RESEARCHERID
THOMSON REUTERS

[INIT: January 2017]

ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

TRUST-BASED MULTIPOINT RELAY SELECTION ALGORITHM FOR ENHANCING SECURITY IN MOBILE ADHOC NETWORKS

Hamela K[*1] & Dr. Kathirvel Ayyaswamy[2]
[*1]Research Scholar, Mother Teresa Women's University, Kodaikanal, India
[2]Professor, Department of CSE, M. N. M. Jain Engineering College, Chennai, India

ABSTRACT

Optimized Link State Routing (OLSR) is a in a popular proactive routing protocol for providing peer-to-peer transmissions in mobile ad hoc networks (MANETs). Since sensitive data are communicated in MANET, security remains a major issue. In this paper, we propose a trust based Multipoint Relay (MPR) selection algorithm for defending a specific type of denial-of-service (DOS) attack called node isolation attack. Our proposed approach is based on cross verifying the exactness of the received HELLO message from a neighbour node before designating it as MPR for this node. Our proposed MPR selection technique includes three main processes, viz. Initialization, Trust computation and Global trust computation. Experimental analysis reveals that our proposed approach defends the node isolation attack with better performance in terms of packet loss ratio, packet delivery ratio and packet overhead

Keywords*- Optimized Link State Routing(OLSR), Mobile Adhoc Network(MANET),Multi-point relay(MPR), network security, Node isolation attack.*

I. INTRODUCTION

MANET is a network of mobile devices associated by remote connections which are self designed and has no infrastructure [1]. The devices in a MANET are permitted to move in any direction and frequently devices links changes happen. This system is exceptionally appropriate for applications including special outdoor events, communications in regions with no wireless infrastructure, emergencies and natural disasters, and military operations. Because of their exceptionally alert and circulated nature, routing becomes one of the key issues in MANETs[2]. For this reason, many routing protocols have been proposed which can be characterized into three distinct groups: namely proactive, reactive and hybrid. The proactive routing protocol determines the routes to all the destinations and maintains it by using a route update process, for example, DSDV and OLSR. The reactive protocols like AODV [3], DSR, determine the routes when they are required by the sources using a route discovery process. The fundamental properties of the initial two classes of protocols are consolidated into one as the hybrid routing protocols.

The nodes keep up ways to all the destinations in the system in a popular proactive routing protocol known as the OLSR, which is done by occasional trade of control messages (HELLO and TC messages) among the nodes in the network. MPR nodes are used for the purpose of broadcasting data in OSLR. Inspite of its proficiency in bandwidth utilization and in path calculation, it is powerless against different attacks such as withholding attacks, link spoofing attacks , flooding attacks , wormhole attacks , replay attacks , black-hole attacks , colluding mis-relay attacks and DOS attacks. Since it depends on the cooperation between network nodes, it is powerless to collude with rogue nodes, and some cases even a solitary noxious hub can bring about routing devastation.

Neighborhood discovery, MPR selection and routing table calculation are the three steps of function in OLSR. Exclusive selection of attacker is being done by MPR selection rule in the case of node isolation attack as it is sole MPR. The coverage of the victim's entire two- hop neighbors including the fictitious node are allowed by MPR as it is minimal set. For enhancing the security of the protocol the intensively considered step MPR selection is the very crucial process. Trust management scheme is deployed in proposed solution for multi point relay selection. In order to prevent any malicious node from giving the false information about any normal node that wants to become MPR, selection process is modified. Trust packets with specific formats are transmitted to the neighboring nodes in

proposed approach. Thus trust table stores the calculated trust value based on the response. Likewise each node maintains the trust table. In order to assign global trust in each node cross refereeing is performed in the entire trust table. The chance of being selected as an MPR is increased as the value of global trust of a node increases.
The rest of this paper is organized as follows: In section 2 some of the most relevant works published recently addressing the similar problems as that of ours is discussed. Section 3, initially introduce a network scenario of node isolation attack and then explains our proposed solution for MPR selection. The simulation results are analyzed and compared with similar existing work in section 4 and the work concludes in section 5.

II. RELATED WORKS

MAC aware concentrated multipoint relay selection algorithm for reducing the medium access control (MAC) layer contention overhead as well as routing overhead was proposed by J.Ahn *et al.* [4]. In this paper information of the number of the MPR selectors help to choose MPRs. Hello messages transmitted by one hop neighbor includes the information on the number of the MPR selectors. The neighbor table with the number of MPR selectors is updated by the hello messages in each node. Then from table information appropriate MPRs are selected in each node that makes more than one MPR selectors to select the same MPR. By sharing MPR the number of MPRs in whole network reduces the concentrated MPR selection mechanism. In this algorithm without considering the influence of any attacks MAC layer contention overhead is reduced by reducing the number of MPR selection.

Fuzzy logic based novel routing metric for MPR selection based on the energy, stability and buffer occupancy of the nodes is presented by A.Kots and M.Kumar [5]. The authors focus on OLSR quality by considering and calculating various attributes in OLSR protocol during the initial phase and MPR selection phase. For easy selection and rejection of a node for the transmission of packets, the probability of a node with different quality metrics are obtained. Quality metrics are predicted using SC techniques. High quality nodes are selected easily by applying SC techniques for reliable transmission in the MANET scenario. The algorithm doesn’t support for high secured routing is the drawback in this paper.

In [6] the paper an energy efficient MPR selection mechanism along with a security measure to eradicate the energy loss exhibited by any of the affected node was presented by A.Anand *et al.* Eligibility of a node for being selected as an MPR is examined with the contribution of Composite Eligibility Index (CEI) For flooding and routing MPRs to provide distinct selection parameters. CEI is used in conjunction with willingness. Energy efficient secure and stable MPRs are selected by simulation study of ES-MPR thereby operational lifetime of the network is prolonged. For the detection of attacks, recently [7] uses an international reputation system. Appointing MPRs are precluded by distrust of nodes. Thereby a group that exhibits malicious behavior is identified by distrust of nodes. It is unable to pinpoint the malicious node within the group. Example which of the nodes in the path between the sender and receiver are colluding to execute the node isolation.

Modification of MPR selection process and addition of two new control messages are proposed by Denial of service free OLSR (DFOLSR) [8]. The node that receives the maximum number of replies are selected as MPR and two-hop neighbors supplies corroboration messages DFOLSR avoids node isolation attacks by not relying on one-hop neighbor. Empirical evaluation of DFOLSR's cost is not provided and an attacker falsifying the responses of fictitious two-hop nodes can render the solution useless. Mitigation of denial of service attacks in OLSR protocol using fictitious nodes is given with another approach by H.N Schweitzer *et al.* [9]. Manipulation of victim into appointing the attacker as a sole MPR by attacker with node isolation attack in this paper. This is being done by attacker control over the communication channel. For providing protection same technique for attacker is used. A node can reduce suspect nodes and refrain from nominating them as a sole MPR by learning local topology and advertising fictitious nodes. Thus the essential element of the attack is sidestepped.

III. PROPOSED TRUST-BASED MULTIPOINT RELAY SELECTION ALGORITHM

Our proposed MPR selection technique includes three main processes, viz. Initialization, Trust computation and Global trust computation.Fig.1 illustrates the node isolation edge connected nodes within broadcast distance is assumed that node x is the attacker, F_x is a fake node and node b is the victim. The rest of the network is represented by the cloud in figure. Based on OLSR rules x should have advertised a legitimate HELLO message contain (b, f). A fake HELLO message that contains (b, f, g, F_x) is sent. b's two- hop neighbors as well as one non-existent node and F_x are contained in the list. By setting the ground for node isolation b would be selected as its sole MPR. Effective isolation of b from the rest of the network is done by advertising b in its TC message.

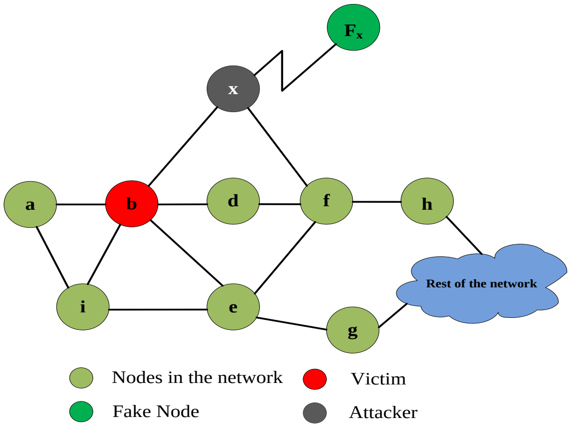

Fig. 1. Node isolation attack scenario

1. Initialization

At time initialization, each node identifies and lists its one one-hop neighbors by broadcasting HELLO message How often the host sends HELLO messages, willingness of host to act as a multipoint relay and information about its neighbor are available in HELLO message.

2. MPR Selection

In our process of MPR selection, each node after receiving the HELLO packets from its neighbor cross verifies whether the received details are true exploiting the available details with its neighboring nodes and compute trust value for each of its 1 hop neighbor node using the below trust formula.

$$T_{mn} = \frac{\sum S}{N-1} \qquad (1)$$

In trust computation, the value of S refers to the verification score provided by a node n after verifying the information provided by a node m, through its neighbour node l. Our predefined verification scores based on the verification outcome is tabulated in table 1.The value of N refers to the number of nodes reported as 1-hop neighbor by the node m.

Table 1. Verification scores

Description	Score
No data available (or) Partially verified	0.5
Verification Pass	1
Verification Fail	0

Each node n computes T_{nml} for each node m through its neighbor node l and maintains a trust table in a format as shown in table 2. Once T_{nml} for all m nodes are computed and tabulated the table values are sorted based on decreasing value.

Table.2. Sample Trust Table of m

m **Node**	**Trust Value provider** l	**Value** T_{nml}
a	*b*	x^{0}
	c	x^{1}
	d	x^{2}
	e	x^{3}
b	*d*	x^{4}
	e	x^{5}
	f	x^{6}

Since trust value computation for a single node is carried by various other nodes within its 1 hop distance we need to compute a final single global trust value based on the below formula.

$$GT_n = \frac{\sum T_{nml}}{N_T} \quad (2)$$

In eqn. (2) GT_n refers to the sum of trust values T_{nml} for a single node m by various trust value providers (1 hop nodes of n). N_T refers to the possible count of l through which the trust value for node m is computed. After computing GT_n ,by exploiting all the available trust values for a node n in the network. Finally, each node includes a global trust table as shown n table 3, for all of its 1-hop neighbors. The GT_n values in the table are sorted in descending order.

Table.3. Global Trust Table of m

Node m	**Global Trust Value** GT_n
a	1
b	1
c	1
d	0.5
e	0.5
f	0
g	0
h	0

From the global trust table associated with each node, the neighboring nodes with global trust value 1 only qualifies as MPR. According to our proposed technique, if a fake HELLO packet is received by a node from an attacker, GT_n for that node will not be 1 and hence will not be in the selection list of MPR thereby avoiding node isolation attack in the OLSR network.

For more clarification about how our proposed MPR selection process identify and defend itself from node isolation attack we'll illustrate by considering the scenario as depicted in Figure 1. After performing the initial process each nodes identifies its 1-hop neighbour and in our case the neighbours of each node in the network are as tabulated in table 4.

Table. 4. List of nodes and its neighbors

Node	**Neighbors**
a	*b,i*
b	*a,i,x,e,d*
i	*a,b,e*
x	*b ,f*
d	*b ,f*
e	*b,i,g,f*
f	*x,f,d*
g	*e*
h	*f*

In our case node x is the attacker and node b is the targeted victim for node isolation attack. The attacker sends a fake HELLO message with b, f, g, F_x as its neighbor. This includes node f which is a 1-hop neighbor of b, node g which is not in 1-hop distance from x and a fake node F_x. After initialization, node b attempts to compute the trust value of x as,

Trust value calculation by b for x

No. of nodes reported by x as a neighbor (N) =4 (b,f,g,F_x)

Verification of f by b through d = Pass

Verification of f by b through e = Pass

Verification score for f =1

Verification of g by b through e = fail

Verification score for g =0

Verification of F_x by b = No data available

Verification score for F_x =0.5

Trust Value for x by b = $\frac{1+0+0.5}{4-1} = 0.5$

Trust value calculation by f for x

Verification of b by f through d = Pass

Verification score for f =1

Verification of g by f through e = fail
Verification score for g =0
Verification of F_x by f = No data available
Verification score for F_x =0.5

Trust Value for x by f $= \frac{1+0+0.5}{4-1} = 0.5$

Global Trust Value for x by $= \frac{0.5+0.5}{2}$

$= 0.5$

Since the Global trust value of node x is not equal to 1, node b will declare x as a malicious node and will not select it as MPR.

IV. RESULT AND DISCUSSION

Table.4. Simulation Settings

Parameters	Values
No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	10,20,30,40 and 50 sec
Routing Protocol	MOLSR
Traffic Source	CBR
Packet Size	512
Speed	5m/s

1. Simulation Model and Parameters

The performance evaluation on the technique using extensive simulation is conducted and presented with the network simulator NS2 [10].Simulation settings and parameters are summarized in table 4.

2. Performance Evaluation

For performance evaluation of our proposed solution against OLSR and EOLSR [11] under attack we consider the following metrics and the comparison results are shown in Figs. 2–4.

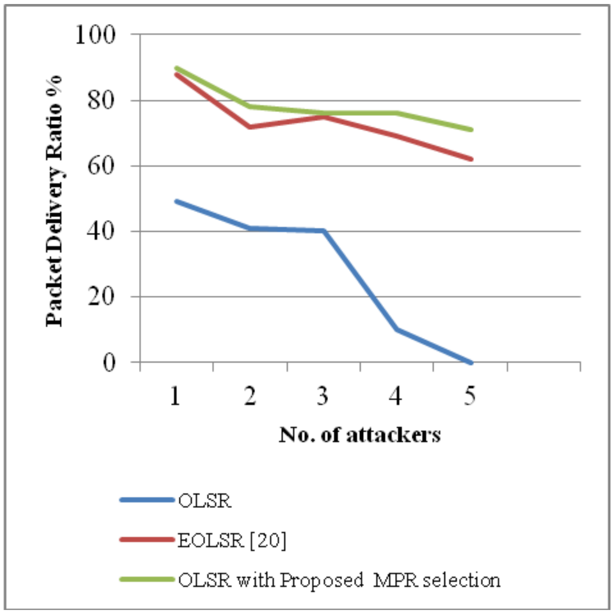

Fig 2. No. of attackers vs Packet delivery ratio

Packet delivery ratio

It is the ratio of the number of packets send by the source nodes to the number of packets received by the destination nodes.

Packet loss rate

It is the number of data packets dropped by the malicious nodes that are selected as MPR nodes.

Control packet overhead:

This is the ratio of number of control packets generated to the data packet received.

Fig. 2 exhibits the variation in packet delivery with respect to increasing attacker count for all the three approaches. For identifying the packet delivery ratio, we have considered attackers ranging from 1 to 5 numbers. In conventional OLSR, victim after selecting the attacker as its MPR, the MPR start dropping the packets it receive. When the number of attacker increases, the packet delivery ratio in the case of OLSR approaches zero, whereas in our proposed approach, the packet delivery and throughput remains more or less the same since the MPR nodes are selected only after verifying its trustworthiness.

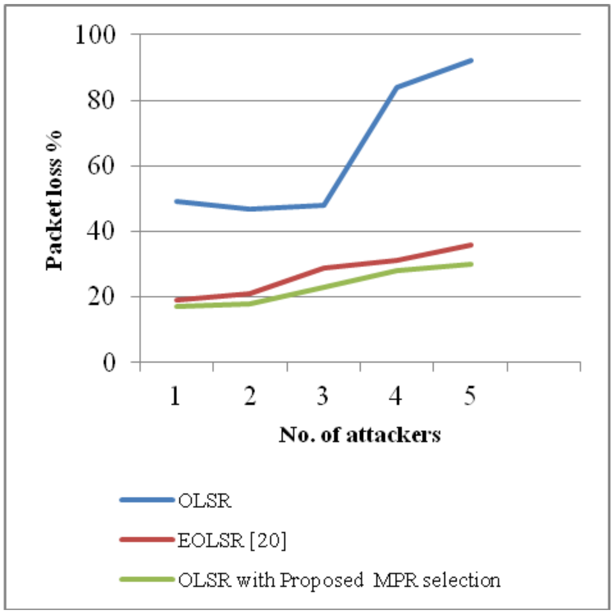

Fig 3. No. of attackers vs Packet loss ratio

Fig 3 shows the number of packets dropped by the malicious nodes in OLSR, EOLSR and our approach. The packet loss with respect to the increase in attackers in our approach and EOLSR remains low and steady, because of the verification process before MPR selection but in the case of conventional OLSR it is too high and unsteady.

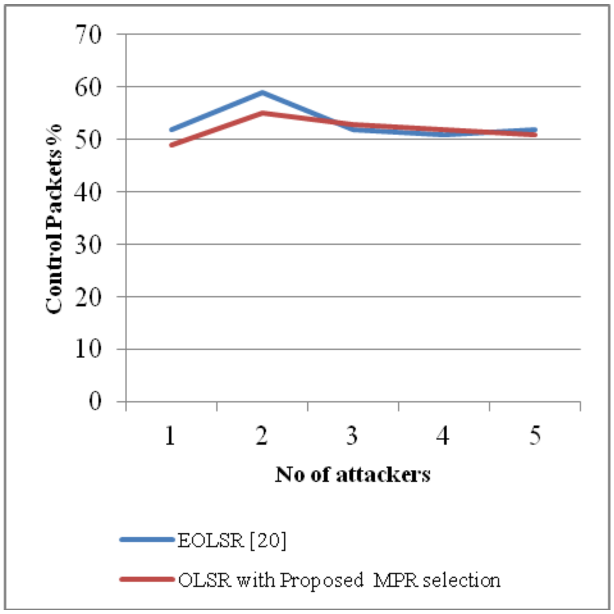

Fig 4. No. of attackers Vs Control packets

The control packet ratio in our case is more or less low than that of EOLSR because of the requirement of additional control packets for node verification process.

ISSN 2348 – 8034
Impact Factor- 4.022

V. CONCLUSION

In this paper, we have proposed a trust based solution for enhancing security against node isolation attack in OLSR protocol for MANET. We have considered a network scenario in which an attacker launches a node isolation attack over a victim. Our proposed approach utilize a trust based MPR selection process, in which trust values for each neighboring node is computed initially and then a global trust is derived for each node in the network . Each node will be listed on the MPR selection only if its global trust value is one. The proposed approach is simulated in NS2 along with conventional OLSR and EOLSR and the results obtained confirm that our approach outperforms the other two in terms of security criteria.

REFERENCES

1. *J. Josh Kumar, A. Kathirvel, N. Kirubakaran, P. Sivaraman and M. Subramaniam, "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT", EURASIP Journal on Wireless Communications and Networking, vol. 2015, no. 1, 2015.*
2. *A. Kathirvel and R. Srinivasan, "ETUS: enhanced triple umpiring system for security and robustness of wireless mobile ad hoc networks", International Journal of Communication Networks and Distributed Systems, vol. 7, no. 12, p. 153, 2011.*
3. *A. Vinoth Kumar, S. Kaja Mohideen and A. Kathirvel, "Performance Enhanced Reverse AODV Routing Protocol for MANETs", Middle-East Journal of Scientific Research, vol. 23, no. 8, pp. 1720-1726, 2015.*
4. *D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation & evaluation of an ids to safeguard olsr integrity in manets," inProc. Int. Conf. Wireless Commun. Mobile Comput., 2006, pp. 45–50.*
5. *D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An advanced signature system for OLSR," inProc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., 2004, pp. 10–16.*
6. *Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," IEEE J. Selected Areas Commun.., vol. 24, no. 2, pp. 370–380, Feb. 2006.*
7. *B. Kannhavong, H. Nakayama, and A. Jamalipour, "Nis01-2: A collusion attack against olsr-based mobile ad hoc networks" in Proc. IEEE Global Telecommun. Conf., Nov. 2006, pp. 1–5.*
8. *J. Ahn, J. Park, W. Cha, S. Kim, P. Mah and T. Lee, "MAC-Aware Concentrated Multi-Point Relay Selection Algorithm in Ad Hoc Networks", Wireless Personal Communications, vol. 86, no. 2, pp. 423-433, 2015.*
9. *A. Kots and M. Kumar, "The fuzzy based QMPR selection for OLSR routing protocol", Wireless Networks, vol. 20, no. 1, pp. 1-10, 2013.*
10. *Network simulator: http:///www.isi.edu/nsnam/ns.*
11. *M. Marimuthu and I. Krishnamurthi, "Enhanced OLSR for defense against DOS attack in ad hoc networks", Journal of Communications and Networks, vol. 15, no. 1, pp. 31-37, 2013*