International Journal of Networks and Communications 2018, 8(4): 115-122
DOI: 10.5923/j.ijnc.20180804.03

Detection of Route Discovery Misbehaving Nodes in AODV MANETs: A Survey

Hala Mustafa, Noureldien A. Noureldien*

Department of Computer Science, University of Science and Technology, Omdurman, Sudan

Abstract The ad-hoc on demand distance vector protocol AODV is the most reactive protocol that is widely used to implement mobile ad-hoc networks (MANETs). As a responsive protocol, it seeks to set up a route on demand when two nodes in the networks need to communicate. When a source node needs a route to a destination, the AODV looks for the route in its routing table where the previously allocated routes are stored. If the route is not in the route table, AODV will launch a route discovery process that aims to return a route to the destination if a network path exists to the destination. Route discovery process fails when a wrong route is returned, or no route is restored although a network path to the destination exists. Both fails are due to misbehaving by one or more nodes in the network. This node misbehaving is due either to a selfishness behavior or malicious behavior. Discovering misbehaving nodes during route discovery is essential to maintain a fresh correct route to destinations. Many methods for detecting such misbehaving nodes have been proposed during the last decades. This paper provides a survey of methods proposed to detect misbehaving nodes and define a classification for these methods. The classification makes the understanding of these methods easier and allows for comparing the pros and cons of each category.

Keywords Misbehaving nodes, Detection methods, Route discovery phase, Control packet-based detection methods, Trust based detection methods, Sequence number based detection methods

1. Introduction

Ad hoc On-demand Distant Vector (AODV) protocol is a simple, efficient, active and reactive method of routing messages between mobile nodes in mobile ad-hoc networks (MANET). AODV defines two phases of communication between two nodes. The route discovery phase, in which the source node seeks a route to the destination node with the cooperation of other nodes, and a packet forward phase in which nodes cooperate in forwarding packets between source and destination along the constructed route. Due to this cooperativeness nature of MANETs, each node is expected to perform in a known behavior as defined by the routing protocol in both phases.

When a node is not behaving as expected, it is called a misbehaving node. Misbehaving by a node can be a result of an intentional or unintentional act. Intentional acts mean the node is intended to misbehave either for selfishness or malicious purpose, while unintentional acts may result from states such as battery gets out, overloading or node is broken.

* Corresponding author:
noureldien@hotmail.com (Noureldien A. Noureldien)
Published online at http://journal.sapub.org/ijnc

Misbehaving is a severe problem since it breaks down the normal trustful operations in route discovery and packet forwarding phases. Misbehaving occurs either during the route discovery phase or the packet forwarding phase. In this paper, we deal only with route discovery misbehaving nodes.

Route misbehaving occurs when a node refuses to forward an RREQ or RREP packets to reserve resources (Selfishness), a node impersonates the destination, or claiming to have a route while it is not (Masquerading) will disrupt the route discovery.

The rest of this paper was organized as follows; section II explains route discovery in AODV MANETs. In section III, the surveyed proposed detection methods are presented in a new classification schema. In section IV conclusions and recommendations for future research are drawn.

2. AODV Route Discovery

In AODV MANETs the route discovery phase is as follows;

When a source node wants to send a message to another node that is not in its neighbors, do not have a route to it or have with very with, it will generate route request message (RREQ) and broadcasts it to its neighbors. The Route Request (RREQ) message contains hop count, broadcast ID, destination IP address, destination sequence number, source IP address, source sequence number, and timestamp [1].

Once a neighbor node receives an RREQ message request, it extracts the destination from the RREQ message and looks in its routing table to find a matching a route to the destination. In AODV, routing table contains destination IP address, sequence number; hop count, next hop IP address, precursor list, the time when entry expires. If the node itself is the destination or it looks up a fresh route to the destination it creates and sends a Route Reply (RREP) message contains the destination IP address, destination sequence number, hop count, source IP address, lifetime and timestamp.

[2] Otherwise, the neighbor node will rebroadcast the RREQ message to its set of neighbors who will act as in 2.

[3] The rebroadcasting of the RREQ won't continue indefinitely; it stops either when the source receives an RREP or when the RREQ lifespan is up. In the last case, the source node has to rebroadcast the original RREQ but this time with a longer lifespan and a new ID number.

Due to the mobility nature of MANETs, AODV uses sequence numbers as timestamps in its messages. Sequence number value is increased whenever a message (any message that is) is broadcasted. So the sequence number of RREP messages can be used by the source node to indicate how fresh the route is. A higher sequence number signifies a fresher route.

In AODV protocol, by default, the source node accepts the first fresh enough RREP message coming to it. The freshness of the RREP is determined as follows; for every RREP control message received, the source node would first check its route table to see whether it has a previous route to the destination or not. If it finds a route, it compares the destination sequence number in the incoming RREP with the destination sequence number it the route table. If the RREP has a higher destination sequence number then the source node will consider the RREP route as a fresh route and update its routing table with the new RREP control message; otherwise if the destination has no previous entry in the route table, and the RREP sequence number is higher than the source sequence number sends in the last RREQ message, then the source node will register RREP in its route table, else RREP is discarded.

In AODV this process is performed by *Receive Reply (Packet P)* method [1]. The manner in which the RREP control message is handled is explained in the pseudo code of the *Receive Reply (Packet P)* function of AODV in Fig. 1.

To maintain routes in routes tables in MANET nodes, AODV makes use of Route Error (RERR) message which allows AODV to reconfigure in the that leads to dead-ends/nodes or nodes detached from the MANET, route defined.

An error message can be broadcasted due to three reasons, firstly when a node receives a data packet that's supposed to be forwarded but a path to the destination node isn't found. Secondly when a node receives a RERR that causes one of its stored routes to be invalidated, if this happens the node will broadcast a RERR with all the new nodes which are now unavailable.

Finally, a node can detect its inability to communicate with one of its neighbor (HELLO message from a neighbor isn't received within expected interval) and thus mark all of its stored routes using dead node as invalid and broadcast RERR message to other neighbors to perform the same operation.

In the route discovery phase, the MANET could be susceptible to many attacks attempts by misbehaving nodes.

```
At Source Node: AODV
1 ReceiveReply (Packet P){
2  if(P has an entry in Route Table){
3    select Dest_Seq_No from routing table
4      if(P.Dest_Seq_No > Dest_Seq_No){
5        update entry of P in routing table
6        unicast data packets to the route
         specified in RREP
7      }
8      else {
9          discard RREP
10     }
11   }
13   else {
14     if(P.Dest_Seq_No >= Src_Seq_No){
15       Make entry of P in routing table
16     }
17     else {
18       discard this RREP
19     }
20   }
21 }
```

Figure 1. Pseudo code of *Receive Reply (Packet P)* method

3. Detection of Misbehaving Nodes in Route Discovery Phase

Many misbehaving detection methods in route discovery phase are introduced in the few past years. These methods aim to detect the misbehaving nodes during the route discovery phase and provide means for the source node to find the most reliable route to the destination.

We collect and study the available published methods to identify the way each method use to detect misbehaving nodes. Based on our analysis, we classify these solutions into four categories; Methods that based on control packets, Trust-based methods, Sequence Number-based methods, and Control packet-sequence number based methods. In the following subsections, we will explain the detection concept behind each of the four categories along with the proposed methods in each category.

3.1. Control-Packets-based Detection Methods

In control-based detection methods, the idea of detection

is based on either adding new control packets to AODV or modifying the existing control packets. These modifications allow the source node to be able to detect the misbehaving nodes in the network and later may determine a genuine path.

Methods fall in this category include R-AODV [2], a robust routing solution [3], a challenged node technique [4], request and reply to route detection method [5] and a further request and response method [6].

3.1.1. Reliable-AODV (R-AODV)

The reliable-AODV [2], modify the structures of RREQ and RREP and add a field to the routing table. For the RREQ message, R-AODV adds a new field called a MALICIOUS_NODE_LIST, which will be used to notify other nodes about malicious nodes in the MANET. For the RREP message, R-AODV adds a flag called DO_NOT_CONSIDER to mark/identify reply from a malicious node. In routing table, R-AODV adds a field called MALICIOUS_NODE for marking a node as a malicious node.

The solution calculates a value called PEAK value based on the number of sent outRREQs, the number of received RREPs and routing table sequence number to detect the existence of a malicious node. The destination sequence number of the received RREP is compared with this PEAK value. The R-AODV modifies the functionalities of nodes sending RREQ, nodes receiving RREQ and nodes receiving RREP using specific algorithms while functionality for nodes sending RREP remains as it is.

Detection of misbehaving nodes is as follows;

1) If an RREP has a destination sequence number that is less than or equal to the PEAK value, the node that sends the RREP is considered as an honest node.
2) If the RREP has destination sequence number that is greater than the PEAK value, the node sending RREP is marked as MALICIOUS_NODE in the routing table, and the RREPis marked as DO_NOT_CONSIDER.

So in R-AODV the RREQ and RREP routing packets are used to propagate information about misbehaving nodes to other nodes in the network.

3.1.2. Robust Routing in Wireless ad hoc Networks

This proposed solution [3], is based on adding two additional control packets to ensure correctness of the route information sent by the intermediate nodes. The extra control packets are route confirmation request (CREQ) and route confirmation reply (CREP). When an intermediate node responds to a route request (RREQ) from the source node with an RREP message, it must verify the correctness of the route by the next hop node towards the destination node.

For example, if E is an intermediate node that has a fresh route to the destination D, then it sends an RREP to the source node A and CREQ to the next hop node F asking node F to verify the correctness of the route. If F finds the route in its cache, then it sends a CREP to the source node A, verifying that the RREP send by the intermediate node E is correct. Otherwise, it does nothing. In the late case, the source node will ignore the RREP from E considering that route to node D is less reliable and it uses another route to data transmission.

When a source node compares the two messages, RREP and CREP, it may find that the information they carry is inconsistent. The source node will use the route based on policy. When the policy is EXACT, the source will use the route when the information advertises in the RREP, and the CREP are identical. When the policy is DIFF_ONE, the source node will only use the route if the difference between two hops counts is not more than one.

3.1.3. Challenged Node Technique

In this method [4], two additional new control messages are added, the challenged route request (CRREQ) and the challenged route reply (CRREP). The method challenged the intermediate node that sends a route reply RREP by its neighbors to verify the correctness of the information on the route reply control message RREP.

When a neighbor overhears the new route reply, they create a challenged route request (CRREQ) that contains the information in the route reply (RREP) and send it to the next hop towards the destination. The next hop node searches its route table entries to check the correctness of the route in the CRREQ, if it is true, then the next hop create the challenged route reply (CRREP) message and send it to the source node. Otherwise, the next hop will not send (CRREP), in which case the neighbors will not hear a CRREP and consider the intermediate node as a misbehaving node.

3.1.4. Request and Reply for Route and Detection

In this proposed solution [5], the original REQ message is modified to become a request to route with detection (DRREQ) and the route reply message to become route reply with detection (DRREP).

The basic idea is that; when the source node broadcast (DRREQ) to find a route to the destination node, it sends two destination IP addresses in the (DRREQ) one is a valid IP address while the other is an invalid one. When an ordinary node receives the (DRREQ), it will search for both destinations IP addresses in its route table entries. If it sends a response, it will be to the valid IP address.

On the other hand, the malicious node will not search both destinations IP addresses in its route table, and it will respond to both IP addresses.

When an intermediate node sends (DRREP), the source node can determine whether it is coming from a normal mode or a malicious node by checking the two bits flag in the new (DRREP) control message. If the reply is from a normal node, the source node will use the route. Otherwise, the source node will mark the node as malicious in its routing table and broadcasts an alert message to its neighbors with the malicious node ID.

3.1.5. Further Request and Reply

In this method [6], a new technique to detect misbehaving nodes in the route discovery phase is proposed. In this method, each intermediate node replies to an RREQ must send information about its next hop node towards the destination. When the source node receives the RREP control message, it will extract the information about the upcoming hop node and send to it a further request asking to verify the correctness of the route to the destination node. Only the requested next hop node can reply to the further request, which includes the check result field. The path of the further reply to the source node must not contain the intermediate node to avoid the fabrication of the further reply message.

When the source node receives the further reply message, it checks the value of the check result field. If the value is True the source node will establish the route to send the data packets. Otherwise, the source node will consider the intermediate node as a misbehaving node, and it will send an alerting message to the whole network to isolate the misbehaving node from the network.

Table (1) shows a summary of control-packet based methods.

Table 1. Summary of control–Packet Based Methods

Method proposed by	New packet (Yes/ No)	Modified existing packet (Yes/ No)	Type of attack	Routing overhead (yes/no)	Prevention method (yes/no)
Jhaveri, Patel & Jinwala 2012	No	Yes	Single	No	Yes
Lee, Han & shin 2002	Yes	No	Single	Yes	No
Reddy & Khilar 2011	Yes	No	Single	Yes	No
Tiwari & Yadav 2015	No	Yes	Single/ cooperative	No	Yes
Deng, Li & Agrawal 2002	Yes	Yes	Single	Yes	Yes

3.2. Trust-based Detection Methods

In trust-based detection methods, the basic idea is the assessment of each node by its neighbors. Neighbors of each node overhear the node incoming and outgoing packets traffic and assess the node accordingly.

Methods in this category include; Trust-embedded AODV [7], A Trust-based routing [8], Trust-based energy efficient detection [9], Light-weight trust-based routing [10] and trust based multi-path routing [11].

3.2.1. Trust-embedded AODV

The Trust-embedded AODV (T-AODV) routing protocol [7] was designed to secure an ad hoc network from independent malicious nodes by finding a secure end-to-end route. In this protocol, trust values are distributed to nodes a priori. In the route discovery phase, the RREQ packet header contains a trust_level field, in addition to the other fields. Each intermediate node rebroadcasts the RREQ after modifying the trust_level by including the trust level of the node that sends it the RREQ. All the RREPs are sent to the source. The source node selects the route with the highest value of the trust_level metric.

3.2.2. A Trust-based Routing

A Trust-based routing is proposed by Pirzada et et al., in this solution a Trust agent derives trust levels from events that are directly experienced by a node, to share trust level of one node with other nodes a Reputation agent is used. The final trust level of a node is calculated by a Combiner based on information it receives from the Trust and Reputation agents. Trust is computed using direct and indirect in formation. The trust value is propagated among nodes by attaching the trust value of the nodes along with RREQ packets [8].

For a source node to select a route to the destination, it scans the routing table looking for all paths that lead to the destination. It compares the direct trust value of all next hops in each path and selects the one with the highest trust value, nodes with low trust values are considered to be misbehaving or malicious nodes.

However, the network overhead is increased because of the indirect information used in trust calculation, as it uses more control packets for advertising trust, calculating observed trust and in using certificates in the trust calculation.

3.2.3. Trust Based Energy Efficient Detection

In this method [9], a new scheme based on trust to build a reliable and secure route in the network is proposed. The method defines the following equation to calculate the trust of a node.

$$trust\_node = Rank * Rem\_b.\ p * S.\ F.\ node,$$

Where

Rank is a reliability value that is measured every time the node participates in a successful forwarding of a packet. The Rank increment after acknowledgment from the destination node to the source node, and when a node rank decrease to 0 it will be detected as a misbehaving, malicious node, and an alarm message is broadcast to an entire network.

Rem_b. P is the remaining battery power of the node, and ***S.F*** is the stability factor represent the stability of a node calculated from equation *S.F = TPause/Vnode, TPause*is time pause indicating the duration node stop for a while ***V node*** indicating node velocity, a higher value of *S.F. Node*

indicating more stable node.

When a node initiates an RREQ to find a reliable route to the destination it waits for a "timer" to receive the RREPs, the source node has to select a route with the highest average trust calculated from the trust value of each node in the selected route.

3.2.4. Light-weight Trust-based Routing

This method [10], modifies the original behavior of the AODV protocol by adding a trust table that holds information about the reliable nodes delivered from a behavior analysis filter. Every node shares this file in the RREQ packet. The method also adds a trust field in the RREP, which will indicate the node reliability. This trust field can only be maintained by the first next hop in the reverse path. It can only hold one of the following values: 2 indicate that the RREP is from the destination itself, 1 indicates that it's a trusted node and 0 indicates that it is a misbehaving node.

3.2.5. Trust Based Multi-path Routing

In this method [11], a new detection technique to detect and isolate misbehaving nodes in both phases, route discovery and data transmission was proposed. To enhance the security in route discovery phase a trust multipath routing protocol is used, it discovers a secure, trustworthy path from the route to the destination with minimal overhead.

The protocol modified the traditional route discovery process by embedding the trust information in the RREQ, and RREP controls massages. The protocol assumes that each node will create a trust table and stores the trust value of its one-hop neighbors. The trust value is assigned in the range 0 to 1, a trusted node must have a trust value bigger than 0.5, while a misbehaving node has a trust value less than 0.5. Path trust is the trust value associated with the path; this value is defined as the weighted average of the trust values of the nodes in the path. To calculate the path trust value, the RREQ and RREP are modified so that they contain the trust value field. The source node calculates the path trust value from the information in the RREP. Hence, a trust path contains mutual trust information about the nodes in the path from the source to the destination these nodes can detect and isolate the misbehaving nodes so they can avoid the routing attacks launched by them.

Table (2) shows a summary of Trust-based methods.

Table 2. A Summary of Trust-Based Methods

Method proposed by	New function/ table	Modified existing packet	Neighbors Assessment (yes/ No)	Type of attack	Computation overhead (yes/no)	Prevention method (yes/no)
Biswas, Nag & Neogy 2014	Timer	-	Yes	Single/ Cooperative	Yes	Yes
Pissinou, Ghosh & Makki 2004	-	Trust_level field RREQ	Yes	Single	Yes	Yes
Marchang & Datta 2012	Trust table	Trust_level field RREQ, RREP	Yes	Single	Yes	No
Gera, Garg & Misra 2010	Trust table	Trust_level field RREQ, RREP	Yes	Single	Yes	No
Pirzada, Datta & McDonald 2004	-	Trust_level field RREQ	Yes	Single	Yes	No

3.3. Sequence Number based Detection Methods

The sequence number value enclosed in RREP message is the peace of the information that is used by AODV at the source to determine the freshness route in the route discovery phase. AODV at source node selects the best route from received RREPs based on the high sequence number and lower hop count. Most of the misbehaving nodes in route discovery phase exploit this by sending RREP with high sequence number pretending to have a fresh route to the destination.

Detection methods that based on sequence number intend to alternate the normal way AODV works by not selecting the RREP directly with the highest sequence number as a legitimate fresh route. Methods in this category include MOSAODV method [12], Detection of misbehaving nodes using sequence numbers [13], Trust and sequence number detection method [14], Mitigation method [15], and ERDA [16].

3.3.1. MOSAODV Method

Nita et al., [12] provided a modification in AODV called MOSAODV. The proposed method added a new table Cmg_RREP_Tab, a timer MOS_WAIT_TIME and a variable Mali_node to the data structures in the default AODV protocol.Cmg_RREP_Tab is used to store RREP until the time, MOS_WAIT_TIME. Based on the heuristics, MOS_WAIT_TIME is initialized to be half the value ofRREP_WAIT_TIME – the time for which source node waits for RREP control messages before regenerating RREQ.

The source node after receiving first RREP control message waits for MOS_WAIT_TIME, then the source node checks stored RREPs from the mg_RREP_Tab table, and discard the RREPs having apparently very high destination sequence number. The node that sent this RREP is suspected to be a misbehaving node. The source node stores nodes that have been identified as misbehaving in the Mali_node, so

that in future, the source node can discard any RREP messages coming from that node.

3.3.2. Detection of Misbehaving Nodes Using Sequence Numbers

Singh and Manpreet [13] have proposed a method to find the secure route and prevent the misbehaving nodes in MANETs. The determine the genuine of the route; the method checks whether there is a significant difference between the sequence number of the source node and the intermediate node which has sent back the first RREP or not.

The detection method builds a table to store RREPs messages received in response to source RREQ. The method compares the sequence number in RREPs with that of the resource node; if there is a significant difference, the method considers that RREP is originated from a malicious, misbehaving node and remove it from the table. The RREP with a reasonable difference is considered to be from a legitimate node and the route defined by that RREP is used by the source node.

3.3.3. Trust and Sequence Number Detection Method

An algorithm that based on trust and sequence numbers is proposed in [14]. The algorithm proposes modifying AODV to use at each node a variable W-TIME as a waiting timer, and two tables, the RREPs_TABLE to store received RREPs during W-Time, and a TRUST_TABLE to store trusted nodes, which are nodes that previously send the source node good routes.

When a source node requests for a route to a destination, all RREP replies are stored in RREPs_TABLE. The source node scans the RREPs_TABLE looking for an RREP originated from a trusted node that is already registered in the trusted nodes table TRUST_TABLE.

If the RREP is found to be from a trusted node, then it will be used, else the sequence number technique will be applied, and RREPs entries with very high sequence numbers will be considered as misbehaving nodes. If an RREP with an adequate sequence number is found, then that RREP will be considered by the source node to originate from a trusted node and the source node adds the RREP to the TRUST_TABLE, and the RREP will be used as a trusted route.

3.3.4. Mitigation Method

In this method [15], authors proposed a method to secure AODV protocol against misbehaving during the route discovery phase by using a threshold value to compare it with the sequence number of the RREQ and RREP packets. The threshold definition is based on three environments which are a small network, medium network, and large network. When the source node receives an RREP from the intermediate node, it compares the sequence number in the RREP control message with the threshold value based on the type of the environment. If the sequence number in the RREP packet is less than the determined threshold value for the environment, the source node will consider that node is normal and will use the route. Otherwise, it will consider it as a misbehaving node and will discard the packet.

3.3.5. ERDA

In this method [16], a new detection technique aims to minimize the routing overhead and the latency time as a result from using the additional control packet as a detection technique for detecting the misbehaving nodes is proposed, the new detection technique is more efficient in processing than control packet-based detection.

The ERDA (Enhanced Route Discovery AODV) is an enhancement of the AODV protocol. It is designed to improve the overhead incurred during route discovery phase. Three new elements are added to AODV protocol; ***rrep_table*** to store all incoming RREP control message, ***mali_list*** to keep the identity of the malicious node, and ***rt_upd***new to receive either true or false indicating whether the node can update the route table entry for the destination.

When a node flood the network with an RREQ asking for a route to a specific destination, it stores all the received RREPs in the ***rrep_table***, at the same time the routing table will be updated by every receive***d*** RREP. Once an RREP is received from the destination node, the rt_updnew will be ***rt_upd***set to false. In such a case, the ***rrep_table*** will be analyzed using a heuristic search method to find nodes that have a high sequence number and mark such nodes as ***mis***behaving and recorded in the mali_list.

Table (3) shows a summary of Sequence Number Based Methods.

Table 3. A Summary of Sequence Number Based Methods

Method proposed by	Protocol used	New function/ table	Threshold value (yes/ No)	Type of attack	Computation overhead (yes/no)	Prevention method (yes/no)
Mistry, Jinwala & Zaveri, 2010	AODV	Cmg_RREP_Tab, Timer, Mali_node	No	Single	Yes	Yes
Singh & Manpreet, 2013	AODV	C_RREP_T, Timer, M_node	No	Single	Yes	Yes
Saeed & Noureldien, 2015	AODV	RREPs_TABLE, TRUST_TABLE, Timer	Yes	Single/ cooperative	Yes	Yes
Kumar, Quyoom & Gouttam, 2015	AODV	-	Yes	Single	Yes	No
Jalil, Ahmad & Manan, 2011	AODV	rrep_table, mali_list, rt_upd	No	Single	Yes	Yes

3.4. Methods Based on Control Packet and Sequence Number

This category contains methods that modify or add AODV control packets and use RREP sequence number to identify misbehaving nodes. Methods in this category include; Dynamic Learning [17], and Modified AODV routing protocol [18].

3.4.1. Dynamic Learning

DPRAODV protocol suggested by Payal et al. [17] adds a new control packet, ALARM, which will be sent by the source node that detects misbehaving node/s to other nodes to disseminate the misbehaving node information.

The method periodically calculates the difference of destination sequence number of received RREP message and that of routing table entry and compares it with the threshold value; for greater difference than the threshold, the node sending RREP is marked as a malicious misbehaving node. Node detecting the malicious node broadcasts an ALARM packet to inform neighbor nodes about existence of a malicious node.

3.4.2. Modified AODV Routing Protocol

In this method [18], an additional control packet is added to verify the sequence number in the RREP control message by an intermediate node. When an intermediate node or a destination node responds to the RREQ, it sends two RREPs containing an additional field called verification field, which will be used later to verify the sequence number. The first RREP has a normal sequence number while the second RREP have a sequence number incremented by one. When an intermediate node receives the first RREP, it stores the RREP message and waits for the second RREP. In obtaining the second RREP, it compares its sequence number with that of the first RREP. If it is less by one than the first RREP sequence number, the intermediate node sets the verification field to 1 and forward the RREP control message towards the source node. Otherwise, it sets the verification field to 0, identifying that the RREP was sent by a misbehaving node that uses a very high sequence number, and the RREP will not be forwarded further in the network.

Table (4) shows a summary of the control packet and sequence number based methods.

Table 4. Summary of Control Packet and Sequence Number Based Methods

Method proposed by	Protocol used	New packet /function/ table	Modified existing packet	Sequence number threshold value (yes/ No)	Type of attack	Routing overhead (yes/no)	Computation overhead (yes/no)	Prevention method (yes/no)
Raj, Swadas & Dpraodv 2010	AODV	Alarm packet	-	Yes	single	Yes	Yes	Yes
Moudni, Er-rouidi, Mouncif & Hadadi 2016	AODV	RREP_table,	Verified field RREP	No	Single/ cooperative	Yes	Yes	No

4. Conclusions

One of the most significant security problems in MANETs is misbehaving nodes. Misbehaving may results in breaching confidentiality and availability. Many detection methods have been proposed to detect misbehaving nodes during the route discovery process phase.

In this paper, we classify the misbehaving detection methods in route discovery phase into four classes methods that based on using an additional packet/s, so the source node can be able to find a secure route to the destination, methods that rely on neighbor's assessment to determine the trustfulness of the route, methods that uses the sequence number in detecting misbehaving nodes, and methods that combine both techniques of control packets and the sequence number.

This paper will help in understanding how detection methods work and how such methods can be improved.

REFERENCES

[1] Perkins CE, Royer EM, "Ad-hoc On-Demand Distance Vector Routing", Paper presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, Louisiana, 25–26 February 1999.

[2] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "Improving Route discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP, v. 11, no. 1, p. 01-12, March of 2012.

[3] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," in ICPP Workshops, pp. 73, 2002.

[4] K. Ganesh Reddy and P. M. Khilar. "Routing misbehavior detection and using reaction challenged node technique in manet." International Journal of Advance in Communication Engineering, vol. 3, pp. 23-28, July-December 2011.

[5] N. Tiwari and R. Yadav. "Detection of Black Hole Attack using Control Packets in AODV Protocol for MANET." International Journal of Computer Applications, vol. 118, pp 0975-8887, May 2015.

[6] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70–75, Oct. 2002.

[7] Pissinou, N., Ghosh, T. and Makki, K. 2004. Collaborative trust-based secure routing in multihop ad hoc networks. Lecture Notes in Computer Science, vol. 3042, 1446-1451.

[8] Pirzada, A. A., Datta, A. and McDonald, C. 2004. Trust-based routing for ad-hoc wireless networks, in Proceeding of IEEE International Conference Networks (Singapore, 2004). 326-330.

[9] S. Biswas, T. Nag, and S. Neogy, "Trust-based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," Application and Innovation in Mobile Computing, 2014, pp. 157–164.

[10] N. Marching and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," IET Information Security, vol. 6, no. 2, pp. 77, 2012.

[11] P. Gera, K. Garg, and M. Misra, "Trust-based multi-path routing for end to end secure data delivery in MANETs," in Proceedings of the 3rd international conference on Security of information and networks - SIN '10, Association for Computing Machinery (ACM), 2010.

[12] Mistry, N., Jinwala, D. C., and Zaveri, M. Improving aodv protocol against blackhole attacks. In Proceeding of International Multiconference of Engineers and Computer Scientists, volume 2, pages 1034–1039, March 2010.

[13] H. Singh and S. Manpreet, "Securing MANETs Routing Protocol under Black Hole Attack," International Journal of Innovative Research in Computer and Communication Engineering, June 2013. vol 1, issue 4, pp. 808-813.

[14] Saeed K. Saeed, Noureldien A. Noureldien, " A Detection and Prevention Algorithm for Single and Cooperative Blackhole Attacks in AODV MANETs," In proceedings of SECURWARE 2015: The Ninth International Conference on Emerging Security Information, Systems and Technologies, pp 79-84.

[15] R. Kumar, A. Quyoom, and D. N. Gouttam, "To mitigate black hole attack in AODV," 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Sep. 2015.

[16] K. A. Jalil, Z. Ahmad, and J.-L. A. Manan, "Securing routing table update in AODV routing protocol," in 2011 IEEE Conference on Open Systems, Institute of Electrical & Electronics Engineers (IEEE), 2011.

[17] Raj, P. N. and Swadas, P. B. Dpraodv: A dynamic learning system against black hole attack in aodvbased manet. International Journal of Computer Science Issues, 2(3): 54–59, 2010.

[18] H. Moudni, M. Er-rouidi, H. Mouncif, and B. E. Hadadi, "Modified AODV routing protocol to improve security and performance against black hole attack," in 2016 International Conference on Information Technology for Organizations Development, Institute of Electrical & Electronics Engineers (IEEE), 2016.