Securing Data from collusion Black Hole Attack Using Optimized Link Source Routing Protocol for MANET

H. Zougagh[1], A.Toumanari[1], R. Latif[1], N. Idboufker[2]

[1]Universityn IBN ZOHR, E.S.S.I Laboratory
ENSA Agadir, Morocco

[2]Universityn Caddi Ayyad, T.I.M Laboratory
ENSA Marrakech, Morocco

Abstarct

In this paper a new algorithm for the selection of multipoint relays (MPR) in optimized link state routing protocol (OLSR) is proposed. OLSR is a routing protocol which could reduce the overhead of control messages by selecting MPRs. So, the number of MPRs is a key for the performance of OLSR. However, as the greedy algorithm introduced in RFC 3626 has some problems with MPR selection, which will make a negative effect on the security performance of OLSR. In fact, the OLSR is known to be vulnerable to various kinds of malicious attacks. This paper proposes a collusion 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, colluding attack.*

1. Introduction

Along with the proliferation of mobile devices and advances in wireless communication technologies, mobile ad hoc networks (MANETs) have been attracting tremendous attention from the networking research and industry community. A MANET is a collection of mobile devices which are connected by wireless links without the use of any fixed infrastructures or centralized access points. In MANET, each node acts not only as a host and but also as a repeater to forward messages for other nodes that are not within the same direct wireless transmission range. Nodes in MANET are free to move and form a dynamic and random topology. MANET can be constructed in situation where infrastructure does not exist, or when deployment of infrastructure is inconvenient or expensive. These inherent flexibilities make MANET attractive for wide range of applications such as emergency operation, disaster relief, maritime communication, military operation or police network, casual meeting network, vehicle-to-vehicle network, robot network, sensor network and so on.

Unlike the conventional wireless networks, MANET has the unique features such as having an open medium, dynamic topology, lacking of a centralized administration, and being bandwidth- and energy-constrained. These inherent features make it difficult to apply security mechanisms similar to that of in wireless network with complex backbone infrastructure network. As a result, MANETs are much more vulnerable and are susceptible to various kinds of security attacks. Typical attacks against MANET includes passive eavesdropping, location disclosure, unauthorized modification, impersonation, jamming, routing disruption, resource consumption and denial-of-service (DoS) attack. In MANET, a malicious node can launch some of these attacks easily by exploiting the flaws in routing protocol [19].

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 collusion attack [2] where two nodes collude 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 pretending that it is connected to all two-hop neighbors of the target's node, 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 algorithms that can ensure the validity of the information contained in HELLO message and assure that the message generated by the node can be successfully received by all its two hop neighbor set.

The rest of the paper is organized as follows. The next section provides a short overview on OLSR, followed by the description of collusion 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.

2. The OLSR Protocol

Optimized link state routing (OLSR) [1] is one of the most important proactive routing protocols designed for MANET. It employs periodic exchange of messages to maintain topology information of the network at each node. The key concept of OLSR is the use of multipoint relay (MPR) to provide efficient flooding mechanism by reducing the number of transmissions required. In this section, we will describe the element of OLSR, required for the purpose of investigation security issues.

2.1. OLSR Control Traffic.

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

2.1.1. 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.

2.1.2. 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].

2.1.2. Multi-Point Relays Selection.

In OLSR, each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes who have been selected as an MPR. This list is called MPR selector list. Only nodes selected as MPR nodes are responsible for advertising as well as forwarding MPR selector list advertised by other MPRs. Figure 1 illustrates a node broadcast its messages throughout the network using standard flooding (Figure 1(a)) where all neighbors relay message transmitted by the leftmost node and MPR flooding (Figure 1(b)) where only MPR nodes relay the message. The protocol is best suitable for large and dense network as the technique of MPRs works well in this context.

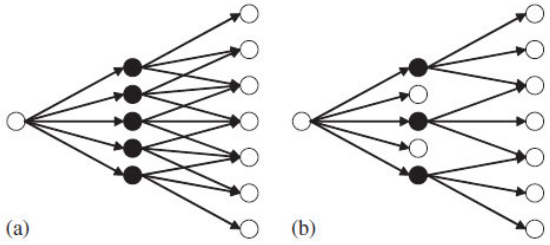

Fig 1. Reduction of duplicate retransmission by MPR selection

3. The Model of Collusion Attack against OLSR Protocol.

In the collusion attack, two nodes work together to prevent the node from being established in the network by declaring an incorrect set of neighbors. A misbehaving node advertising a neighbor relationship to non-neighbor nodes in its HELLO messages may cause inaccurate MPR selection. Thus the necessary condition for the attack is that misbehaving node be MPR node.

Consider the network in (Fig 2). Let 3 and 12 are the first and second colluding nodes, and 1 is the target node. Firstly, the node 3 sends to 1 a Hello message containing all two-hop neighbouring nodes {10,11,12,13,4,15,16,17,18,19,20,21} (node 3 can easily learn of the 1's two-hop neighborhood using information in its topology set). According to the protocol OLSR, node 3 will be chosen as the 1's only MPR. After being selected as an MPR node for 1, the first attacker 3 chooses 12 as its own MPR node. Therefore, 3 will be the only node that can forward TC message generated by node 1. These

TC messages are dropped by 12 the second attacker. The collusion attack will result in the network containing no topology tuple with information regarding 1. Fig 3 shows how all nodes beyond 1's three-hop neighborhood will not be able to build a route to the arget.

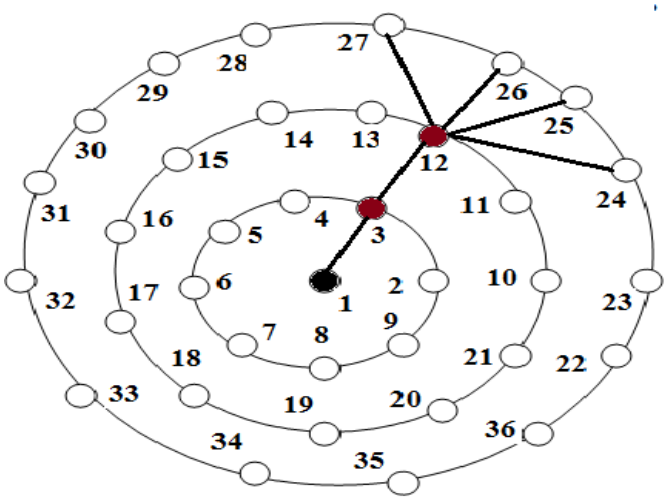

Fig .2. MANET example; node 1 is the target, node 3 and 12 are colluding attackers.

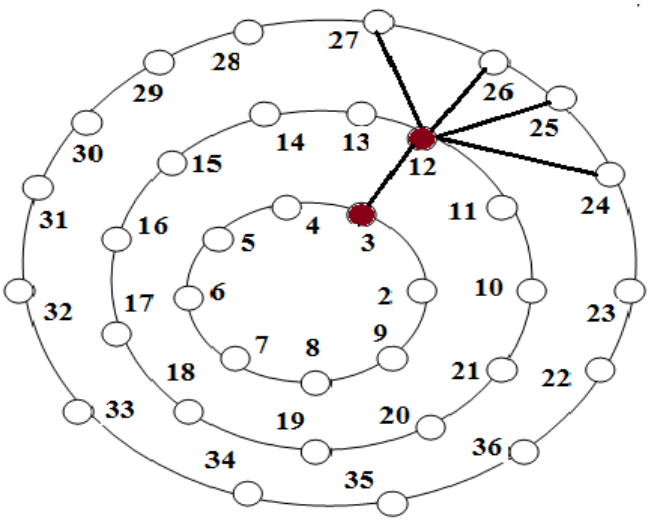

Fig 3. Topology perceived by three-hop neighbourhood of target node [22…..36] after attack.

4. 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 [13].

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 [14].

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 [15].

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 [16].

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 [17].

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 [18].

5. The Proposed Solution

In the collusion attack the first attacker Y creates fake link to make the target choose it as only MPR, while the second attacker drops all TC packets generated by a target node and relayed by Y. to deal with this problem, we present algorithms that can ensure the validity of the information contained in the HELLO message.

Our scheme introduces the following concept of trustworthiness: a node S should not trust any neighbor X showing strong characteristics which can maintain its willingness to will_always and $|MPR\_set(X)|=1$. ($2HN\_set(receiver\_addr) \subseteq 1HN\_set(orig\_addr)$).

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.

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.

.

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 1HN_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 2 : Routing Table Calculation

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

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 2HN_set(receiver_addr) ⊆ 1HN_set(orig_addr), it recalculates its MPR set without it. Otherwise, if Y has more than one MPR neighbor node, X will process HELLO message normally.

Based on the information in the topology set, the node calculates its routing table by application of this algorithm which discards the node with high Willingness to reach the two hop neighbor (algorithm 2).

6. Illustration Example

To understand how the algorithm works we consider Fig 4, that illustrates the colluding attack. The first attacker node 3 sends a HELLO message to the target node 0 advertizing that it has direct links with 0's all 2-hops neighbors and one unique extra link according to the protocol. The target node 0 will choose node 3 as its only MPR. Therefore, all TC traffic generated/forwarded from 0 will be routed through node 3 only. 3 then chooses the second attacker 8 as its only MPR. By so doing, node 8 can drop or modify packets generated by a target node 0.

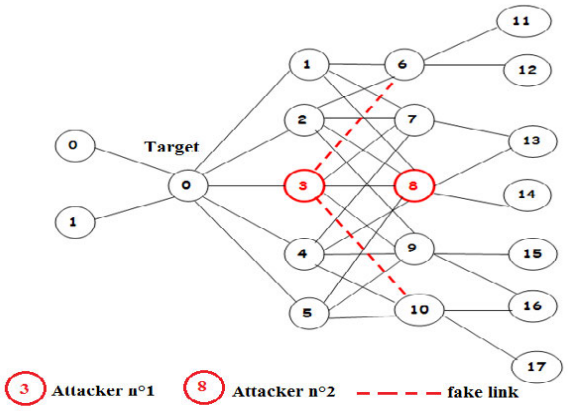

Fig. 4. Example of colluding attack model

Table 1: Willingnesses of nodes in 1NH_set (E)

Nodes	Willingnesse
1	3
2	**3**
3	**7**
4	3
5	3

The statement of our algorithm is as following:

- Calculating the degree of each node in 1HN_set (0): degree = {1 (3), 2 (4), 3 (3), 4(4),5(3)}.
- Adds to the MPR_set (0) those nodes in 1HN_set(0), which are the only nodes to provide reachability to a node in 2HN_set(0); isolate_nodes = {Ø} then MPR_set(0) = {Ø} and $2HN^*$_set(0)= $2HN^*$_set(0) \ {Ø} = { 6,7,8,9,10}.
- Since, as $2HN^*$_set (0) = { 6,7,8,9,10 } ≠ Ø, the algorithm proceeds by calculating the reachability of nodes in $1HN^*$_set (0): reachability (1) = 3, reachability (2) = 4, reachability (3) = 3, reachability (4) = 4, reachability (8) = 3. Then it adds node 2 to the MPR_set(0), because it has a minimum value of Willingness and a maximum reachability.
- Removes node 2 from $1HN^*$_set (0) and 1HN_set (2) from $2HN^*$_set (0): $1HN^*$_set (0)={1,3,4,5}, $2HN^*$_set (0)={10}.
- Reacahbility (1) =0, Reacahbility (3) =0, Reacahbility (4) =1, Reacahbility (5) =1.
- Nodes 4 and 5 have the same willingness = 3 and the same reachability = 1, our approach will select node 4 as MPR because it has a maximum degree.
- Finally, we have $2HN^*$_set (0) = Ø then the algorithm return MPR_set (0) = {2,4} (Fig 5).

Suppose now, that (3,8) a colluding black hole attacks. By the application of our approach, 3 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 3 lunch the attack by selecting node 8 as its MPR node, it sends a HELLO message to a node 0. This last detects that 3 shows strong characteristics of malicious node, then it will will choose {2,4} as its MPR to cover {6,7,8,9,10}.

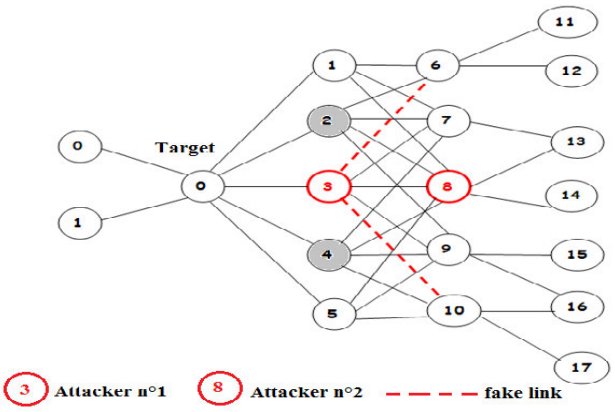

Fig 5: An Example of selecting MPRs using Algorithm 1. MPR_set(2) = {2,4}.

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 3 will be selected as multipoint relays (Fig. 6), which means the convergence of cooperatives attacks. The consequently of the attacks is that node {11,12,13,14,15,16,17} can not build a route toward 0's MPR selectors because the 0's TC messages are never received.

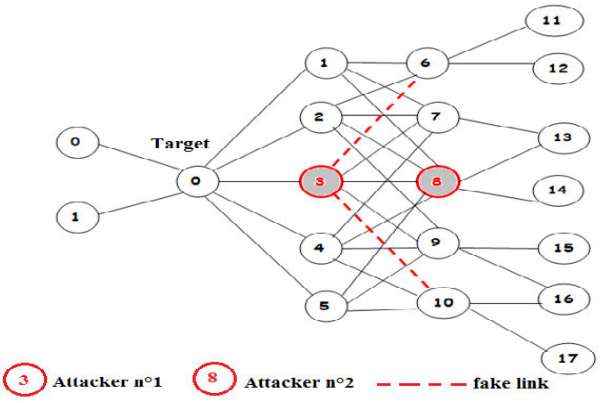

Fig 6: Example of selecting MPRs using standard OLSR. MPR_set(0) = {3}.

7. Simulation and Results

To test the effectiveness of our solution, simulations were implemented using network simulator NS2 with modified version of the UM-OLSR implementation. We embedded our scheme in implemented OLSR protocol for the detection of the collusion attack. All the default values for the OLSR protocol from [1] were used (Table 2). The simulations were performed for 20 to 100 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 0 m/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 3).

Table 2: OLSR parameter

Parameter	Values
TC interval	5 s
HELLO interval	2 s
Refresh Timout Interval	2 s
Neighbor hold time	6 s
Topology hold time	15 s
Duplicate hold time	30 s

Table 3: 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

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 [12].

Fig 9 compares OLSR and our solution 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, the PDR is equal to 100% for all values of speed.the reason is that, our method uses a preventive approach. Ie. It does not allow the attackers nodes to be elected as MPRs nodes for converging attack.

Fig10 shows the variation in PDR versus speed of the nodes for different values of density. In the case of New-OLSR and the network under attack we see that the PDR decrease when the speed of nodes increases and when the density increase.

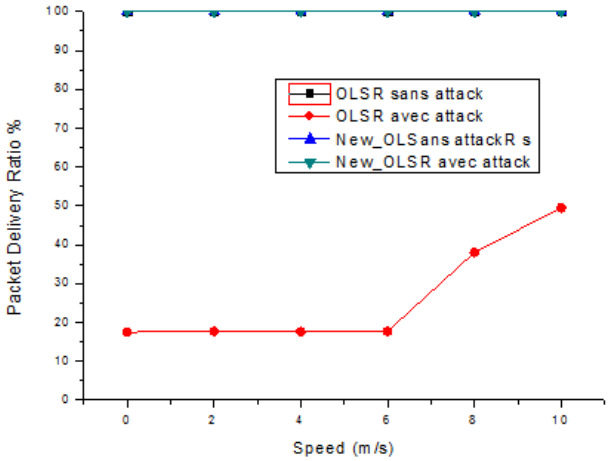

Fig 9: PDR versus Speed under different scenarios.

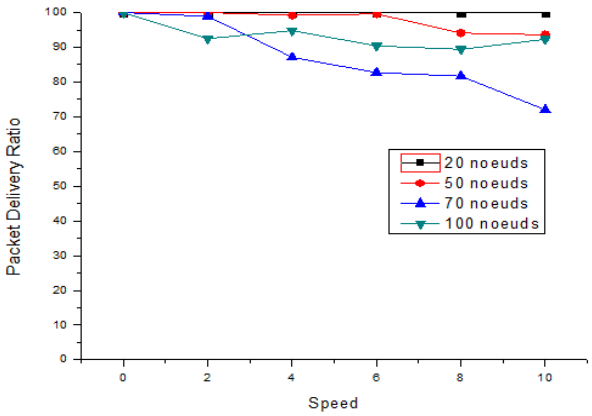

Fig 10: PDR versus Speed for different values of timer T when target is under attack.

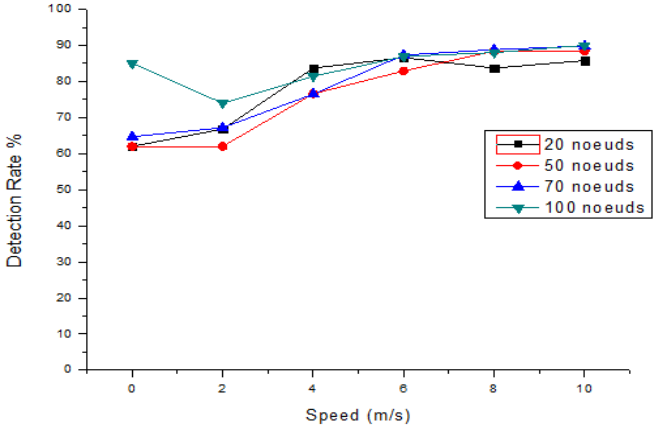

Fig 11: Detection Rate under different number of nodes.

The detection rate is calculated as the percentage of nodes detected attack among all nodes in the one hops neighbor of the second attacker node. We vary the number of nodes from

20 to 100 in order to study the impact of density on detection rate. (fig 11) shows the results. We notice that the detection rate increases as node density grows. Also, it gives more detection with maximal speed. because the target node will have several alternatives to choose its MPR nodes.

VIII. Conclusion

The collusion 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 collusion 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 Naŕt-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] Bounpadith Kannhavong, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto. A study of a routing attack in OLSR-based mobile ad hoc networks. Int. J. Commun. Syst. Volume 20, Issue 11, pages 1245–1261, November 2007.

[12] Kun Yu, Sanyue Bu. Promote Cooperation to Forward Packets in Multi-Hop Wireless Networks, Routing. International Review on Computers and Software, Vol. 7 N. 5 (Part B), pp. 2360-2366, September 2012.

[13] 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.

[14] 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.

[15] 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

[16] 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

[17] 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.

[18] Aishwarya Sagar Anand Ukey, Meenu Chawla, Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET. International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010.

[19] Fasee Ullah, Waqas Tariq, Muhammad Arshad, Muhammad Saqib, Noor Gul. Analysis of Security Techniques for Detecting Suspicious Activities and Intrusion Detection in Network Traffic. International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.