decreasing the throughput.

3.3 Greyhole Attack

Greyhole attack is a hard type of attack to identify as the malicious nodes drop packets selectively; the malicious nodes forward the control packets genuinely while dropping the data packets later in the show [16]. These nodes help in finding the route to the destination node and later on carry away the attacks such as packet dropping. We illustrate this type of attack on the AODV routing protocol. Fig. 6, below shows this type of attack.

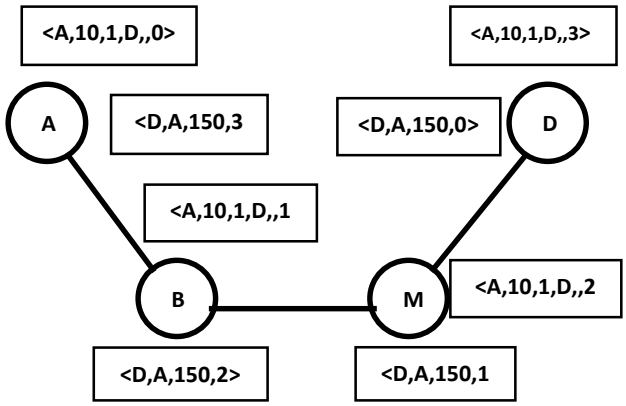

Figure 6: Grey Hole Attack

AODV routing protocol uses *route-request-packet* (RREQ) and *route-reply-packet* (RREP) to discover and establish the path respectively from the start node to the target node. Each node has the responsibility or maintains a couple of counters; a sequence number counter and a brd_id (broadcast) counter which increments whenever the start node issues a new RREQ. The RREQ has the following format:

<*src_add*, *src_seq_no*, brd_*id*, *target_add*, *target_seq_nno*, *hop_counter*>

The RREP has the following format:

<src_adr, target_addr, target_seq_no, hop_counter>

In Fig.6., the start node A wishes to communicate with the target node D, so it broadcasts an RREQ packet that contains:

<A, 10, 1, D, , 0>

where A is the start address, 10 is the *src_seq_no*, 1 is the *brd_id* , 0 is the *hop_ counter* is the total count of hops from the originator of the packet to the current node. Since there is no information about the destination at the beginning, the *target_no* field is left blank. This packet is received by node B which contains the information <A,10,1,D, ,0> and node B updates this information to <A, 10, 1, D, ,1>. Since node C do not have any information about node D, so it broadcast this packet further to node M. Presently, node M does not show any malicious behaviour so it receives the packet <A, 10, 1, D, ,1> and updates it to <A, 10, 1, D, 2> and sends the updated packet to node D. Node D, after receiving this packet understands that node A wishes to forward packets to it. So node D creates a route-reply-packet (RREP) which contains the information <D, A, 150, 0>. Node M receives this RREP from node E and updates it to <D, A, 150, 1>. Then node M forwards this packet to node B which updates it to <D, A, 150, 2> and finally this packet is forwarded to node A and contains information <D, A, 150, 3>. Now node A knows that the hop count is 3 and the target sequence number which represents the newness of the path is 3.

So, node A now begins to forward the data to node B which then sends the packets to node M. At this point, node M begins to show its malicious behaviour and begins to discard the data selectively. In this way, the greyhole attack is executed by malicious node M.

3.4 Byzantine Attack

Byzantine is the type of attack that is executed by a few nodes in the network that have been compromised, which were once the legitimate nodes [35-37]; these are also referred to as insider attacks. The adversary nodes can selectively drop the data packets, modify hop count or ids of packets, and can also create routing loops and can decrease the network performance by forwarding the data packets over the non-optimal routes which may produce traffic congestion and higher resource consumption in the network. These malicious nodes are very difficult to identify and prevent [17, 18].

4. Mitigation of MANET Routing Attacks

Routing attacks in MANETs is a serious problem that results in packet loss, high latency, and bandwidth underutilization in the network. So, it becomes necessary to mitigate such attacks and minimize their negative effects. To mitigate the attacks in MANETs, several techniques have been designed and tested over time and again. The next section discusses such mitigation techniques for different attacks in the MANETs.

4.1 Blackhole mitigation techniques

An exchange of packets between a source node and a target node requires control packets (RREQ and RREP) to discover the path to the target and eventually to send the packets. There are two parameters namely, hop count and target sequence number, which are required to select the path to the target. The malicious nodes take the advantage of these two parameters and send fake RREP containing the fake hop count and fake destination sequence number to be selected by the start node and once these malicious are selected as the route to the target, this drops the data packets and results in the performance degradation of the network.

In [19], the authors propose to use the target sequence number threshold to determine whether the source of the RREP is malicious or genuine. When the RREP packet is received by the start node, the start node examines the blacklisted table that contains the entries of the blacklisted nodes and if it is found that the origin of the RREP is not present in this list, the next step involves the evaluation of the target sequence number against the threshold sequence number. If the received sequence number has a value that is higher than the calculated threshold sequence number, the node is marked as malicious, and by using the *Hello message* packet; the start node broadcasts the id of the node to its neighbours so that these nodes also blacklist this node.

In [20], the authors propose to mitigate the blackhole attack in AODV by creating a new table Cmg_RREP_Tab which will store all the RREPs from multiple nodes. The start node now analyses these RREPs and those RREPs containing a very large sequence number are eliminated and the originator of this RREP is marked as fraudulent/malicious. Then the RREP containing the highest sequence number among the remaining RREPs is selected and data is forwarded normally. The start node also saves the identity of this fraudulent node and subsequently, the control packets from this node are discarded.

In [21], the authors propose to use Merkle trees or hash trees to detect whether there is a fraudulent node present on the path from the start to the target. The assumption is that the start node holds the pre-calculated value that is created by the values of all the nodes present in the network. To confirm that the target node has received the data packet successfully, the destination node along with the intermediary nodes sends their values to the start node. The start node then recalculates the hash value from the values received by it and its value. If the precalculated value and the recalculated turn out to be the same, it is expected that the packets are successfully received by the target node and the path is free from any malicious node; otherwise, the path is suspected to contain any malicious node. This approach performs well but is quite resource-demanding in this type of network where there is already a scarcity of resources.

Table 2: Comparison of different mitigation techniques

Ref	Attack	Protocol	Approach	Simulation Environment	Results
[19]	Blackhole	AODV	Uses Sequence numbers	NS 2	Reduced overhead
[20]	Blackhole	AODV	Stores multiple route replies	NS 2.33	Higher PDR and a marginal increase in average end-to-end delay
[21]	Blackhole	AODV, OLSR	Merkle tree	OPNET 11.5	The better delivery ratio of packets. The higher detection rate of malicious nodes.
[22]	Wormhole	AODV	Round trip time and topological comparisons	NS 2	Higher detection rate with an accuracy of alarms
[23]	Wormhole	AODV	Uses route redundancy, route aggregation, and RTT	OPNET 14.5	Reduces packet drop
[24]	Wormhole	AODV	Employs fuzzy logic system and artificial immune system	NS 2	Outperforms other existing solutions in terms of false-negative ratio, false-positive ratio, detection ratio, packet delivery ratio, packets loss ratio, and packets drop ratio.
[25]	Greyhole	DSR	Uses Association table	NS 2	Proposed ADSR has higher throughput compared to normal DSR.

4.2 Wormhole Attack Mitigation Techniques

In [22], the researchers make use of *round-trip-time (RTT)* measurements in addition to the *topological* comparisons to detect the possibility of wormhole attacks. During the route discovery process, the path which contains the wormhole attackers has higher RTT due to the packet latency as compared to the average RTT. As such it is believed that there exists a path that contains the fraudulent nodes. In the later phase of this technique, control packets ENQ and ENQ_r are used to separate the genuine nodes from the suspect list.

In [23], the authors proposed to use three parameters; route redundancy, route aggregation, and RTT to detect the wormhole attack. Route redundancy is beneficial when many paths are available to the target and ensures that RREQ is received by the destination node. Route aggregation happens if the next hop of two nodes is the same node and then the route request is aggregated and combined into a single route request. The start node, in the RTT phase, calculates the RRT and hops count of every RREQ through multiple paths and stores this information in the form of a table. The hop count and RTT determines the nature of the path. If for a particular path the hop count is k and its RTT is more than $3k$ it is suspected to be containing the wormhole nodes and this path is avoided.

In [24], the authors proposed to use a fuzzy logic expert system and computationally intelligent artificial immune system to guard against the attacks particular wormhole attacks in MANETs. By applying fuzzy logic, high-performance routes are selected from the available routes from the start node to the target node. After this step, an artificial immune system is applied to every route wherein the nodes are examined for their behaviour and finally a route containing the highest immune is selected to be the path from the start to the target.

4.3 Grey-hole Attack Mitigation Techniques

In [25], the authors proposed to use an Association model with a focus on trust values of the neighbouring nodes. These nodes are classified into known, unknown, and

companion nodes. Whenever multiple RREP comes, the path that contains the nodes with the largest trust is designated as a communication medium. In [26], the authors make use of the Cuckoo search (CS) algorithm along with support vector machines (SVM) on AODV protocol to detect greyhole attacks. CS finds the best route based on properties such as energy consumption, coordinates of the nodes and later optimizes them and finally, these are fed to the SVM classification algorithm which then detects the malicious nodes.

4.4. Byzantine Attack Mitigation Techniques

In [27], the authors proposed a new protocol, ODSBR that is resilient to Byzantine attacks [40]. Whenever there is a significant drop in the throughput of the system, ODSBR enters a probing phase and narrows down logarithmically the search for the location of a

malicious node. The link that is suspected to be malicious is assigned more weight so that in the future that path is avoided.

In [28], the author proposed to use an enhanced cooperative bait detection system (ECBDS) wherein that detects and prevents the malicious nodes from taking part in the communication in the network. In this proposed method, a bait RREQ is broadcasted and if any node sends an RREP to this request, it is confirmed that it is a malicious node and an alarm is raised in the system informing about the malicious node.

5. Discussion

MANETs are vulnerable to both inside and outside attacks. The outside attacks such as Blackhole, wormhole, and greyhole attacks can be mitigated with different techniques provided in the literature. Blackhole attacks are the most common attacks in MANETs and need a lot of attention when these are executed cooperatively by the malicious nodes. Non-cooperative attacks can be detected and handled easily. While the inside attacks such as Byzantine attacks are executed by the nodes which were once genuine nodes of the network. These attacks are very difficult to identify and mitigate. Several techniques have been proposed to mitigate such attacks. Each technique has some advantages and limitations. As these networks are decentralized in nature, techniques that are employed in decentralized systems should be looked upon. Blockchain technology was first implemented in the Bitcoin network in 2008, healthcare systems [41], finance, IoT [42], agriculture, and various other fields and is a good candidate to be selected to mitigate such attacks. Employing consensus algorithms, it will be difficult for the malicious nodes to execute such attacks. Further Inter-Planetary File System (IPFS) can be used to store the routing information so that malicious nodes cannot tamper with the information stored therein.

6. Conclusion

MANETs have been a prominent topic in the research from the last decade to their flexibility and ease of deployment. In this paper, we presented various routing protocols and the various attacks that are executed on these protocols. We also discussed the mitigation techniques to counter these attacks A comparison of different routing attacks and their mitigation techniques is also discussed. The routing protocols in MANETs are considered efficient on lower packet delay rates. AODV and DSDV are more efficient in performance than other protocols. The significance of detection and mitigation techniques makes this field wide open for researchers to work on the security aspect of these networks.

Many techniques are available to detect and mitigate each attack, however, each technique has its pros and cons. Some techniques come with higher throughput but at the same time, we have to compromise on the end-to-end delay parameter. Detection techniques can perform better but can result in higher overhead also. A trade-off between the detection technique and its effect on PDR, end-to-end delay, and overhead at the same time should be kept in mind while designing the new technique.

References

1. Abolhasan,M.,Wysocki,T.,Dutkiewicz,E.: A review of routing protocols for mobile ad hoc networks. In: Ad Hoc Networks, vol. 2, no. 1, pp. 1–22, Jan. 2004
2. Kannhavong,B.,Nakayama,H., Nemoto, Y., Kato,N., Jamalipour,A.: A survey of routing attacks in mobile ad hoc networks. In: IEEE Wireless Communications, vol. 14, no. 5, pp. 85–91, Oct. 2007
3. Hu,Y.C.,Perrig, A.,Johnson,D. B.: Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In: Wireless Networks, vol. 11, no. 1–2, pp. 21–38, Jan. 2005
4. Alani, M. M. (2014, November). MANET security: A survey. In 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE 2014) (pp. 559-564). IEEE
5. Boukerche,A.,Turgut,B.,Aydin, N.,Ahmad,M. Z.,Bölöni,L., Turgut,D.:Routing protocols in ad hoc networks: A survey. In: Computer Networks, vol. 55, no. 13, pp. 3032–3080, Sep. 2011
6. Saeed,N. H.,Abbod, M. F., Al-Raweshidy,H. S.: MANET routing protocols taxonomy. In: International Conference on Future Communication Networks, Apr. 2012
7. Royer,E. M., Chai-KeongToh.: A review of current routing protocols for ad hoc mobile wireless networks. In: IEEE Personal Communications, vol. 6, no. 2, pp. 46–55, Apr. 1999
8. Broch,J.,Maltz,D. A., Johnson, D. B., Hu, Y.-C.,Jetcheva, J.: A performance comparison of multi-hop wireless ad hoc network routing protocols. In: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking - MobiCom '98, 1998
9. Beijar, N.: Zone routing protocol (ZRP). In: Networking Laboratory, Helsinki University of Technology, Finland, *9*, 1-12. 2002
10. Fan,X.,Cai,W.,Lin,J.:A survey of routing protocols for highly dynamic mobile ad hoc networks. In: IEEE 17th International Conference on Communication Technology (ICCT), Oct. 2017
11. Khan,F. A.,Imran,M., Abbas,H.,Durad,M. H.: A detection and prevention system against collaborative attacks in Mobile Ad

hoc Networks. In: Future Generation Computer Systems, vol. 68, pp. 416–427, Mar. 2017

12. Al-Shurman,M.,Yoo,S.M.,Park,S.: Black hole attack in mobile Ad Hoc networks. In: Proceedings of the 42nd annual Southeast regional conference on - ACM-SE 42, 2004
13. Junhai, L., Mingyu F., Danxia Y.: Black hole attack prevention based on authentication mechanism. In: 11th IEEE Singapore International Conference on Communication Systems, Nov. 2008
14. Jhaveri,R. H., Desai, A., Patel,A.,Zhong,Y.: A Sequence Number Prediction Based Bait Detection Scheme to Mitigate Sequence Number Attacks in MANETs. In: Security and Communication Networks, vol. 2018, pp. 1–13, Nov. 2018
15. Jha,H. N., Gupta,S.,Maity,D.:Effect of Wormhole Attacks on MANET. In: Design Frameworks for Wireless Networks, pp. 177–195, Aug. 2019
16. Jamal,T., Butt, S. A.:Malicious node analysis in MANETS. In: International Journal of Information Technology, vol. 11, no. 4, pp. 859–867, Apr. 2018
17. Ojetunde,B., Shibata, N.,Gao, J.: Securing Link State Routing for Wireless Networks against Byzantine Attacks: A Monitoring Approach. In: IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Jul. 2017
18. Geetha,A.,Sreenath,N.: Byzantine Attacks and its Security Measures in Mobile Adhoc Networks. In: International Journal of Computing, Communication and Instrumentation Engineering, vol. 3, no. 1, Jan. 2016
19. Kumar,J.,Kulkarni,M., Gupta,D.,Indu,S.: Secure route discovery in AODV in presence of blackhole attack. In: CSI Transactions on ICT, vol. 3, no. 2–4, pp. 91–98, Dec. 2015
20. Nital,M.,Jinwala,C.,Zaveri. M.: Improving AODV protocol against blackhole attacks. In:*Proceedings of the international multi conference of engineers and computer scientists*. Vol. 2. 2010
21. Baadache, A.,Belmehdi,A.: Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. In: Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1130–1139, May 2012
22. Alam, M.R.,Chan,K.S.: RTT-TC: A topological comparison based method to detect wormhole attacks in MANET. In: IEEE 12th International Conference on Communication Technology, Nov. 2010
23. Shin, S.Y.,Halim,E. H.:Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation. In: International Conference on ICT Convergence (ICTC), Oct. 2012
24. Jamali,S.,Fotohi, R.: DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system. In: The Journal of Supercomputing, vol. 73, no. 12, pp. 5173–5196, May 2017
25. Bhalaji,N.,Shanmugam,A.: Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Adhoc Networks. In: Procedia Engineering, vol. 30, pp. 881–888, 2012
26. Thakur, S.,Dalwal, S.: Mitigating Gray Hole attack in Mobile AD HOC Network using Artificial Intelligence Mechanism. In: ijacms, Special Issue, vol. 8, no. 9S, pp. 640–645, Aug. 2019.
27. Awerbuch,B.,Curtmola,R.,Holmer,D., Nita-Rotaru,C., Rubens, H.:ODSBRIn: ACM Transactions on Information and System Security, vol. 10, no. 4, pp. 1–35, Jan. 2008
28. Mehta,A.: Combating against Byzantine Attacks in MANET using Enhanced Cooperative Bait Detection Scheme (ECBDS). In: *IOSR Journal of Computer Engineering (IOSR-JCE)* Jun. 2017
29. Tuteja,A., Gujral,R., Thalia,S.: Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET Using NS2. In: International Conference on Advances in Computer Engineering, Jun. 2010
30. S. K.: ANALYSIS OF ZONE ROUTING PROTOCOL IN MANET. In: International Journal of Research in Engineering and Technology, vol. 02, no. 09, pp. 520–524, Sep. 2013
31. Patil,P. N., Bhole, A. T.:Black hole attack prevention in mobile Ad Hoc networks using route caching. In: Tenth International Conference on Wireless and Optical Communications Networks (WOCN), Jul. 2013
32. Mahmood, R. A. R., Khan, A. I.: A survey on detecting black hole attack in AODV-based mobile ad hoc networks. In: International Symposium on High Capacity Optical Networks and Enabling Technologies, Nov. 2007
33. Alem, Y. F., Xuan, Z. C.: Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. In: 2nd International Conference on Future Computer and Communication, 2010
34. R., Popli, D. R.: A WORM HOLE ATTACK DETECTION IN MOBILE AD-HOC NETWORK USING GA AND SVM. In: International Journal of Engineering Applied Sciences and Technology, vol. 5, no. 3, pp. 582–588, Jul. 2020
35. Chiang, M. L.:Eventually Byzantine Agreement on CDS-based mobile ad hoc network. In: Ad Hoc Networks, vol. 10, no. 3, pp. 388–400, May 2012
36. Lent, R., Barri, J.:Towards Reliable Mobile Ad Hoc Networks. In: Mobile Ad-Hoc Networks: Protocol Design, Jan. 2011
37. Pandit,V., Jun, J. H., Agrawal,D. P.: Inherent Security Benefits of Analog Network Coding for the Detection of Byzantine Attacks in Multi-Hop Wireless Networks. In: IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems,

Oct. 2011

38. S. Jamali, L. Rezaei, and S. J. Gudakahriz, “An Energy-efficient Routing Protocol for MANETs: a Particle Swarm Optimization Approach,” Journal of Applied Research and Technology, vol. 11, no. 6, pp. 803–812, Dec. 2013.
39. J. Edwards, “Covert channels in ad hoc networking : an analysis using the optimized link state routing protocol.”
40. R. Yousuf, Z. Jeelani, D. A. Khan, O. Bhat, and T. A. Teli, “Consensus Algorithms in Blockchain-Based Cryptocurrencies,” 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Feb. 2021.
41. R. Yousuf, D. Ashraf Khan, and Z. Jeelani, “Security and Privacy Concerns for Blockchain While Handling Healthcare Data,” Blockchain for Healthcare Systems, pp. 177–192, Jul. 2021.
42. T. A Teli, F. Masoodi & R Yousuf .”Security Concerns and Privacy Preservation in Blockchain based IoT Systems: Opportunities and Challenges.”(2021)