International Journal of Technology and Engineering System (IJTES)
Vol 7. No.3 2015 Pp. 239-243
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

IMPROVING MPR SELECTION ALGORITHM IN OLSR PROTOCOL BASED ON DOS FREE TRANSMISSION IN MANET MPR SELECTION PROCESS

[1]G.EZHILARASI [2]R.NAVEENKUMAR., [3]R.RAVIKUMAR., [4]C.SETHUPATHI
[1]Asst. professor , [2,3,4]Final year CSE
UNIVERSITY COLLEGE OF ENGINEERING VILLUPURAM
[1]ezhilgarasi@gmail.com, [2]naveenravichandiran@gmail.com, [3]
ravikumarraja552@gmail.com,
[4]csethupathicse@gmail.com

ABSTRACT

Mobile Ad hoc network is consists of moving nodes that having mobility and the network can organize them self without requiring any fixed platform. Because of wireless communication any node can join or leave network which affectss vey big security constraint and due to limited battery many MANET protocol designers are doing researches on energy saving routing in MANET. In OLSR there is need of selecting MPR set, which minimize unnecessary broadcast in network, that conserve energy of node in network. In this paper an attempt is made to propose a new energy conversant and secured protocol by modifying standard OLSR which provide optimal MPR set and also protect network from node isolation attack is called Denial Of Service Free OLSR (DFOLSR).

1. INTRODUCTION

Mobile Ad-hoc Network is a network of mobile node which has limited transmission range. In this network node act as arouter as well to forward packet. For which there is need ofrouting protocol. [1] Such networks have random, dynamic,rapidly changing topology and limited bandwidth. There are following characteristic of a MANET:

- Packets have to travel from many nodes to Reach destination.
- Not have fixed topology because of mobility, any node can leave or join the network.
- Every node has limited battery.

There is need of frequent exchange of control message, in order to obtain suitable network topology mean that change innetwork topology must be known to every node in network.These control messages will use value wireless bandwidthresource, which cause a challenge for developing routingprotocol. The routing protocols are broadly organized into threemajor categories as Proactive (Table driven), Hybrid andReactive (on-demand). Optimized Link State Routing protocol

(OLSR) is an example of Proactive, due to this proactive nature routes are available immediately when ever needed and Ad-hoc On-demand distance vector Routing (AODV) is one of the most important example of Reactive routing protocol. One ofthe major issues of mobile network is limited energy. Wirelessinterface consume energy in several modes of operationincluding packet sending and receiving. There energy isconsumed in ideal state also. Due to this constraint, lot ofresearch has been done from many years, for making routingprotocol energy aware.Due to wireless communication, anyone can connect to network and able to modify control message without knowledge of other node in the network. This cause lot of security attack in MANET. OLSR is defenseless against various kinds of security threats [3],[4],[5] such as replay attack, flooding attack, link withholding attack, black hole attack, node isolation attack etc and lot of solution.

II. WORKING OF OLSR

OLSR protocol optimize a pure link state protocol for mobile ad hoc network by reducing the size of control packets, instead of declaring all links, its declares only a subset of links with its neighbors and by minimizing flooding of control traffic by using only selected nodes, called Multi Point Relays (MPR).Only the MPR node retransmits its broadcast messages.In Fig. 1 Node N selected two MPRs which cover whole network. This protocol is basically suitable for dense networks. The protocol dose not depends upon any central entity as it works completely in a distributed manner. Hop by hop routing is performed by OLSR protocol. [2] In OLSR there we make use of two types of routing message named, HELLO and TC messages. In OLSR, HELLO message is generate by each node periodically (every HELLO INTERVAL) in order to neighbor sensing and MPR selection. A node's HELLO message contains the list of its 1-hop and 22- hop neighbors. Each MPR node basically used for advertises TC messages periodically, which is used for route calculation. A TC message contains the list of the sender's MPR selector.

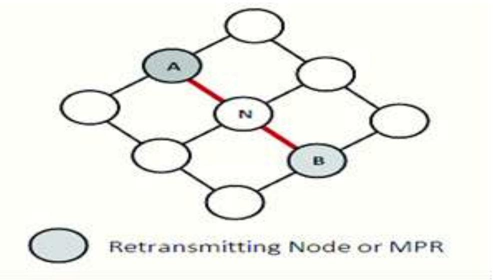


Fig:1 Multipoint Relays

The protocol work as follows:

- Neighborhood discovery will take place by broadcasting of HELLO packets.
- After processing of HELLO packet it is checked whether record is already present in neighbor table in this case simple updation will take place.
- If not records will be added to neighbor table.
- Select the MPR on basis of information gathered.
- Now with help of TC messages topology announcement will take place through MPR.

III. NODE ISOLATOIN ATTACK

In OLSR, Node isolation attack is a kind of Denial Of Service (DOS) attack whose goal is to isolate a node from communicating with other nodes within that network. In this attack, attacker prevents victim node or group of nodes route information by dropping TC message. Thus, other nodes could not able to receive route information of the effected node so those nodes become not reachable or isolated from network. In this attack, the attacker sends incorrect information about 2-hop neighbors in HELLO message, the attacker gather victim's 2-hop neighbor's information by analyzing TCmessage of its 1-hop neighbor [10]. Then attacker claims MPR status to the victim by showing that it covers all 2-hop nodes along with one extra node. Thus, the only mean to forward TC message generated by victim is attacker. By dropping TC message received from the target and prevent route information from being disseminated to the whole network, results victim will not able to receive data from other node. As shown in Fig.2.

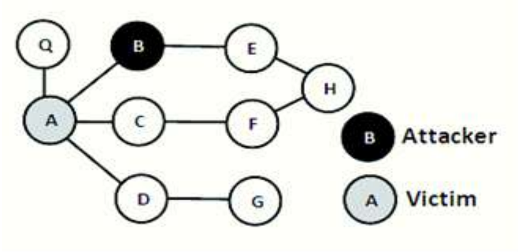


Fig: 2 Node isolation attack

In Fig. 2 NODE B want to Attack NODE A so instead of sending {A, E} in HELLO message it send {A, E, F, G, X} which consist of wrong information and with a route to X which does not exist. Thus on receiving HELLO messages from all nodes, node A will that B cover all the 2-hop node along with one extra node thus select it as a MPR for themselves. As result B is only node form which TC control message to be send thus it drop all TC message from node A. As a result A gets isolated from the network and topology is look like as shown in Fig. 3.

.

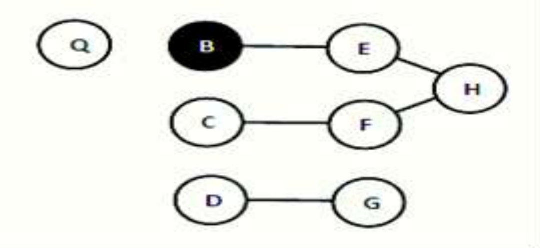


Fig:3 Topology read by node H after attack

IV. RELATED WORK

In [6], network is protected by a cryptographic based approach. It integrates a signature and time stamp with routing control message. There signature is used to authenticate messages from trusted nodes, and in order to prevent replay attacks timestamps are used. The drawback of this approach is that it does not deal with defense against compromised trusted nodes. In [7], the authors make use of public key infrastructure (PKI) and a timestamp algorithm also consider the compromise of trusted nodes. It makes use of additional message ADVSIG that contain information about time stamp and signature. Each node maintains a table where information gathered in ADVSIG message is stored for verifies the correctness of the link state information. In this technique imposes a large overhead to the network in terms of additional traffic and signature computation which result in high energy consumption at each node. In [8] authors to reduce the cost of service in the network make use of authentication system based on one-way hash chain. The cost of the password and digest that we use to ensure authentication, is much less than DVSIG. In [9] the authors employed distributed key management techniques in order to defend against wormhole and message replay attacks. In [10] the authors propose one more way to authenticate, MPR selected Node by sending 2-hostrequest to 2-hop node. Ifnode replays the 2-hostreplay packet then MPR selected is authenticated MPR. But there one overhead is added after MPR selection.

V. PROPOSED WORK

The proposed algorithm is called DFOLSR is modification of the basic OLSR routing protocol, which will be able to detect the presence of malicious nodes in the network along with the MPR selection. In this approach MPR selection procedure is modified which prevent any malicious node from giving the false information about any normal node that wants to become MPR. In this approach, following steps are followed in first iteration:

STEP 1:

There are two new messages VOTEFOR and VOTERPL. Initially VOTEFOR message is unicast to first 1-hop neighbor in sequence, which is further broadcast to their neighbor as shown in Fig. 4. After receiving VOTEFOR message 2-hop node generate VOTEREP message as shown in Fig. 5. The number of replays is recorded in TABLE 1.

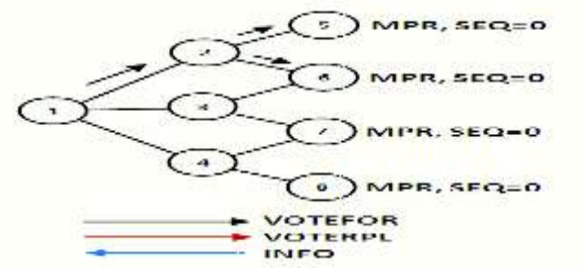


Fig:5*Show first step of Request process*

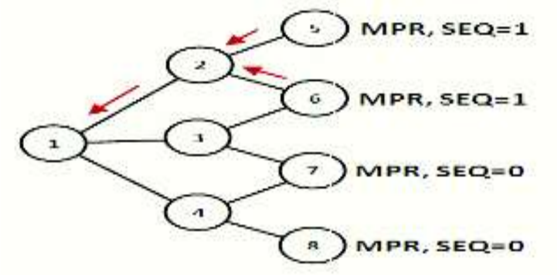
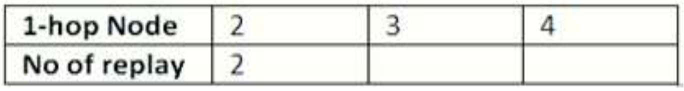


Fig 4:Show first step of Replay process

TABLE 1 CONTAIN INFORMATION OF NUMBER OF REPLAY



1-hop Node	2	3	4
No of replay	2		

STEP 2:

Same process is done for next 1-hop neighbor in the sequence as shown in Fig.6. There 2-hop node whose MPR selected or SEQ is same does not replay as shown in Fig.7 and each node record there number of replay in the table which is maintain by each node as shown in TABLE

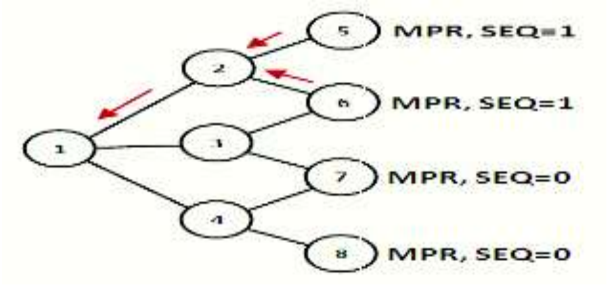


Fig 6 :Show second step of Request process

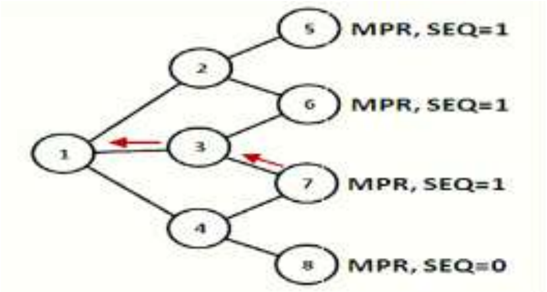
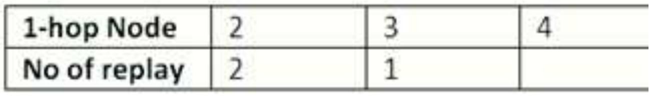


Fig 7 : Show second step of Replay process

TABLE II. CONTAIN INFORMATION OF NUMBER OF REPLAY



1-hop Node	2	3	4
No of replay	2	1	

STEP 3:
In this case 2-hop node whose MPR selected or SEQ is same does not replay and each node record there number ofreplay in the table which is maintain by each node. As shownin Fig.8, Fig.9 and respective entries are displayed in TABLE 3.

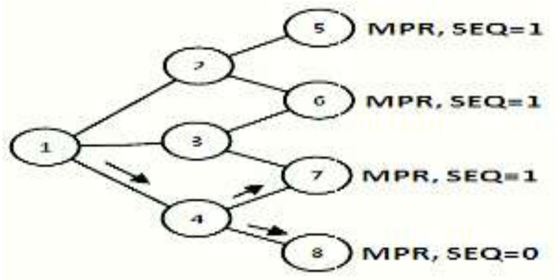


Fig. 8. Show third step of Request process

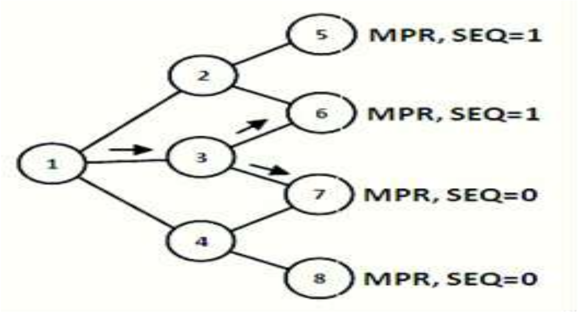
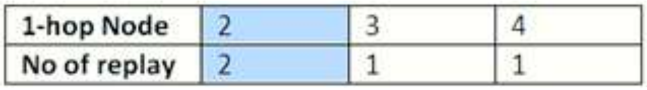


Fig. 9. Show third step of Replay process

TABLE III. CONTAIN INFORMATION OF NUMBER OF REPLAY



1-hop Node	2	3	4
No of replay	2	1	1

STEP 4:
The node which has maximum replay is selected as MPR and placed in MPR set. Those nodes which are selected as MPR are removed from N (u) set. In this step those nodes who have zero vote also removed from set.
STEP 5:
After this step rotate sequence of N (u) which contain remaining 1-hop node and repeat the process for them and inform 2-hop node about their MPR with help of INFO as shown in Fig.10.

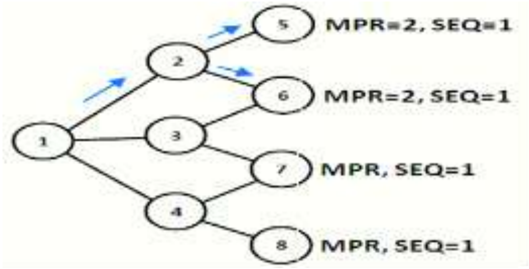


Fig :10 Show Fifth step of informing 2-hop node

After this MPR set contain two nodes {2,4} which cover all 2-hop neighbor shown in Fig.11**.**

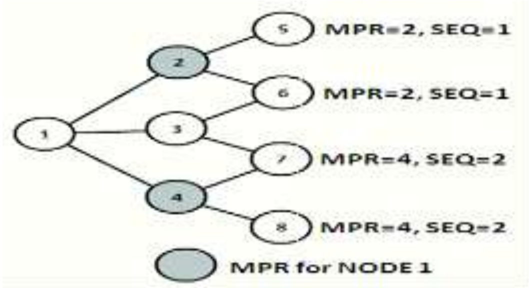


Fig:11 Show Fifth step of informing 2-hop node

In order to reduce number of broadcast in link state routing, there is optimal link state routing, which play important role in reducing these broadcast by selecting MPR. It is well known that selection of optimal MPR set for any network is one of research topic. In this approach a new method of MPR selection is introduced which is free from DOS attack. Following are the steps to achieve the objectives**:** Let N (u) is list of 1-hop node and MPR () is set of selected MPR

- X node which is MPR selector, gather information about 1-hop neighbor.
- Now arrange these 1-hop neighbor nodes in a sequence.
- Then poll for every 1-hop node one –by-one. From 2-hop neighbor which has maximum vote, that is selected as MPR and put in MPR () set.
- Then remove those node from array, who have maximum votes or zero votes
- Then rotate remaining element by one.
- Repeat the procedure from 1 to 5 until array become empty or everyone should get at least one chance.

ALGORITHM FOR SOURCE NODE

N (x) is set of 1-hop neighbor
MPR () is set of MPR

```
n = number of element in N (x)
1-hopnum is number of node selected
While (N (x) □ ¢ OR 1-hopnum = n) {
For (I = 0; I < n; I ++)
{
Unicast message to N [I];
Count the number of replay for N [I];
Store value of replay;
}
Delete value have maximum replay
from N(x) and ADD to MPR () and
inform to 2-hop neighbor
Delete value having zero replays from
N (x)
n = number of element remain in array
N (x)
Rotate left (N (x));
1-hopnum++;
}
Delete remaining value from N (x) and add to
MPR () also inform to 2-hop node about their MPR.
```

ALGORITHM FOR 1-HOP NODE

```
If (packet types == 5)
Broadcast the packet to their neighbors
```

ALGORITHM FOR 2-HOP NODE

```
If (MPR=0 AND SEQ □ Packet SEQ AND SEQ <
Packet SEQ AND Packet MPR=0)
{
Set the value of SEQ equal to packet SEQ;
Replay to source address return in packet
}
Else If (Packet MPR □ 0)
{
Set value of MPR = Packet MPR;
}
Else
{
Discard packet
}
```

In the above example, we can see that we are not takinginformation form 1-hop neighbor, thus there is no chance of getting false information about 2-hop node thus there is no chance of Node isolation attack. One more benefit of this is that it also provides Optimal MPR set along with security. As in above example we see that our algorithm provide optimal MPR set which minimize unnecessary broadcast of network thus we can say that it conserve energy of network.

form 1-hop neighbor, thus there is no chance of getting false information about 2-hop node thus there is no chance of Node isolation attack. One more benefit of this is that it also provides Optimal MPR set along with security. As in above example we see that our algorithm provide optimal MPR set which minimize unnecessary broadcast of network thus we can say that it conserve energy of network.

VI. CONCLUSION

In the Ad Hoc network Energy efficient routing algorithm and security is major concern. In this work it is tried to overcome the problem of node isolation in OLSR by modifying the existing standard OLSR which used the new method of MPR selection. Gives more security to the OLSR and also address the energy conservation problem. The newly modified OLSR will be named as DFOLSR.

REFERENCES

[1] Thomas Kunz "Energy-Efficient Variations of OLSR" IWCMC 2008**.**

[2] T. Clausen and P. Jacquet, “IETF RFC3626: Optimized link state routing protocol (OLSR),” Experimental, 2003

[3] B. Kannhavong, H. Nakayama and A. Jamalipour, “A study of routing attack in OLSR-based mobile ad hoc networks,” Int. J. Commun. Syst., 2007.

[4] T. Clausen and U.Herberg, “Security issues in the optimized link state routing protocol version 2 (OLSRv2),” Int. J. Netw. Security Appl., 2010.

[5] Hiba Sanadikia, Hadi Otrokb, Azzam Mourada, and Jean-Marc Robert "Detecting Attacks in QoS-OLSR Protocol" IWCMC, 2013.

[6] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, “Securing the OLSR protocol,” in Proc. Med-Hoc-Net, 2003.

[7] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, “An advanced signature system for OLSR,” in Proc. ACM SASN, 2004.

[8] Khadidja Ayad, Thouraya Bouabana-Tebibel,"New efficient mechanisms to secure OLSR protocol" FGCT 2012.

[9] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, “Attacks against OLSR: Distributed key management for security,” in Proc. OLSR Interop and Workshop, 2005.

[10] Mohanapriya Marimuthu and Ilango Krishnamurthi "Enhanced OLSR
for Defense against DOS Attack in Ad Hoc Networks" JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 15, NO. 1,
FEBRUARY,2013