Journal of Network and Information Security
6 (1), June 2018, 24-29
http://www.publishingindia.com/jnis

Analysis of Secure Route Re-computation Mechanisms on OLSR Based MANET

Chithra V.
M. Tech, Computer Science & Engineering, Thejus Engineering College, Thrissur, Kerala, India.
Email: chithravenugopal28@gmail.com

Abstract: The Optimized Link State Routing (OLSR) protocol is a proactive routing protocol that uses an efficient link state packet forwarding mechanism called multipoint relaying. OLSR is unsuitable for highly mobile network and the MPR node, which has the responsibility for broadcasting packet, is vulnerable to active attacks, link failure, link spoofing etc. In this paper, the methods for securing route re-computation mechanisms on OLSR under MANET are compared. The Denial Contradictions with Fictitious Node Mechanism (DCFM) is suspect a gray-hole node by using contradiction rules before an attack has happened where control packets are again broadcasted on a route failure. The route re-computation is done based on Dijkstra's algorithm. The BR-OLSR (Back up-Routing based OLSR) and OLSR-OPP (OLSR Opportunistic) are mitigation techniques that function only after the attack has commenced and re-routing process can done with minimum overhead using Dijkstra's algorithm. This paper aims to identify the re-routing process and countermeasures for route failure from analyzing the methods on the basis of mobility, node density, network overhead and Reliability of MPR node.

Keywords: Back up routing, DCFM, Dijkstra's algorithm, Multipoint relaying, OLSR opportunistic, Re-routing process.

I. Introduction

Mobile Ad-hoc NETwork (MANET) is vulnerable to several attacks because of the characteristics like mobility decentralized working and changes in topology. A routing protocol is used to establish a path between sender and receiver to transmit the data. Due to the mobile nature of nodes in MANET designing of a routing protocol is difficult. Based on routing update mechanism the routing protocols are classified into Proactive, Reactive and Hybrid routing protocols. Proactive routing protocols are known as table-driven protocol where every node wants to maintain topological information in table format. In MANET, every node is moving which leads to the updating of topological table that maintained by every node. OLSR, DSDV, CGSR, WRP, STAR are some examples for the protocols that belongs to this category.

OLSR (Optimized Link State Routing) is an optimization for Link State Routing where the

Redundancy of control packets are reduced by the use of multipoint relaying mechanism. In OLSR selective node called MPR will broadcast the control packets to maintain the topological information. The selected MPR node can affect by attackers like grey- hole which selectively drop the packet. The route failure or node failure in OLSR leads to the re- broadcasting of control packets which increase the network overhead. In this paper, the security mechanisms like DCFM, Back up routing and Opportunistic routing over OLSR based MANET are compared and it's rerouting process of these methods on route failure using Dijkstra's Algorithm is also proposed.

The remainder of this paper is organized as follows: Section 2 analyses the OLSR overview, Problems in OLSR routing protocol and Existing mechanism to avoid the problems. Section 3 describes the three security mechanisms, DCFM, Back up routing and Opportunistic routing over OLSR. Section 4 is analyzing the mechanism and Section 5 draws the conclusion from the analysis.

II. Related Work

A. Overview of OLSR

The OLSR protocol is utilizes Multipoint relaying mechanisms, in which the selected MPR node will broadcast the control packets to every other node. The first stage of OLSR is neighbor sensing where every node will identify its one-hop and two-hop neighbours using HELLO messages. Every node maintains a neighbour table which contain its one-hop and two-hop neighbour details. In Stage 2 a MPR node will selected for every node. A MPR node is the one that cover maximum 2-hop neighbours of a node. This selected MPR will broadcast the topological information to every other node for eliminating

the redundancy of control packets in Stage 3. The message send by MPR is known as TC (Topology Control) message, in which a MPR and the nodes who selected this as an MPR will contain. Every node will maintain a topological table too. The table will provide the entire topological view of the network. The final stage is Routing table creation. Based on the information available from neighbour table and topological table the routing table can be created.

B. Problems in OLSR

OLSR is eliminating the redundancy of control packets by using MPR node as compared to Link State Routing. But OLSR have several other problems:

a. Grey Hole Attack: OLSR is not promises a reliable MPR node. Suppose the selected MPR node is a grey hole node, it will drop the packet that want to transmit to the destination. A grey hole node will participate in neighbour sensing process by broadcasting the wrong HELLO messages. There is no additional mechanism in OLSR to check the reliability of HELLO packets.

b. Overhead due to Route Failure: A route node can be failed due to mobility or expiring the battery power. The route failure leads to the

c. Packet drop due to route failure.

C. Existing Security Mechanisms

There have been proposed several methods to secure the OLSR based MANET. S. Djahel et al. attempt to eliminate the cooperative black hole using acknowledgment based scheme. Two additional control packets are used, 3-hop ACK and HELLO- rep. Each MPR node should know its 3-hop neighbor set and all TC message from all MPR selector set. The node will identify whether one node intentionally drop the packet or not. ACK based method can't identify the attacker nodes that are consecutive. B. Kannhavong et al. modified the HELLO message and include all 2-hop neighbors, check the contradiction occurring in messages. But the method can't identify whether the contradiction is due to the attacker node or topological changes.

Krishnamurthy S. V. et al. proposed a route recovery mechanism using mean and variance of the lifetime of link between nodes. A time-driven mechanism and data driven mechanism are used to collect the neighbour table information. In time driven mechanism the topology change will determine after a quiet time later it has happened. This drawback is eliminated in data driven mechanism where unreachable route is added to a beckon packet. After receiving the beckon packet every node will update the neighbour table. The transmission of beckon packet will increase the network overhead.

Pant R. et al. used a modified OLSR control messages to build hierarchical network. The overhead due to extra signaling of the modified control messages for maintaining and building the network is the major drawback of this method. In this proposed method only the packet loss due to link/node failure is considered. If a node get failed store and forward routing is used and otherwise end to end routing is used.

III. Proposed System

Security over OLSR is achieved in terms of reliability of MPR node, reduction of network overhead, elimination of packet drop from failed route. In the following secure OLSR protocols, routing path selection is based on Dijkstra's algorithm which work differently in three mechanisms and based on the working the network overhead is varied.

A. DCFM Based OLSR

DCFM (Denial Contradictions with Fictitious Node Mechanism) based OLSR uses contradiction rules to identify whether a HELLO message is reliable or not.

By using this mechanism the reliability of selected MPR node get increased. This method suspect an attacker node before the attack get happened without any additional mechanism. Therefore the implementation cost of network is negligible. DCFM will eliminate a gray hole node by using three contradiction rules. The modified OLSR using DCFM is explained below:

Step 1: Neighbour Sensing

In Neighbour sensing every node will broadcast a HELLO message to identify the 1-hop and 2-hop neighnours. Suppose a node send a false HELLO message and elected as MPR node, then it can influence the entire topological information.

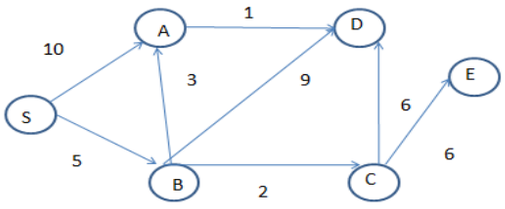


Fig. 1: Sample Topology

As shown in fig. 1 node S send HELLO message to 1-hop neighbours A and B. Node B is the MPR of S where 2-hop neighbours of S (D, C) is covered. Suppose node A is a grey hole node and interested to elected by S as MPR. A send a wrong HELLO message to S, that is {D, C} where A do not have a link to node C. Now S can select A also as MPR node. If the grey hole node A selected as a MPR, it will further broadcast TC message as its own wish which affect the entire network badly. To avoid this three contradiction rules are proposed:

Rule 1: If the attacker node broadcast a HELLO message to Victim, The Victim should verify that every common one-hop

neighbours of Victim and Attacker should contain attacker as its one-hop neighbour. Otherwise a contradiction will occur.

From fig. 1 consider S is victim and A is attacker, where B is the common one-hop neighbour of S and A. One-hop neighbour set of B should contain A. If not contain then S suspect node A.

Rule 2: If attacker node contains 2-hop neighbours of victim as 1-hop neighbours, then its 1- hop neighbours should be the 2-hop neighbours of attacker node.

Consider the figure 1 node S is the victim and A is the attacker node, node A sending a wrong HELLO message that contain C as its 1-hop neighbour. Then 1-hop neighbours of C, that is E should be the 2-hop neighbour of A. But A don't contain E as its 1-hop neighbour and a contradiction occurred. S suspect A as the attacker node.

Rule 3: Every HELLO message will go through Rule 1 and 2.

Every node should check the contradictions rules and a fictitious node attached to each node for checking whether the intention of node is successful or not. It is an imaginary node in the network. A reliable node should satisfy both rule 1, 2 and 3 otherwise it will suspect as attacker node.

Step 2: MPR Selection

Every node will select a MPR node that covers maximum 2-hop neighbours.

Step 3: MPR Information Declaration

The selected MPR broadcast a TC message to its 1- hop neighbours where TC message contains the MPR selector set. After this step every node will have the entire topological information.

Step 4: Routing Table Creation

Based on the information available from neighbour table and topological table the sender node will find a path to destination.

The path selection can be done using Dijkstra's algorithm in which the shortest path between sender and receiver will find out. Dijkstra's algorithm solves the single-source shortest-paths problem on a weighted, directed graph G = (V, E) for the case in which all edge weights are nonnegative. The weight is the distance between two nodes. The running time of Dijkstra's algorithm is lower than that of the Bellman-Ford algorithm.

In fig. 2 node S select node B where the distance is 5. Node B is closer to node S than A. The initial cost of S is zero and cost of node B is updated as 5 where 5 is the distance between node S and B. Node B has one-hop neighbours C, A, D where C is closer to B. Node B select C as its next connected pair. S is selected path S-B-C- D with shortest distance 12. Node A is not covered where A reach form S and B. The shortest path is S- B-A to reach node A. Node S can reach to node D through S-B-C-D with distance 13 and S- B-A-D with distance 9. So the shortest path will select, that is S-B-A-D to transmit the data packet.

Suppose the route node A get failed then DCFM based OLSR will again start from step 1 (neighbour sensing) to update the neighbour table and topological table. Broadcasting of control packets will increase the overhead of network.

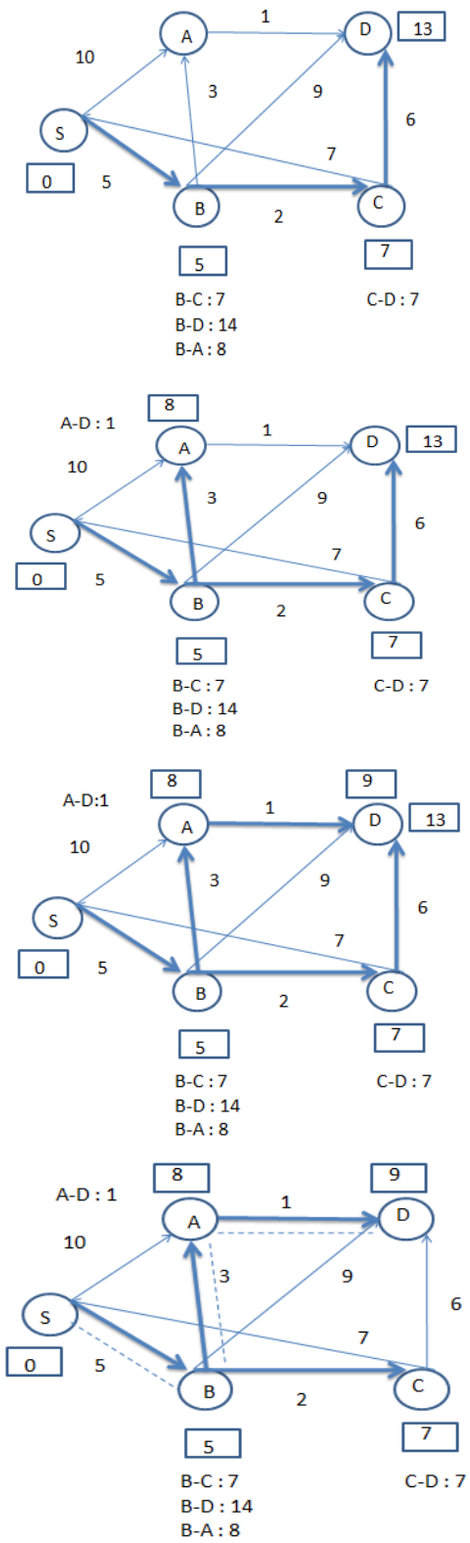


Fig. 2: Routing Process in DCFM based OLSR using Dijkstra's Algorithm

B. BR-OLSR

In BR-OLSR (Back up Routing-OLSR), the overhead due to rebroadcasting of control packets will decremented by maintaining back up routes.

In routing table the backup routes for sender node will maintain and by using Dijkstra's algorithm every possible path from sender to destination will find out. Neighbour sensing, MPR selection and MPR information declaration are same as OLSR

Step 1: Routing Table Creation

This stage is different in BR-OLSR from DCFM based OLSR.

(a) Adjacent Node List Calculation

First the small distance will set as ∞. The propagation radio range want to calculate based on the transmitter, receiver gain and height of antenna. Using Euclidean distance formula, distance between every node want to calculate. Check whether the distance between nodes are within propagation radio range then the node will added into the neighbour list. The first next hop is the adjacent node with smallest distance.

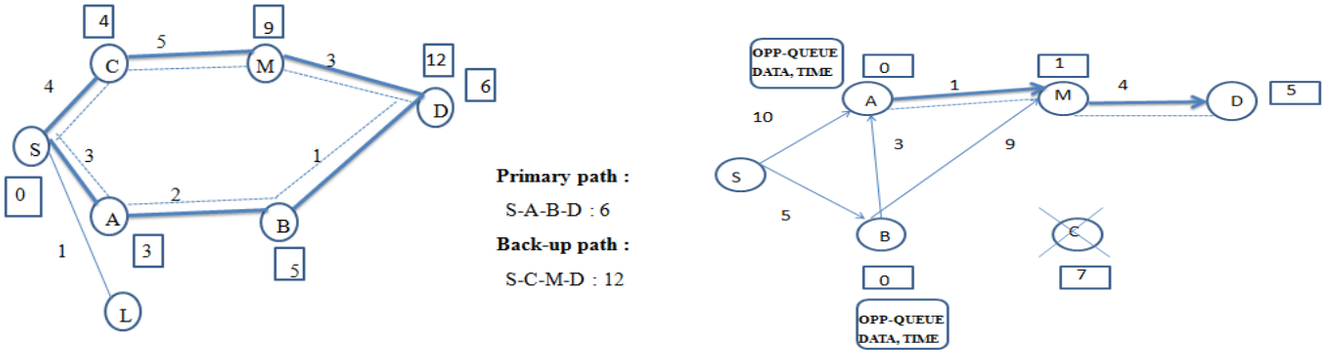
(b) Path Selection

Two additional control packets are used to check whether a node can be the backup route for source or not.

- Next route available
- ACK

A node will send a message "next route available" to neighbour nodes in adjacent node list. If next route are available the node will replay with an ACK to the sender. That will maintain as a backup route. Likewise all possible back up routes from sender to destination will be identified. The shortest path selection algorithm will applied to back up route to find shortest routing.

If primary routing path get failed then alternative path can used to transmit the data. On route failure without re-broadcasting the control packets, new routing path can be selected. The network overhead is less in case of BR-OLSR. If the nodes are less mobile, the link/route failure will be infrequent. Then the maintenance of all possible paths from sender to destination will waste the resources.



(a) (b)

Fig. 3: Routing Process in BR-OLSR using Dijkstra's Algorithm

In fig. 3 the routing path calculation based on dijkstra's algorithm is illustrated. Initially the cost of every node is infinity and distance is the parameter used to select the route node. The cost of a node is sum of distance between two nodes and cost of previous node. The primary path is S-A-B-D with shortest distance 6. On the time of primary path calculation the alternative path from source node to the destination is calculated. In fig. (b), the back-up path is S-C-M-D with distance 12. Likewise all the possible path from source to destination will be calculated. The route nodes in all paths are exclusive with each other.

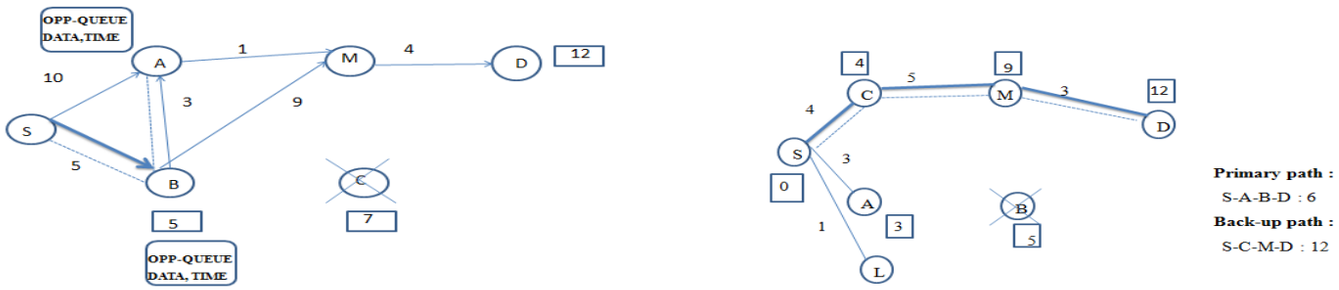
If the route node in primary path is failed then the data packet can be transmitted through alternative path without dropping the data packets. As shown in figure c the node B gets failed and primary route path is also failed. The data will forward by source node through back-up path S-C- M- D. The route failure does not trigger the OLSR protocol from the stage of neighbour sensing. In BR-OLSR all possible routing path are pre-computed. Whenever the primary routing path failed the traffic can transmit through alternative path without updating the topological information. The broadcasting of topological information in the entire network on route failure or link failure leads to incrementation of network overhead.

C. OLSR-OPP

BR-OLSR is not suitable if the network nodes are less mobile where the re-routing is infrequent. OLSR-OPP is useful for both less mobile and highly mobile network. In OLSR whenever a route gets failed the packet to be transmitted through route will drop. The route failure also causes the packet drop problem in the network. In OLSR-OPP every node will maintain a buffer called OPPQUEUE. The packets to be dropped will reside in

the buffer. Every node can define a copy count value which indicates the number of copies of data packet that want to transmit to the 1-hop neighbours. The copy count parameter is decremented whenever a copy of a packet is sent to an immediate neighbour of a node. The node stops forwarding packets when all neighbours have received a copy, or if the copy count reaches 0. A timestamp is attached with the packet for identifying the residing time of packet in the buffer. If a new neighbour is arrived for a node then it will check whether the neighbour is the packet's destination. If that is the case, OLSR-OPP will deliver the packet to the new neighbour and remove the packet from the OppQueue. If the new neighbour is not the destination, the protocol checks if the copy count is greater than zero and if yes a copy of packet is also send to new neighbour node. In OLSR-OPP every node will maintain a buffer called OPP-QUEUE.

The node B can make copies of data packet and packet transmitted to neighbour node A. From the nodes that have data packets, the dijkstra's algorithm will trigger. In fig. 4 (c) node A which has the data packet will select shortest path A-M-D with cost 5. This will leads the routing path selection without updating the topological information.



(a) (b)

Fig. 4: Routing Process in OLSR-OPP using Dijkstra's Algorithm

IV. Analysis Result

The DCFM based OLSR, Back up routing based OLSR and OLSR-OPP are analyzed on the basis of common parameters.

Table I: Analysis of Secure Re-Routing Mechanisms

Parameters	*DCFM based OLSR*	*BR-OLSR*	*OLSR- OPP*
Load in network	Less	Less	High
Memory usage	Less	High	High
High node density	Less efficient	Efficient	Efficient
Packet drop	High	High	Low
Misbehav-ior node detection	Detect and avoid	Not detecting	Not detecting
Handling a Node failure	Packet drop at failed node	Packet drop at failed node	Buffer the packet
In Highly mobile network	Not suitable	Suitable	Suitable
Network overhead 1. In less Mobile network	Low No additional control packets than OLSR	High Additional control packets are: 1. Next route avail able 2. ACK	Low No additio- nal con-trol packets than OLSR
2. In Highly mobile network	High	Low	Low
Routing path	Multiple path from S to D	A single path from S to D	

V. Conclusion

DCFM based OLSR promising the reliability of MPR node and unsuitable for highly mobile network which leads to a re-routing process with huge overhead. Unlike DCFM based OLSR, BR-OLSR and OLSR-OPP is well suitable for highly mobile network, where the re-routing can be done with minimum overhead and reliability of MPR node is not guaranteed. BR-OLSR and OLSR-OPP will compute new routing path on a primary route failure without broadcasting the control packets to update topological information unlike DCFM based OLSR. BR-OLSR aims to create back up routing path, which can be used when a link or node in primary path get failed. OLSR-OPP combine the end-to-end routing with store and forward concept to eliminate the packet drop after a node or link get failed. Among BR-OLSR and OLSR-OPP, BR-OLSR is unfavorable for less-mobile network where the route failure is infrequent and the later is suitable for High and less mobile network with minimum overhead and packet drop.

References

[1] D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, "An advanced signature system for OLSR," *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks,* vol. 4, pp. 10-16, 2004.

[2] R. A. Saaidal, A. Harith, P. Marius, A. Ismail, and P. Ranjana, "An efficient hybrid MANET-DTN routing scheme for OLSR," *International Journal of Wireless Personal Communications,* vol. 89, no. 4, pp. 1335-1354, 2016.

[3] N. Schweitzer, A. Stulman, A. Shabtai, and R. D. Margalit, "Contradiction based gray-hole attack minimization for ad-hoc networks," *IEEE Transactions on Mobile Computing,* vol. 15, no. 1, pp. 163-172, 2017.

[4] Z. Ye, S. V. Krishnamurthy, S. K. Tripathi, A. Pant, R. Tunpan, A. Mekbungwan, P. Virochpoka, and K. Kanchanasut, "DTN overlay on OLSR network," *Proceedings of the 6th Asian Internet Engineering Conference,* vol. 10, pp. 56-63, 2010.

[5] S. Djahel, F. Nait-Abdesselam, and A. Khokhar, "An acknowledgment based scheme to defend against co-operative black hole attacks in optimized link state routing protocol," *IEEE International Conference on Communications,* pp. 2780-2785, 2008.

[6] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, Nis01-2: A collusion attack against OLSR-based mobile ad hoc networks," *IEEE Globecom,* pp. 1-5, 2004.

[7] R. S. Abujassar, "Mitigation fault of node mobility for the MANET networks by constructing a backup path with loop free: Enhance the recovery mechanism for pro- active MANET protocol," *International Journal of Wireless Networks,* vol. 22, no. 1 pp. 119-133, 2015.