Mitigating Black Hole attack in MANET by Extending Network Knowledge

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

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

***Abstract*—The Optimized Link State Routing Protocol is developed for Mobile Ad Hoc Network. It operates as a table driven, proactive protocol. The core of the OLSR protocol is the selection of Multipoint Relays (MPRs), used as a flooding mechanism for distributing control traffic messages in the network, and reducing the redundancy in the flooding process. A node in an OLSR network selects its MPR set so that all two hop neighbor are reachable by the minimum number of MPR. However, if an MPR misbehaves during the execution of the protocol, the connectivity of the network is compromised. This paper introduces a new algorithm for the selection of Multipoint Relays (MPR) with additional coverage whose aims is to provide each node to selects alternative paths to reach any destination two hops away. This technique helps avoid the effect of malicious attacks and its easily to implement the corresponding algorithm.**

Keywords—MANET; OLSR; Security; Routing Protocol; Black Hole attack

I. INTRODUCTION

Today, mobile Ad-hoc networks (MANETs) are a major element of the business environment, allowing wireless devices such as cell phones, laptops, and PDAs to provide mobility to users and enable them to be in constant contact with others. Technically. Mobile Ad hoc Networks (MANET) are dynamic and self-organized networks that are able to operate without an dependability on fixed or pre-installed infrastructure, using only wireless devices that act both as hosts and routers, and thus cooperatively provide multi-hop communications [1]. Because of these characteristics, MANETs are much more vulnerable to several types of security attacks.

The communication in mobile ad hoc networks comprises two phases: the route discovery and the data transmission. In an adverse environment, both phases are vulnerable to a variety of attacks. First, rivals can disrupt the route discovery by impersonating the destination, and responding with stale or corrupted routing information, or by disseminating forged control traffic. This way, attackers can obstruct the propagation of legitimate route control traffic and adversely influence the topological knowledge of benign nodes.

However, adversaries can also disrupt the data transmission phase and, thus, cause significant data loss by fraudulently tampering, redirecting and dropping data or injecting forgets data packets. To provide comprehensive security, both phases of MANET communication must be safeguarded. It is noteworthy that secure routing protocols, which ensure the correctness of the discovered topology information cannot, by themselves, ensure the secure and undisrupted delivery of transmitted data [2].

One way to secure a mobile ad hoc network at the network layer is to secure the routing protocols, in order to prevent possible attacks. In brief the 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 so as to construct routes.

Routing in MANET can be classified into three categories: reactive protocol (e.g. AODV [3], DSR [4]), proactive protocol (e.g. optimized link state routing (OLSR) [5], TBRPF [6]), and hybrid protocol (e,g, ZRP [7]). Early works in MANET security research (e.g. ARAN [8], Aridane [9], SAODV [10,11], SEAD [12], [13–14]) have focused on providing preventive schemes to protect the routing protocol in MANET. Most of these schemes are based on key management or encryption techniques to prevent unauthorized nodes from joining the network.

However, these approaches cannot prevent attacks launched by a compromised node who owns a valid key. Therefore, intrusion detection and response system are required to counter the attack as a second line of protection. To design an effective and efficient intrusion detection and reaction system, in-depth understanding of how a compromised node can attack a MANET is indispensable.

The Optimized Link Stat Routing Protocol (OLSR) [5] 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 Black hole attack...). As a result, it is also necessary to provide security scheme for the OLSR protocol.

In this paper, we focus on the single black hole attack in which an intermediate node drops packets passing through it. The motivation of the dropper node is the preservation of its resources, such as its limited battery, while at the same time using the resources of others to deliver its data. In our approach, 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 Single 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 presents the result of simulations. Section VIII concludes the paper. In the end section XI present the futur work.

II. THE OLSR PROTOCOL

Optimized Link State Routing Protocol (OLSR) [5] is a routing protocol developed for mobile ad hoc networks (MANETs), it is a proactive routing protocol that employs an efficient link state packet forwarding a mechanism called Multipoint relaying. OLSR optimizes the pure link state routing protocol. Conceptually OLSR topology discovery involves tow phases: neighbor discovery and topology discovery. In the first phase, neighbor nodes are discovered by using Hello messages. The exchange of Hello messages in OLSR allows the selection of those MPR nodes. MPR nodes are responsible for broadcasting topology control (TC) message which would be flooded through the network in the second phase.

A. OLSR Control Traffic.

A node detects its one hop and two hop neighbors through link sensing which is accomplished though broadcasting periodic Hello messages containing neighbor link state (sym, asym, MPR or lost). Fig. 1 shows the basic information of a Hello message.

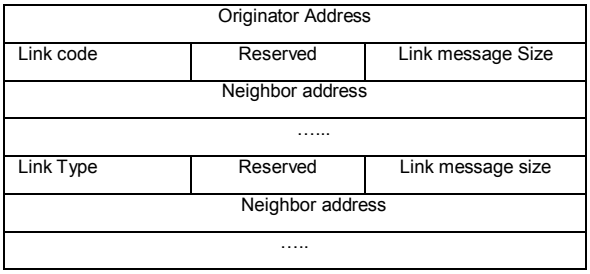

Fig. 1. OLSR Hello Message Format.

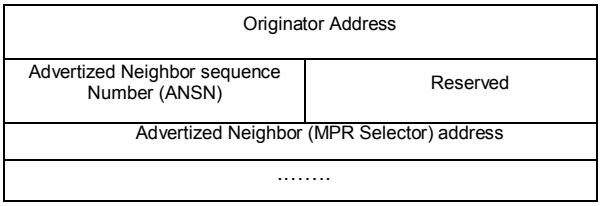

Fig. 2. OLSR TC message Format

These messages are broadcast by all nodes heard only by immediate neighbors; they are never relayed any further. Upon the reception of Hello messages, other nodes can derive information concerning their one hop neighbor and two hop neighbors. They can also calculate a subset of one hop symmetric neighbor nodes as its MPR set. This MPR set is declared in its next Hello message broadcast. Furthermore, through receiving a Hello message, nodes can create or update their MPR selector set. That demonstrates nodes which have currently selected this node as their MPR.

A Topology Control (TC) message is periodically sent to the whole MANET by each MPR in the network to respectively declare its MPR selector set. It is, then, used in the construction of routing tables in every MANET node. Fig. 2 shows the basic format of a TC message [5].

Thus, a TC message contains the list of neighbors that have selected the sender node as an MPR (MPR Selector Set), and an Advertized Neighbor Sequence Number (ANSN) is used by a receiving node to check if the information advertized in the TC messages is more recent.

Only MPR nodes are allowed to generate and forward TC messages. The information embedded in TC messages generated by an MPR includes at least the existing links between itself and its MPR selectors. The non-MPR nodes do receive TC messages from their MPRs and process them. However, non-MPR nodes do not forward the received TC messages. This feature of OLSR reduces the number of messages exchanged in topology discovery Fig 3.

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.

MPR calculation is based on willingness announced by neighbors using Hello messages. Willingness is one of the fields in a Hello message, which specifies the willingness of a node to carry and forward traffic on behalf of other nodes. According to the standard OLSR, willingness may be set to integer value between 0 and 7. The willingness value of WILL_NEVER (integer value of 0) means that a node does not wish to carry traffic to other nodes and it will not be included in the MPR set. The willingness value of WILL_ALWAYS (integer value of 7) means that a node is willing or has resources to forward traffic to other nodes. Therefore, for a given node. That all the neighbor nodes with willingness equal to WILL_ALWAYS will always be included in the set of MPRs [15].

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. 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. The MPR selection algorithm proceeds in four steps:

- Start with an MPR set made of all members of M with M_Willingness equal to Will_always.
- A node M first selects as MPR the neighbors that have the one neighbor in the two hop node from M.
- It then selects as MPR a neighbor that has the largest count of uncovered two-hop nodes. This step is repeated until all two-hop nodes are covered.
- Finally, any MPR node N can be discarded since the MPR set covers all two hop neighbors without the MPR node N.

Each node in the network maintains an MPR selector set, which has selected this node as an MPR.

III. The Model Of Single Black Hole Attack Against OLSR Protocol.

In this section, we describe how malicious node can launch a Single black hole attack in MANET. To launch this attack is that the attacker node can force its selection as MPR by constantly maintaining its willingness field to Will_always in its HELLO messages. According to the specification of the OLSR protocol [15], its neighbors will always select it as MPR. Using this mechanism, and due to the lack of security measures in OLSR, the malicious node can launch a single black hole attack by dropping all, or selected, messages that pass through it. This misbehaving node affects the integrity and the construction of routing tables for each node in the network. The node will isolate and will not calculate a complete view of the network topology.

Fig 3 is an example of single back whole attack, i.e., when receiving HELLO message (With Willingness fields positioned to Will_always) from the attacker node E, the node S selects E as MPR and updates its routing table accordingly. To reach the destination node D, Topology Control messages and Data packets must pass through E. The latter will not relay all packets. Thus H will never learn that the last hop to reach S is node E.

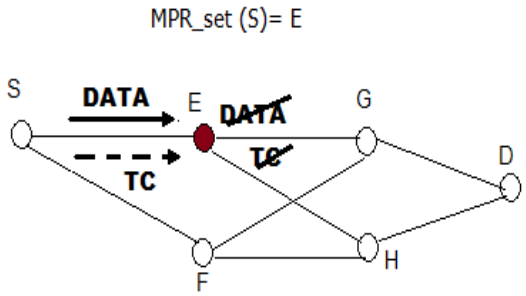

Fig. 3. A Single Black Hole attack model.

IV. Related Work

In [16] the authors propose the integration of a trust-based reasoning in every node. Thus, each node is able to identify misbehaving nodes by analyzing received messages using the protocol trust rules, Authors focus on the MPR selection and propose that the MPR selection can be strengthened and violated by exploiting trust properties and relations.

In [17], Cuppens et al investigate the use of AOP in MANETs to provide availability issues in OLSR. Authors formally describe normal and incorrect node behaviors to derive security properties using AOP. The proposed algorithm verifies if those security properties are violated. If they are, then the detector node sends its neighbors the detection information to avoid choosing the intruder as part of valid path to be constructed. A node chooses valid paths based on the reputation of their nodes.

Wang et al [18] present an intrusion detection approach for OLSR. The semantique properties that are Implified by the protocol definition are used by every MANET node for conflict checking regarding the correct OLSR routing behavior.

In [19], the watchdog and pathrater mechanism is proposed to mitigate routing misbehavior. In each node, the watchdog monitors the successor node, after sending to a packet, by overhearing the channel and checking whether it relays or drops the packet. Then the pathrater accuses a monitored node for misbehavior if it drops more than a given number (threshold) of packets.

In [20] 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 neighbor 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 [21] is a solution to detecting malicious attacks 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 [22] 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 a new field named Requested-value in the HELLO message.

[23] Suggest a modular solution structured around fives modules. The first one is the monitor which control packet forwarding. The second module is the detector of monitored nodes misbehavior. The third module is the isolator of detected misbehaving nodes. The fourth module is investigates accusation before testifying if the node has not enough experience with the accused one, and the last module is the witness which responds to testimony request of the isolator

[24] Propose an approach to cope with packet droppers. The core of the idea is that all intermediate nodes need to acknowledge the reception of the packet. Using this acknowledgement, the source node constructs a Merkle tree and compares the values of the tree rout with a precalculated value. If both values are equal then the end-to-end path is packet droppers free.

V. THE PROPOSED SOLUTION

As previously mentioned, each node in the network has to select a set of one-hop neighbors MPR set, which is constructed by the smallest number of nodes that allow the MPR selector to cover every two-hop neighbor through, at least one of its MPRs.

To deal with a Single Black Hole attack, we propose an algorithm to select MPR with additional coverage without giving priority to nodes with higher willingness. The aim of this algorithm is to reduce the impact of malicious nodes trying to be selected as MPR nodes.

Our approach is a modified version of the RFC 3626 [1] MPR coverage parameter which allows increasing the number of nodes through which, the MPR selector can reach every two hop neighbor. For example, if MPR-Coverage is equal to K it means that, if possible every two-hop neighbor can be reached though at least K nodes (K=1, standard OLSR).

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.
- MPR_set (E): the set of nodes selected as MPR by the node E. (MPR_set (E) $\subseteq$ 1HN_set (E)).
- MPRS_set (E): the set of symmetric neighbours which have selected the node E as MPR. (MPRS_set (E) $\subseteq$ 1HN_set (E)).
- 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) $\cap$ 1HN_set(Y) $\neq \emptyset$ } assuming that Y $\in$ 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.
- Poorly_set: A subset of 2NH_set(X) which is covered by less than K nodes in 1NH_set(X).

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 poorly covered nodes in two hop neighbor.

3) *We remove the poorly covered 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) not in MPR_set.
- Select as MPR the node which provide reachability to the maximum number of nodes in 2HN_set(X) and maximum degree.
- Eliminate all the nodes in 2HN_set(X) now covered by at least, K node in the MPR_set.

Algorithm 1: MPR Selection with K-Coverage

```
1HN*_set(X) ← 1HN_set(X)
2HN*_set(X) ← 2HN_set(X)
Poorly_set ← Ø
MPR_set (x) ← Ø
For all node Y ∈ 1HN_set(X) do
 Degree(X, Y) ← | 1HN_set(Y) \ 1HN_set(X) \ {X,Y} |
End.
For each Y ∈ 2HN*_set(X) do
      If | 1HN_set(Y) ∩ 1HN*_set(X) | < K  then
         Poorly_set(X) ← Poorly_set(X) ∪{Y}
        MPR_set(X) ← MPR_set(X) ∪ {1HN*_set(X) ∩ 1HN_set(Y) }
        2HN*_set(X) ← 2HN*_set(X) \ {Y}
      Endif
Endif
For each Z ∈ 2HN*_set(X) : |1HN_set(Z) ∩MPR_set(X)| > K  do
            2HN*_set(X) ← 2HN*_set(X) \ {Z}
  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.
  If        Reachability (X,Y)= Max { Reachability (X,Y), Y ∈
1HN*_set(X)}  and     Degree(X,Y) = Max { Degree  (X,Y), Y ∈
1HN*_set(X)}     then
     MPR_set(X) ← MPR_set(X) ∪ {Y}
     2HN*_set(X) ← 2HN*_set(X) \ {1HN_set(Y) ∩   2HN*_set(X)}
  Endif
End.
Return MPR_set (X)
End
```

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 A and their Willingness.

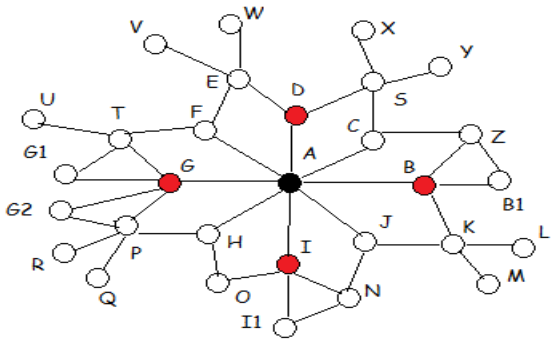

Fig. 4. Example of multiple attackers {B, D, G, I} arround the victim node A.

TABLE I. WILLINGNESSES OF NODES IN 1HN_SET (A)

Nodes	Willingnesse
B	7
C	3
D	7
F	4
G	7
H	5
I	7
J	4

Suppose now that B, D, G, I are the misbehaving nodes , our approach will select MPR_set such as every node in two hop neighbor will be covered by K = 2 MPRs nodes.

Thus the redundant link State information is included in the TC messages; more nodes will emit TC-messages, Which are flooded through a redundant set of link in the network. In Fig 4 the attacking nodes (B, D, G, I) drop all TC messages that pass through them. Our solution will select (C, F, H, G) list as the alternative MPRs nodes to cover the two hop neighbor.

The statement of our algorithm (K = 2) is as following:

- Calculate the degree of each node in 1HN_set (A): degree = {B (3), C (2), D (2), F (2), G (4), H(2), I(3), J(2)}.
- Poorly_set = {B1, G1, G2, I1}: Select as MPRs those nodes in one hop neighbor which cover the poorly covered nodes in two hop neighbor. MPR_set (A) = {B, G, I} and 1HN*_set (A) = {C, D, F, H, J}.
- Remove the poorly covered nodes from two hop neighbor set for the rest of the computation: 2HN*_set (A) = {Z, S, E, T, P, O, N, K}
- Calculate the reacahbility of nodes {C, D, F, H, J}: Reachability = {C(1), D(2), F(2), H(2), J (2)}
- MPR_set (A) ={B,G, I,C, D, F, H}
- Finally, we have 2HN*_set (A) = Ø then the algorithm return MPR_set (A) = {B, G, I, C, D, F, H} (Fig 4).

VII. 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 Single black hole attack. All the default values for the OLSR protocol from [1] were used (Table 2). The simulations were performed for 50-100 nodes with a transmission range of 200 meters, in an area of size 1000*1000 meters during 300 seconds. Random waypoint model is used as the mobility model of each node. Nodes speed is 5 m/s. The number of malicious node is varied from 0 to 4.

In our experiments, we assume that all the nodes haves the same characteristics, every node has just one interface and all the links between the nodes have that same Willingness to carry and forward traffic on behalf of other nodes, except for those that have been selected as misbehaving nodes.

TABLE II. 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
K-Coverage	1-2
Duplicate hold time	30 s

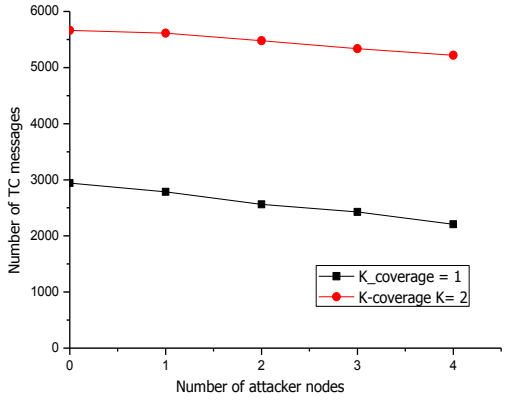

Fig. 5. Number of TC messages VS Number of attacker nodes

Fig 5 shows how our strategy offers additional protection to mitigate the effect of misbehaving nodes trying to be selected as MPR nodes by maintaining constantly its Willingess field to Will_always in its Hello messages. We point out that it is not always possible to find K-MPR nodes for all the nodes in the network. Thus, if the number of attacker nodes increase the level of protection decreases.

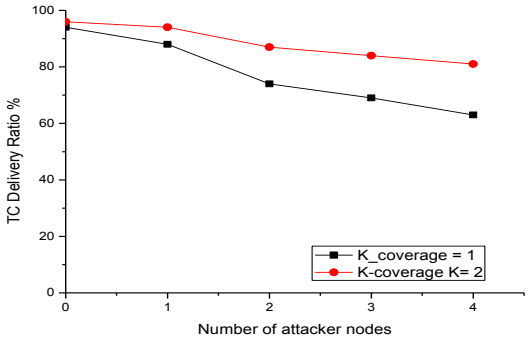

Fig. 6. TC Delivery Rate VS Number of attacker nodes

Fig 6 shows the delivery Rate of TC-message under variable number of attackers. We observe that the Delivery Ratio decreases when we increase the number of attacking nodes.

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 7 compares standard OLSR to Our approach OLSR with K_coverage = 2. We observe that in the presence of the attack, the PDR in K_coverage =1 is very low, the only packets received by the node are the ones received before launching the attack, and we see that the PDR increases when the speed of the node increases. The reason is that, when the destination node moves rapidly, it has more chances to select node as MPR other than the victim node.

On the other hand when the New-OLSR is under attack we see that the PDR is better than a standard OLSR under attack. The reason is that; in K_coverage = 2 the source node has (if possible) two alternatives to reach its two hop Neighbors. If one of them is a misbehaving node the Dijkstra algorithm can select the route connecting a given source and destination nodes which not content this misbehaving node.

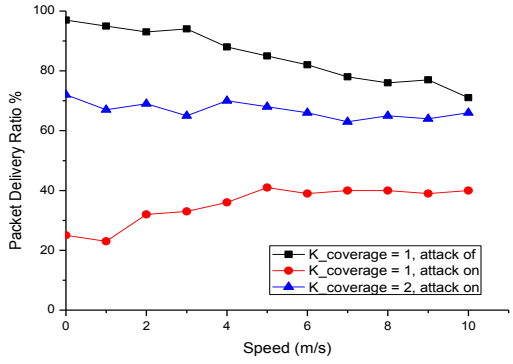

Fig. 7. Packet Delivery Ratio Vs Speed

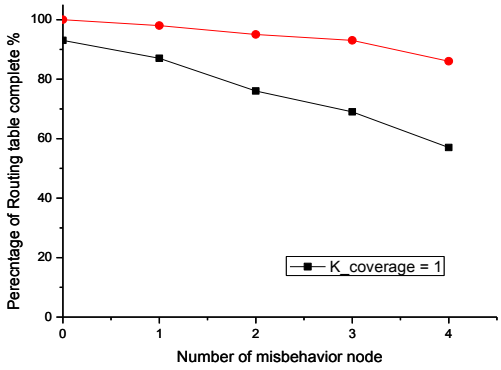

Fig. 8. Percentage of nodes with complete routing table

Fig 8 shows how our strategy offers additional protection to mitigate the effect of misbehaving nodes. The percentage of routing table complete is between 100 % and 92 %. Thus our approach is beneficial in spite of the cost paid in overhead communication.

VIII. Conclusion

The black hole attack exploits the routing protocol's vulnerabilities by forcing its selection as a Multipoint relay by constantly maintaining 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 by additional Coverage. This gives priority to a node that covers maximum nodes in two hop neighbors which do not show strong characteristics to influence the MPR selection to be selected as MPR. Simulation results demonstrate that the proposed method is effective in mitigating black hole attack. It shows high Topology Control delivery ratio and increases topology knowledge which provides significant benefits for communication protocols. This additional knowledge may support the construction of more robust routing paths, or event multipath, in order to provide security.

IX. Future Work

As most of our contributions have evaluated through simulation using NS2 network simulator, we intended to implement them into real tested and assess their performance in such real network environment.

References

[1] J. Coriil, S. Ochoa, J. Pino. High level MANET protocol: Enhancing the communication support for mobile collaborative work. Elseiver journal of Network and Computer Applications. 2012; 35 (1), 145-155.

[2] P. Papadimitratos, Z.J. Haas, Secure message transmission in mobile ad hoc networks, in journal Ad Hoc networks. 2003; 1(1),193-209.

[3] Perkins C, Belding-Royer E, Das S. Ad hoc on-demand distance vector (AODV) routing. IETF RFC 3561, 2003.

[4] Johnson DB, Maltz DA, Hu Y-C. The dynamic source routing protocol for mobile ad hoc networks (DSR). IETF Internet Draft, draft-ietf-manet-dsr-09, 2003.

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

[6] Ogier R, Lewis M, Templin F. Topology dissemination based on reverse-path forwarding (TBRPF). IETF Internet Draft, draft-ietf-manet-tbrpf-07.txt, 2003.

[7] J-H. Zygmunt : A new routing protocol for the recon_gurable wireless networks. In Proceedings of 6th IEEE International Conference on Universal Personal Communications, IEEE ICUPC'97, October 12-16, 1997, San Diego, California, USA, volume 2, pages 562{566. IEEE, IEEE, October 1997.

[8] Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer E. A secure routing protocol for ad hoc networks. Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[9] Hu Y-C, Perrig A, Johnson DB. Ariadne: a secure on-demand routing protocol for ad hoc networks. Proceedings of the MobiCom 2002, Atlanta, Georgia, U.S.A., 23–28 September 2002.

[10] Zapata MG. Secure ad hoc on-demand distance vector routing. ACM Mobile Computing and Communications Review (MC2R) 2002; 6(3):106–107.

[11] Zapata MG, Asokan N. Securing ad-hoc routing protocols. Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), Atlanta, GA, U.S.A., September 2002; 1–10.

[12] Hu Y-C, Johnson DB, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002). IEEE: Calicoon, NY, June 2002; 3–13.

[13] Papadimitratos P, Haas Z. Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, 27–31 January, 2002.

[14] Zhou L, Haas ZJ. Securing ad hoc networks. IEEE Networks Special Issue on Network Security, November/ December 1999; 24–30.

[15] 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.

[16] A. Adnane, R.T. de Sousa Jr., C. Bidan, and L. Mé. Autonomic trust reasoning enables misbehavior detection in OLSR. In ACM Symposium on Applied computing (SAC), pages 2006–2013, New York, USA, 2008.

[17] F. Cuppens, N. Cuppens-Boulahia, T. Ramard, and J. Thomas. Misbehaviors detection to ensure availability in OLSR. In Mobile Sensor Networks (MSN), volume 4864 of Lecture Notes in Computer Science, pages 799–813. Springer, 2007.

[18] M. Wang, L. Lamont, P. Mason, M. Gorlatova, An effective intrusion detection approach for OLSR MANET protocol, in: Proceedings of the First International Conference on Secure Network Protocols (NPSEC), IEEE Computer Society, Washington, USA, 2005, pp. 55–60.

[19] Marti S, Giuli TJ, Kevin L, Mary B. Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on mobile computing and networking (MobiCom'00); 2000. p. 255–65.

[20] 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.

[21] 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.

[22] 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, 2007; 20 (11), p.1245-1261.

[23] D.Djenouri, N.badach, On eliminating packet droppers in MANET: A modular solution. Ad Hoc Networks 2009; 7(6): 1243-58.

[24] A. Badach, A. Belmehdi, Fighting against packet dropping misbehavior in multi-hop wireless ad hoc network, Network and Computer Application 35(2012) 1130-1139.