Discovering a Secure Path in MANET by Avoiding Black Hole Attack

Hicham Zougagh, Ahmed Toumanari, Rachid Latif, Y. Elmourabit
Laboratory ESSI,
National School of Applied sciences
Agadir, Morocco

Noureddine.Idboufker
Laboratory TIM
National School of Applied sciences
Marrakech, Morocco

***Abstract*—In a mobile ad hoc network (MANET), a source node must rely on intermediate nodes to forward its packets along multi-hop routes to the destination node. Due to the lack of infrastructure in such networks, secure and reliable packet delivery is challenging. The performance of a Mobile Ad hoc Network (MANET) is closely related to the capability of the implemented routing protocol to adapt itself to unpredictable changes of topology network and link status. One of this routing protocol is OLSR [1] (Optimized Link State Routing Protocol) which assumes that all nodes are trusted. However, in hostile environnement, the OLSR is known to be vulnerable to various kinds of malicious attacks. This paper proposes a cooperative black hole attack against MANETs exploiting vulnerabilities of OLSR. In this attack, two attacking nodes cooperate in order to disrupt the topology discovery and prevent routes to a target node from being established in the network.**

Keywords—MANET; OLSR; Security; Routing Protocol Cooperative black hole attack

I. Introduction

A Mobile Ad-hoc NETwork (MANET) is a collection of nodes which are able to connect to a wireless medium forming an arbitrary and dynamic network. Implicitly herein is the ability for the network topology to change over time as links in the network appear and disappear. In order to enable communication between pair of nodes in such a MANET, a routing protocol is employed. The abstract task of the routing protocol is to discover the topology to ensure that each node is able to acquire a recent map of the network topology to construct routes.

One way of securing a mobile ad hoc network at the network layer is to secure the routing protocols, so all possible attacks are prevented. The abstract task of the routing protocol is to discover the topology to ensure that each node is able to acquire a recent map of network topology to construct routes.

The Optimized Link Stat Routing Protocol (OLSR) is a proactive routing protocol for MANET, i.e. All nodes need to maintain a consistent view of the network topology. They are also vulnerable to a number of disruptive attacks in the presence of malicious nodes (identity spoofing, link withholding, link spoofing, miserly attack, wormhole attack and collusion attack..).

In this paper, we focus on the cooperative black hole attack [2] where two nodes cooperate to prevent routes to a target node from being established; the first attacker forces the target to choose it as its MPR node. It simply sends HELLO messages with willingness equal to Will_always, after this it will choose the second attacker as its only multi-point relay that can drop, alter or look at any packet it forwards. The result is that the routes to target node cannot be established by nodes more than two hops away from it.

In our approach, we present, we present an improved MPR selection algorithm that can reduce the number of malicious nodes trying to be selected as Multipoint Relay by maintaining its Willingness fields equal to Will_always.

The rest of the paper is organized as follows. The next section provides a short overview on OLSR, followed by the description of cooperative black hole attack. Section IV summarizes the literature. In section V, we present our approach to secure OLSR protocol. In section VI we give an Illustration and an example. Section VII concludes the paper.

II. The OLSR Protocol

The Optimized Link State Routing Protocol (OLSR)[1], is a proactive link routing protocol, designed specifically for mobile ad hoc networks. OLSR employs an optimized flooding mechanism to diffuse link state information to all nodes in the network. In this section, we will describe the element of OLSR, required for the purpose of investigation security issues.

A. *OLSR Control Traffic.*

Control traffic in OLSR is exchanged through two different types of messages.

1) *HELLO messages*

To detect its neighbors with which it has a direct link, each node, periodically and at regular intervals (*HELLO Interval seconds*) broadcasts hello messages, containing the list of neighbors known to the node and their link status (symmetric, asymmetric, Multi-Point Relay or Lost).These messages are broadcast by all nodes and heard only by immediate neighbors; they are never relayed any further, i.e. these packets have a *Time-To-Live (TTL)* value of 1.

In addition to information about neighbor nodes, the periodic exchange of HELLO messages allows each node to maintain information describing the link between neighbor nodes and nodes which are two hops away. Based on this information, each node independently selects its own set of Multi-Point Relay (MPR) among its one-hop neighbors so that the MPR covers all two-hop neighbors.

2) *Topology Control (TC) messages*

TC (Topology Control) messages are also broadcast by MPR-nodes in the network at regular intervals (*TC_Interval second*). Thus, a TC message contains the list of neighbors that have selected the sender node as a MPR (MPR Selector Set), and an *Advertized Neighbor Sequence Number* (*ANSN*) is used by a receiving node to verify if the information advertized in the TC messages is more recent. The TC messages are flooded to all nodes in the network and take advantage of Multi-Point Relay to reduce the number of retransmissions.

Using information of a TC message, a node generates topology tuples *(T_des_adr, T_last_adr, T_seq, T_time*), the set of these tuples is denoted the "Topology Set". Here *T_des_adr* is the destination address, *T_last_adr* is the address of the node that generated the TC message, *T_seq* is a sequence number of the TC message and the *T_time* is the time duration after which the topology tuple expires [1].

Based on the information in the topology set, the node calculates its routing table; each entry in the table consists of *R_des_adr*, *R_next_adr*, *R_dist*, and *R_iface_adr*.

Such entry specifies that the node identified by *R_dest_adr* is estimated to be *R_dist* hops away from the local node, that the symmetric neighbor node with interface address *R_next_adr* is the next hop node in the route to *R_des_adr*, and that this symmetric neighbor node is reached through the local interface with the address *R_iface_adr*. All entries are recorded in the routing table for each destination in the network for which a route is known [10].

B. *Multi-Point Relays Selection.*

Multi-Point Relays Selection is done in such a way that all the two-hop neighbors are reachable from the MPR in terms of radio range.

The two-hop neighbor set found by the exchange of HELLO messages is used to calculate the MPR set and the nodes signal their MPRs selections through the same mechanism.

The aim of Multi-Point Relays is to minimize the flooding of the network with broadcast packets by reducing duplicate retransmission in the same region Fig 1. Each node of the network selects the smallest set (MPRs) of neighbor nodes that can reach all of its symmetric two hop neighbors which may forward its messages. Each node in the network maintains an MPR selector set, which has selected this node as an MPR.

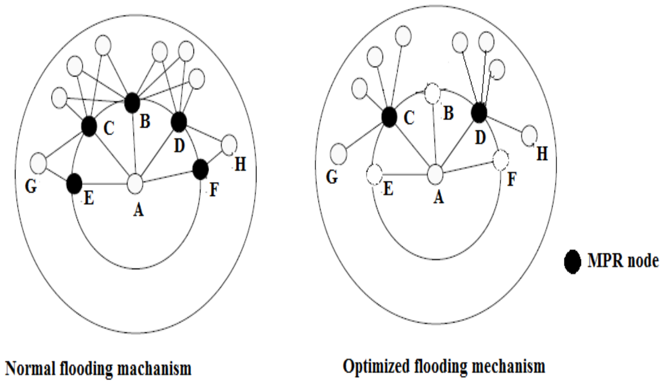

Fig. 1. Reduction of duplicate retransmission by MPR selection

III. The Model of Cooperative Attack Against OLSR Protocol.

In this section, we describe how malicious node can launch a cooperative black hole attack in MANET. The first step to launch the cooperative black hole attack is that a malicious node S1 can force its election as MPR by maintaining constantly its willingness field to Will_always in its HELLO messages. According to the protocol, its neighbors will always select it as MPR. Using this mechanism, a malicious node can easily earn, as an MPR, a privileged position within the network, it can then exploit its rank to carry out deny of service attacks and alike. The second step S1 select its adjacent node S2 as MPR, after this, S2 can drops all TC messages forwarded by node S1. The attacked node, in the set of MPR selectors of S1, cannot detect this misbehavior because node S2 is out of its radio range.

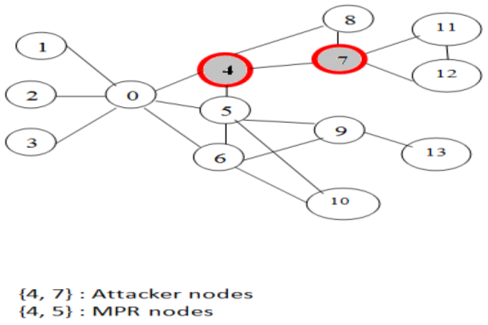

Fig. 2. A cooperative black hole attack model

Fig 2 shows an illustrative description of this cooperative black hole attack. Let {1,2,3} a set of nodes to be attacked and 4, 7 the attacker nodes, {4,5} the set of 0's MPR set nodes, {7,9} is the subset of 0's tow hop neighbors which constitutes the MPR set of nodes in 0's MPR set and {11,12,13} the set of 0's 3hop neighbors. The attack is launched as follows: node 4 sends its HELLO message with the value of willingness field as will_always, according to the protocol; all its one hop neighbors will choose it as an MPR. Then it chooses the node 7 as the only MPR node to relay its TC messages. By doing this if node 4 broadcast a TC message, then node 7 might be responsible to retransmit the message but may decide not to do so. In consequence, nodes {11,12} will never learn that the last hop to reach nodes {1,2,3} is node 0. The consequence of this attack is illustrated in Fig 3, where node C5, C6 and C7 can not build a route toward T's MPR selector because the 0's TC messages are never received (i.e. the topology information held by these nodes is incomplete).

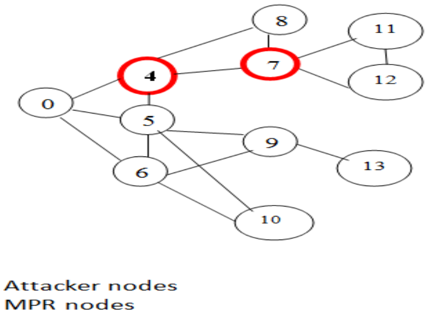

Fig. 3. Topology perceived by nodes 11, 12 after attack

IV. Related Work

In [2], to detect a collusion attack the authors propose to extend the HELLO messages by including the two-hop neighbours list. Based on this extension, a node can learn its tree-hop neighbours without the need of TC message. The aim of this method is that a target node can detect the contradiction due to the attack. Though the proposed method detects an attack, it cannot differentiate between an actual attack and topology changing.

In [4] the authors propose the theoretical information framework for trust modeling. The method uses special packets to request neighbouring nodes for calculating the trust value of other nodes in the network. After a certain threshold the nodes will be blacklisted. This method involves observation of the suspected attackers and requires cooperatives of neighbouring nodes to arrive at correct results.

In [8] the authors address the problem of collusion attack in OLSR using an acknowledgement (ACK) based mechanism to detect attackers, so this scheme has a considerable overhead induced by the extra control messages.

In [7] the author proposes a method to avoid a virtual link attack by using SNVP protocol based on the Principle of checking the symmetry of the link advertised by the neighbour before confirming it. The problem of the proposed solution is that it might not detect the misbehaving nodes that launch the proper attack.

A SU-OLSR[6] is a solution to detecting malicious attack that can use either HELLO messages claiming illegitimate neighbours or TC messages claiming falsely that is has been selected as MPR. In this method the authors extend the HELLO messages by listing the selected trusted MPR set and the discovered non trusted suspicious set. The MPR selection of SU-OLSR has a different goal. Its objective is to reduce the impact of malicious nodes trying to be selected as MPR nodes. Thus, the MPR selection algorithm has to find the non trusted nodes according to the selected criterion and the trusted MPR covering a maximum subset of two-hop neighbours.

In [3] the authors address another problem called Node Isolation Attack. In this attack, an MPR node does not generate its TC message. To defend against this attack the authors propose a countermeasure that consists of two phases: detection phase and avoidance phase. In the first phase the target observes its MPR node to check whether the MPR is generating TC message or not. In the second phase, to avoid the impact of this attack, the authors include in the HELLO message a new field named Requested-value.

In the suggested technique [9], when the node detects a symptom of collusion attack, it adds the lone MPR to an AvoidanceSet after waiting for AvoidanceDelay. All entries in the AvoidanceSet of X are not included in its MPRs computation process. Theses entries are removed from AvoidanceSet after duration AvoidanceOld. In addition the authors discuss two possible convergences of the attack. This method is simple but it affects a network performance by repeating the processes selection of MPR set in case of legitimate node.

In method [5], the authors present a scruple when a symptom is checked right. The node waits for a fixed duration and sends scruple packet. The inconvenience of this method is that it increases the overhead.

Sanjay Ramaswamy et al. exploit data routing information (DRI) table and cross checking method to identify the cooperative black hole nodes, and utilize modified AODV routing protocol to achieve this methodology [11].

Chang Wu Yu et al. propose a distributed and cooperative mechanism viz. DCM to solve the collaborative black hole attacks. Because the nodes works cooperatively, they can analyze, detect, mitigate multiple black hole attacks. The DCM is composed of four sub-modules [12].

Weichao Wang et al. design a hash based defending method to generate node behavioral which involve the data traffic information within the routing path. The developing mechanism is based on auditing technique for preventing collaborative packet drop attacks, such as collaborative black hole and grey hole problems [13].

Zhao Min and Zhou Jiliu propose two hash-based authentication mechanisms, the message authentication code (MAC) and the pseudo random function (PRF). These two proposals are submitted to provide fast message verification and group identification, find the collaborative suspicious hole nodes and discover the secure routing path to prevent cooperative black hole attacks [14].

Vishnu K. and Amos J. Paul address a mechanism to detect and remove the black and gray hole attack. This solution is able to find the collaborative malicious nodes which introduce massive packet drop percentage. Authors, refer this method to penetrate their system model, and also add a novel scheme videlicet restricted IP (RIP) to avoid collaborative black and gray attacks [15].

Po-Chun Tsou et al. design a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major essence is the DSR on-demand routing [16].

The main goal in this paper is to detect successfully and isolate the data packet dropping attackers from routing path in OLSR routing protocol for MANETs [17].

V. the Proposed Solution

To deal with cooperative black hole attack, we present an improved MPR selection algorithm which has a different goal; its objectif is to reduce the impact of malicious nodes trying to be selected as MPR nodes by maintaining constantly its willingness fields equal to will_always in the HELLO message. In order to limit the impact of this attack the following concept of trustworthiness is used: a node S should not trust any neighbor X showing strong characteristics which can maintain its willingness to will_always and $|$MPR_set(X)$|$=1.

In [1] the standard way of selecting MPR set, start with an MPR set made of all members of node with willingness equal to will_always, then it select as a MPR the node with highest willingness among the nodes in its one hop neighbor with non zero reachability (the number of nodes in two hop neighbor which are not yet covered by at least one node in the MPR set, and which are reachable through this one hop neighbor). In our algorithm we give priority to a node that covers maximum nodes in two hop neighbors without giving priority to node with highest willingness.

Before introducing this algorithm, some notations should be described first:

- 1HN_set(X): the set of node X's one hop symmetric neighbors. It is created by the way of changing HELLO messages between nodes.
- 2HN_set(X): the set of node X's two hop symmetric neighbors excluding any node in 1HN_set(X). It is also created by the way of changing HELLO messages.
- Degree (X ,Y): the degree of node X's one hop neighbor; returns the number of nodes in 2HN_set(X) such that {2HN_set(X) ∩ 1HN_set(Y) ≠ Ø } assuming that Y ∈ 1HN_set(X).
- Reachability(X,Y): the number of nodes in 2HN_set(X) which are not yet covered by at least one node in the MPR_set(X), and which are reachable through node Y
- MPR_set (X): the set of nodes selected as MPR by the node E. (MPR_set (X) ⊆ 1HN_set (X)).
- MPRS_set (X): the set of symmetric neighbours which have selected the node X as MPR. (MPRS_set (X) ⊆ 1HN_set (X)).
- Isolate_set: A subset of 2NH_set(X) which are covered by only node in 1NH_set(X).

Our proposed algorithm for selection of MPRs, constructs an MPR_set that enable a node to reach any node in the symmetrical strict 2_hop neighborhood through relaying by one MPR node without giving opportunity to node with willingness equal to will_always.

The proposed heuristic for selecting MPRs is then as follows:

1) Calculate degree of each node in one hop neighbor of X

2) Select as MPRs those nodes in one hop neighbor which cover the isolate nodes in two hop neighbor.

3) We remove the isolate nodes from two hop neighbor set for the rest of the computation.

While there exist nodes in two hop neighbor which are not covered by at least k nodes in the MPR set.

- Calculate the reachability of each node in 1HN_set(X) node in MPR_set(X).
- For each node in 1HN_set(X), calculate the reachability, i.e., the number of nodes in 2HN_set(X) which are not yet covered by at least one node in the MPR set, and which are reachable through this 1-hop neighbor.
- Select as a MPR the node with lower willingness among the nodes in 1HN_set(X) with non-zero reachability. In case of multiple choice select the node which provides reachability to the maximum number of nodes in 2HN_set(X),. In case of multiple nodes providing the same amount of reachability, select the node as MPR whose D(y) is greater.
- Eliminate all the nodes in 2HN_set(X) now covered by at least one node in the MPR_set.

Algorithm 1: MPR Selection

```
1HN*_set(X) ← 1HN_set(X)
2HN*_set(X) ← 2HN_set(X)
MPR_set (x) ← Ø
S1← Ø
S2← Ø
For all node Y ∈ 1HN_set(X) do
 Degree(X,Y)←│ 1HN_set(Y) \ 1HN_set(X) \ {X,Y}│
End.
 While (∃ Z: Z ∈ 2HN*_set(X) ∩ ∃! Y ∈ 1HN*_set(X): Z ∈ 1HN_set(Y)) do
      MPR_set(X) ← MPR_set(X) ←{Y}
      1HN*_set(X) ← 1HN*_set(X) \ {Y}
      2HN*_set(X) ← 2HN*_set(X) \ 1HN_set(Y)
End.
While (2HN*_set(X) ≠ Ø) do
   For each Y ∈ 1HN*_set(X) do
   Reachability(X, Y) ←│ {F / F ∈ 2HN*_set(X) ∩ 1HN_set(Y) and MPR_set(X) ∩ 1HN_set(F) = Ø } │
   End.
   For each Y ∈ 1HN*_set(X)  with reachability(X,Y) ≠0 do
      S1← {Y/ Willingness = min (willingness(Y))}
   End.
  If │S1│=1 then
                 MPR_set(X) ← MPR_set(X) ←{Y}
                 1HN*_set(X) ← 1HN*_set(X) \ {Y}
                 2HN*_set(X) ← 2HN*_set(X) \ 1HN_set(Y)
 Else
         S2← { Y/  Reachability (X,Y)= max (Reachability (X,Y), Y ∈ 1HN*_set(X)  )}
          If │S2│=1 then
                        MPR_set(X) ← MPR_set(X) ←{Y}
                        1HN*_set(X) ← 1HN*_set(X) \ {Y}
                        2HN*_set(X) ← 2HN*_set(X) \ 1HN_set(Y)
         Else
                MPR_set(X) ← MPR_set(X) ←{Y/ Degree(X,Y) = max { Degree (X,Y), Y ∈ 1HN*_set(X)}
                1HN*_set(X) ← 1HN*_set(X) \ {Y}
                2HN*_set(X) ← 2HN*_set(X) \ 1HN_set(Y)
        End if
  End if
END.
```

Algorithm 1, start with an empty Multipoint Relay Set, select those one-hop neighbor nodes in 1HN_set(X) as MPR which are the only neighbor of some nodes in 2HN_set(X) with willingness different to will_never which covers a nodes in isolate_set, and add these one-hop neighbor nodes to the multipoint relay set of X. Then if there are still some node in two-hop neighbors set which is not covered by the multipoint relay set, select the one-hop neighbors with lower willingness and who could cover the most uncovered two hop neighbor as MPRs and which has de maximum degree. Repeat this step until all the two-hop neighbors are covered by MPRs.

As soon as node X receives a HELLO message from its MPR node Y which showing the same characteristics of attacker node (Y_willingess = will_always and |MPR(Z)| = 1), it recalculates its MPR set without it. Otherwise, if Y has more than one MPR neighbor node, X will process HELLO message normally (Algorithm 2).

Algorithm 2 :HELLO reception

```
If orig_adr_willigness = Will_always and orig_adr ∈ MPR_set
(receiver_adr)   then
      If |MPR(orig_adr)| = 1 then
          If |1HN_set(orig_adr)| ≠ 1 then
                  Recalculate MPR_set (receiver_adr) without orig_adr
                  Drops Hello message
          Else    Process HELLO message
      Else        Process HELLO message
      Endif
     Else          Process HELLO message
  Endif
 END.
```

Based on the information in the topology set, the node calculates its routing table by application of this algorithm which discard the node with high Willingness to reash the two hop neighbor:

1) All the entries from the routing table are removed.

2) The new routing entries are added starting with the symmetric neighbors (h=1) as the destination nodes.

3) For each node in N2 create a new entry in the routing table:

N2 is the set of 2-hop neighbors reachable from this node, excluding:

- The nodes only reachable by members of 1HN_set with willingness equal to WILL_Always.
- The node performing the computation.
- All the symmetric neighbors: the nodes for which there exists a symmetric link to this node on some interface.

4) For each topology entry in the topology table, if its T_dest_addr does not correspond to R_dest_addr of any route entry in the routing table AND its T_last_addr corresponds to R_dest_addr of a route entry whose R_dist is equal to h, then a new route entry MUST be recorded in the routing table:

- R_dest_addr = T_dest_addr
- R_next_addr = R_next_addr of the entry with (R_dest_addr = T_last_addr)
- R_dist = h+1

VI. Illustrative Example.

To understand the mechanism of our solution, we present a schema which shows an example of MANET (Fig. 4). Table 1 represents the nodes in one hop neighbors of E and their Willingnesses.

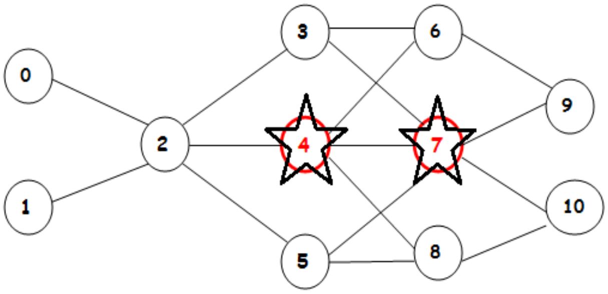

Fig. 4. Example of cooperative black hole attack model: {0,1} Target nodes and {4,7} a cooperative black hole attakers nodes.

TABLE I. Willingnesses of Nodes in 1NH_Set (2)

Nodes	Willingnesse
3	3
4	7
5	3

The statement of our algorithm is as following:

- Calculating the degree of each node in 1HN_set (2): degree = {3 (2), 4 (3), 5 (2)}.
- Adds to the MPR_set (2) those nodes in 1HN_set(2), which are the only nodes to provide reachability to a node in 2HN_set(2); isolate_nodes = {Ø} then MPR_set(2) = {Ø} and $2HN^*$_set(2)= $2HN^*$_set(2) \ {Ø} = { 6,7,8 }.
- Since, as $2HN^*$_set (2) = { 6,7,8 } ≠ Ø, the algorithm proceeds by calculating the reachability of nodes in $1HN^*$_set (2): reachability (3) = 2, reachability (4) = 3, reachability (5) = 2. Then it adds nodes 3 and 5 to the MPR_set (2) because willingness of 4 is equal to will_always and removes 1HN_set (3,8) from 2HN_set (2).
- Finally, we have $2HN^*$_set (2) = Ø then the algorithm return MPR_set (2) = {3,5} (Fig 5).

Suppose now, that (4,7) a cooperative black hole attacks. By the application of our approach, 4 will never be selected as MPR, because it has a high willingness and there exist other nodes with lower willingness which covers all nodes in to hop neighbors. After this when the first attacker 4 lunch the attack by selecting node 7 as its MPR node, it sends a HELLO message to a node 2. This last detects that 4 shows strong characteristics of malicious node, then it will recalculate the MPR_set (2) without 4, this operations will have result as 2 will choose {3,5} as its MPR to cover {9,10}.

In general our approach not favors nodes that have a Willingness equal to Will_always to the other nodes (Fig. 5). Otherwise, if we use the standard way of selecting MPRs [1], node 4 will be selected as multipoint relays (Fig. 6), which means the convergence of cooperatives attacks. The consequently of the attacks is that node 9,1,0 can not build a route toward 2's MPR selectors because the 2's TC messages are never received.

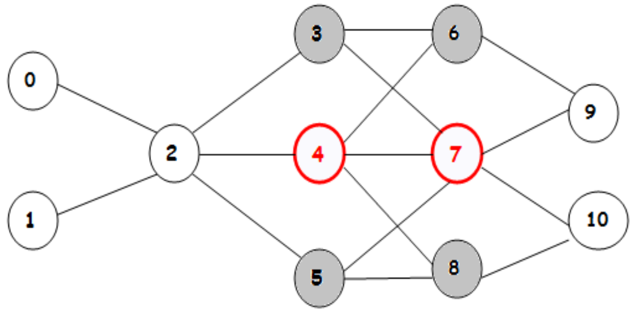

Fig. 5. An Example of selecting MPRs using Algorithm 1.MPR_set(2) = {3,5}.

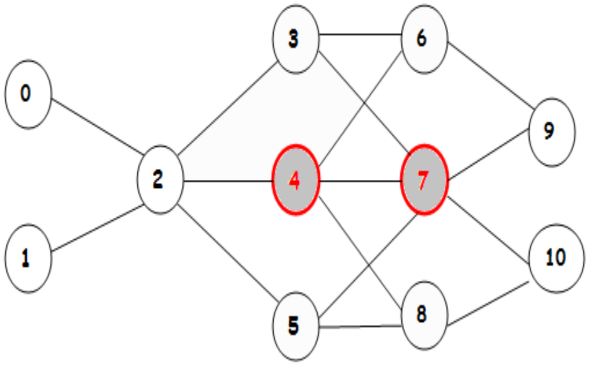

Fig. 6. An Example of selecting MPRs using standard OLSR..MPR_set(2) = {4}.

VII. Simulation and Results

To test the effectiveness of our solution, simulations were implemented using network simulator NS-2.35 with modified version of the UM-OLSR implementation. We embedded our scheme in implemented OLSR protocol for the detection of the cooperative black hole attack. All the default values for the OLSR protocol from [1] were used. The simulations were performed for 20 to100 nodes with a transmission range of 250 meters, in an area of size 1000*1000 meters during 150 seconds. Random waypoint model is used as the mobility model of each node. Nodes speed is varied from 0m/s to 10 m/s. A single source generate UDP packets to the target (that has a distance further than two hops away) from 10th second. To launch the attack, the first attacker chooses a victim node from its MPR selector set that has to be an MPR of the other neighbors at the 20th second (Table 2).

TABLE II. Simulation Parameter

Parameter	Values
Connection type	CBR/UDP
Simulation area	1000*1000
Transmission Range	250 m
Packet size	512 bytes
Number of Nodes	20-40-60-80-100
Duration	150 s
Pause time	0 s
CBR_Start	10s
Attack_start	20s

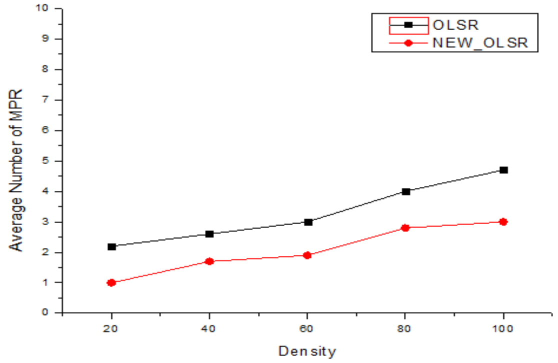

Fig. 7. Average number of MPR versus Density

Fig 7 gives the average number of MPR nodes selected by OLSR and New_OLSR for different densities (50% of nodes are willingness equal to 7). We can see that density clearly affects the number of MPR node selected by both protocols. It increases when density is increased and the number of MPR nodes selected by New_OLSR is low than the number selected by OLSR. The reason is that our algorithm of selection don't gives priority to a node with Willingness equal to Will_always but select as MPR the nodes that covers maximum nodes in its two hop neighbors with lower willingness.

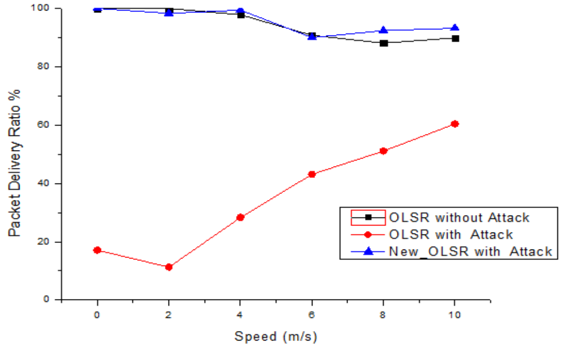

Fig. 8. PDR versus Speed under different scenarios

We also define the packet delivery ratio (PDR) as a value of the number of received data packets to that of packets being sent by the source node. Fig 8 compares OLSR and our approach New-OLSR. We observe that in presence of the attack, the PDR in OLSR is very low, the only packets received by the node are before launching the attack and we see that the PDR increase when the speed of the node increases. On the other hand when the New-OLSR is under attack we see that, generally. PDR is stable (minimum value equal to 90%) and better than the OLSR performance without attack. This is due to our approach route calculation, eliminating nodes with symptoms of malicious nodes routes to the destination node.

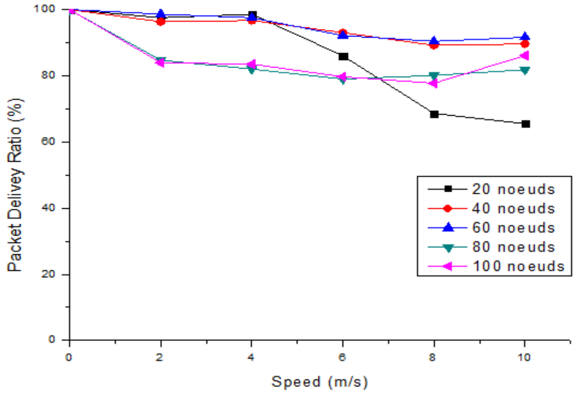

Fig. 9. Packet Delivery ratio under different number of nodes.

Fig 9, shows the relationship between Packet Delivery Ratio and speed. Generally the PDR decreases slightly with increasing velocity. Firstly with increasing speed in the case of 20 nodes the PDR does not exceed 65.5%. This is because the target has no choice in its one hop neighbor to select its MPR nodes. Secondly in case (80,100) we notice a slight decrease which exceeds 80%. Finally, for the case (40 and 60) a similar behavior can be seen with a reduction not exceeding 90%.

Fig 10 shows how our strategy offers a higher prevention to mitigate the effect of cooperative black hole attack. The percentage of detection rate is 100 % in static network, we observe an increase of detection rate in the case of large density.

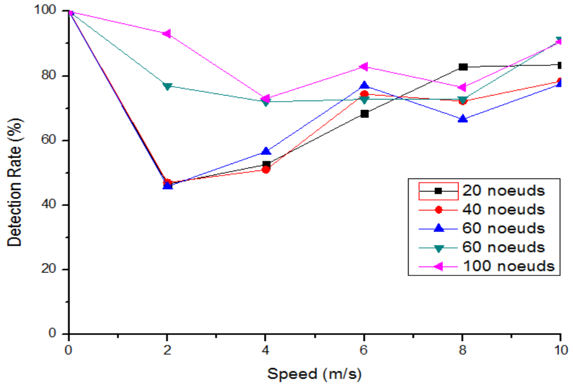

Fig. 10. Detection rate when changing mobility of nodes and a number of nodes.

VIII. Conclusion

The cooperative black hole attack exploits the routing protocol's vulnerabilities by forcing its election as Multipoint relay by maintaining constantly its willingness field to will_always in its HELLO message.

In order to deal with this sophisticated attack, we have proposed a novel approach to select MPR nodes. This gives priority to a node that covers maximum nodes in two hop neighbors with lower willingness which not showing strong characteristics to influence the MPR selection to be selected as MPR. We modified the procedure of calculating routes through the elimination the node with high Willingness to reach the two hop neighbor.

Simulation results demonstrate that the proposed method is effective in struggling cooperative black hole attack. It shows high packet delivery ratio and high detection rate of malicious nodes.

References

[1] T.Clausen, P. Jaquet, IETF Request for Comments: 3626 Optimized Link State Routing Protocol OLSR, october 2003.

[2] A. Jamalipour B. Kannhavong, H. Nakayama.A collusion attack against OLSR-based mobile ad hoc networks. In Global Telecommunications Conference, GLOBECOM '06. IEEE, pages 1--5, November 2006.

[3] Bounpadith Kannhavong , Hidehisa Nakayama , Nei Kato , Abbas Jamalipour , Yoshiaki Nemoto, A study of a routing attack in OLSR-based mobile ad hoc networks, International Journal of Communication Systems, v.20 n.11, p.1245-1261, November 2007.

[4] Kishore Babu Madasu, A. Antony Franklin, and C. Siva Ram Murthy. On the Prevention of Collusion Attack in OLSR-based Mobile Ad hoc Networks. In IEEE International Conference on Networks (ICON 2008), New Delhi, India, December 2008.

[5] Lalith Suresh P, Rajbir kaur, Manoj Singh Gaur, Vijay Laxmi. A collusion attack detection method for OLSR-based MANETS employing scruple packets. the 3rd international conference on Security of information and networks. 2010.

[6] Rachid abdellaoui and Jean Marc Robert. SU-OLSR : A new solution to thwart attacks against the olsr protocol. Mster thesis.Height school of technology (ETS) Canada. 2009.

[7] Soufian Djahel, Farid Nait Abslam, Avoiding virtual link attack in wireless ad hoc networks, Proceeding of the 2008 IEEE/ACS Internetional conference of computer systems and application, p 355-360. March 31 avril 04, 2008.

[8] Soufiene Djahel, Farid Naït-Abdesselam, Zonghua Zhang, and Ashfaq Khokhar. Defending against packet dropping attack in vehicular ad hoc networks. Security and Communication Networks, 1(3):245--258, 2008.

[9] Suresh, P.L.; Kaur, R.; Gaur, M.S.; Laxmi, V.Collusion attack resistance through forced MPR switching in OLSR. Wireless Day IFIP 2010. Venice. Italy.

[10] C.Adjih, A.Laouiti, P.Minet, P.Muhlethan, A. Quayyum, L.Viennot. The Optimized Routing Protocol for Mobile ad hoc Networks: Protocol Specification. Projet HIPERCOM.INRIA research report N° 5145, March 2004.

[11] Weerasinghe H, Fu H (2007) Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007.

[12] Yu CW, Wu T-K, Cheng RH, Chang SC (2007) A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007.

[13] Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009.

[14] Min Z, Jiliu Z (2009) Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks. Paper presented at the International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16-17 May 2009

[15] Vishnu KA, Paul J (2010) Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks. International Journal of Computer Applications 1(22):38–42. doi: 10.5120/445-679.

[16] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L (2011) Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs. Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011.

[17] Ahmed Mohamed Abdalla, Ahmad H. Almazeed, Imane Aly Saroit, Amira Kotb, Detection and Isolation of Packet Dropping Attacker in MANETs. International Journal of Advanced Computer Science and Applications,Vol. 4, No.4, 2013.