Analytical Approach to Secure OLSR from Black Hole Attack

Hamela K[1], Dr. A. Kathirvel[2]

[1]*Research Scholar,MTWU,Kodaikanal and Assistant Professor, GFGC,Malur, IndiaBC Institute*

[2]*Professor & HOD, Department of Computer Science and Engineering, MNM Jain Engineering College*

***Abstract* -** A mobile ad hoc network (MANET) is a gathering of self-sufficient hubs that communicate with one another by framing a multi-hop radio system without depending on any standard organize framework. For nodes to communicate with each other nodes, routing protocol places a vital role. In MANET, there are two classification of routing protocol such as pro-active protocol and reactive protocol. For this work we use one of the pro-active routing protocols such as Optimized Link State Protocol (OLSR). A large portion of the routing conventions for MANETs were created with no safety efforts and because of this MANET are influenced by different kinds of attacks. Some of the attack which MANET suffer are Node Isolation attack, Black Hole attack, Grey Hole attack, Co-operative attack, Worm Hole attack etc. In this paper, we are proposing a technique to identify black hole attack and to improve the security of MANET. For this work, we use co-operation rate and path vacant rate to identify the black hole attack and to secure routing path of OLSR in MANET. We also check the performance of our work through NS2 simulation tool.

Keywords - MANET, OLSR, Black Hole Attack

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an impermanent framework less multi-hop remote system in which the hubs can move discretionarily [6]. These systems expand the restricted remote transmission scope of every node by multi-hop packet sending, and appropriate for a situation in which pre-conveyed infrastructure is not established. In an ad-hoc system, there is no fixed infrastructure, for example, base stations not exist. The nodes within the network will communicate with each other through wireless links, the nodes which are away from the range depends on other nodes to transfer messages. In ad-hoc network, frequent change in the network structure also exist. Thus, to communicate between source to destination nodes, the role of routing protocols is very important. Routing protocol [2] in MANET is classified into reactive protocol which has the capability to update its routing information when required, such as AODV, DSR etc and proactive routing protocol which has the capacity to update its routing information frequently, such as OLSR, DSDV. In this work, we try to use one of the pro-active routing protocol OLSR. These types of network infrastructure are finding regularly expanding applications in both military and non-military personnel situations [5].

One of the proactive directing conventions is OLSR [3], which was planned dependent on Link State Protocol. Link State Protocol utilizes customary method for broadcasting all node data to every other node. OLSR utilizes multipoint relay (MPR) for ascertaining the identity of shortest path between neighboring nodes. The flooding system is kept up by MPR, with the goal that it can keep away from the continued transmission of same data again and again. OLSR comprises of two sorts of routing message to be specific HELLO message and TC message. HELLO messages are occasionally traded among neighboring nodes to discover the status of the neighbor nodes. Hello message will keep up MPR determination details. It keeps up a table called neighbor table, which comprise of neighbor node status, and connection status of the nodes to be specific unidirectional, bidirectional and multipoint relay. It very well may be sent just to one hop network. Utilizing TC messages, every node occasionally communicated TC message all through the system. TC message used to send MPR selector list and MPR host will forward the TC message. The principle movement of TC message is to send all topology data to the whole system structure. Multiple Interface Declaration (MID) message is additionally kept up in OLSR [4]. MID used to educate about all the nodes participating in the OLSR routing.

Nodes which go about as black hole send wrong hello messages. This black hole node expands themselves as node with more association to its neighbors. By which, black hole node will be chosen as MPR node. There by black hole node will focus for TC message and attempt to catch the course of the network structure. During Black hole attack, the attacker node transmits fake route in the infrastructure to receive all the packets and after receiving all the packet, it will make the nodes to drop the packets.

The black hole attack is one of the biggest threats in Mobile Ad-hoc network [2]. This work we would like to bring a solution for black hole attack in OLSR in Manet. The rest of the paper is organized as follows, Chapter II talks about Literature Review. Chapter III deals with mechanism to eradicate black hole attack. Chapter IV evaluate the implementation work and Chapter V focus on simulated result and we conclude in Chapter VI.

II. LITERATURE SURVEY

First, Hicham Amraoui et al[7], proposed a new idea based on a game theoretic approach to improve OLSR security mechanism in MANETs. Each node keeps a cooperation rate (CR) record of other nodes to cope with the behaviours and mitigate aggregate effect of other malicious devices. Two strategies during this suggested model was adopted to identify the cooperate and not-cooperate rate of the nodes through game theory model.

S Sankara et al[8], proposed a defence mechanism is presented against these black hole attacks in a MANET. This work makes use of the MAC address of the destination to check the validity of each node in its path thereby providing a direct negotiation for secure route. The simulation is carried out on the proposed scheme to demonstrate the effectiveness of the mechanism in mitigation of the attack while maintaining a reasonable level of throughput, packet delivery ratio and end to end delay in the network.

Shashi Gurung et al [9], proposed a model called as Mitigating Black Hole effects through Detection and Prevention (MBDP-AODV). Their work is based on a dynamic threshold value of the destination sequence number. By this method black hole can be prevented and detected. This validity of the model is verified by NS-2.35 simulator.

J. Kumar et al [10], proposed the attacked produced to AODV due to black hole node had been evaluated and solution to prevent black hole attack has been proposed. The original AODV will be modified to detect routing behaviour and alert other nodes about attacker node. This proposed work is implemented through NS2 simulator

III. MECHANISM FOR ELIMINATING BLACK HOLE ATTACK

Before Our research area is majorly focused in Optimized Link State Protocol (OLSR). It is one of the widely used routing protocols. In this work, we introduced the co-operation concept among the nodes to improve the performance of the node. The node co-operation rate (NCR) indicates the value of how many times node co-operates and not co-operate during its network lifetime. In this work, each node whose NCR>0 is legitimate node and NCR<0 is considered to be non-co-operative node or fake node. Through this co-operative value, each node can identify the behaviors of neighbor node before sending a packet.

The work mechanism is as follows:

Step 1: Firstly, each node maintains node co-operation rate (NCR) [11] of other node to avoid fake node.

$$NCR(i,t,F) = \sum(x_1(t) + x_2(t)) \quad (1)$$

Where NCR is node co-operation rate, the joint exertion rate of focus point (i) at time interval (t) and in light of a structure operation (F).

Step 2: To calculate the vacant rate of each path [11], which can be identified by the routing path load, main paths and nodes arrangement over multi-path. The vacant rate of each path is calculated by

$$vr_i = \frac{\sum_{i=1}^{N} PI(P_i) - PI(P_i)}{\sum_{i=1}^{N} PI(P_i)} \quad (2)$$

where vr is vacant rate of the path i is v_i and $V = \{v_i, 1 \le i \le m\}$ and $PI(P_i)$ is the path importance index, which calculates a measurable indicator of a path in multi-paths.

Step 3: We have found node co-operative rate (NCR) and path vacant rate(vr), which identifies set of optimal solution. From the optimal solution to calculate the best path between source to destination we use evolutionary game theory approach is used. To obtain single optimal solution we used Rastrigin's function(f i,j)[11]:

$$f(i,j) = \sum_{i=1}^{n}\left[p_i^2 - 10\cos(2\pi\,\mathrm{p_i}) + 10\right] \quad (3)$$

Step 4: Identify the number of possible paths between source node to destination node using co-operation rate and path vacant rate. The possible path is represented Pi

$$p_i = \frac{p_i(y_j) - I_i}{\sum_{l=1}^{m}(p_l(y_j) - I_l)}; \quad j = 1,2,\ldots,d \quad (4)$$

where d is the number of restrictions used for this optimization and the function of path1, $i = 0$ (for example) as follows:

$$p_i(y_j) = p_1(y_1) + p_1(y_2) + p_1(y_3); \quad i = 1, j = 3 \quad (5)$$

Step 5: To find the suitable path from source to destination path, we try to apply Pareto-talented Nash Equilibrium game theory.

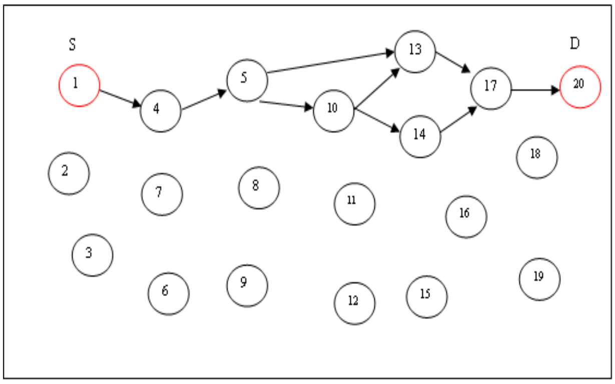
[1] Nash equilibrium is when no player in a game can increase his or her payoff by unilaterally changing their actions.

[2] Pareto optimal is when it is not possible to make any player better off in the game without hurting another player at the same time.

[3] So, to find the optimal path between the source and destination, game theory approach is used and with the help of multi-evaluation metrics values of one path compared with another path.

And node with higher pay-off is taken for path selection. Through this method we will be able to find optimal path between source and destination by avoiding black hole attack.

IV. WORK IMPLEMENTATION



Consider a network sample model for our implementation work. Here, we consider possible paths are 1-4-5-13-17-20, 1-4-5-10-13-17-20, and 1-4-5-10-14-17-20 as per our model.

Step 1: As per our model, we want to compute the co-operation rate and path vacant rate for each node in the network.

Cooperation rate (NCR) from formula(1) is :

$$\mathrm{N}CR(i,t,F) = \sum\left(x_1(t) + x_2(t)\right)$$

Where $x_1(t)$, $x_2(t)$ is the data transmission and receiving delay. For this case, we consider the Tx and Rx delay as follows.

CR (1, 9.01 time, 1) = (0.5 + 0.5) = 1
CR (1, 9.02 time, 2) = (0.4 + 0.3) = 0.7
CR (1, 9.03 time, 3) = (0.5 + 0.3) = 0.8
CR (1, 9.04 time, 4) = (0.4 + 0.5) = 0.9
……………………………

So, for this 4 seconds CR for node 1 = 0.85
Similarly we compute the CR for every node.
We consider, the CR as follows

CR (1) = 0.85	CR (13) = 0.79
CR (4) = 0.8	CR (14) = 0.82
CR (5) = 0.7	CR (17) = 0.75
CR (10) = 0.82	CR (20) = 0.72

The average CR for possible paths as follows.

CR (P1) = 1-4-5-13-17-20 = Avg (0.85, 0.8, 0.7, 0.79, 0.75, 0.72) ~ 0.75

CR (P2) = 1-4-5-10-13-17-20 = Avg (0.85, 0.8, 0.7, 0.7, 0.79, 0.75, 0.72) ~ 0.72

CR (P3) = 1-4-5-10-14-17-20 = Avg (0.85, 0.8, 0.7, 0.7, 0.82, 0.75, 0.72) ~ 0.74

Step 2 : Calculate Path vacant ratio using the formula(2) given below

$$vr_i = \frac{\sum_{i=1}^{N} PI(P_i) - PI(P_i)}{\sum_{i=1}^{N} PI(P_i)}$$

1--------4 -------5--------13-----17-----20

VR(P1) = (0-1) + (1-1) + (2-1) + (2-1)+ (2-1)+ (1-1) / (0+1+1+2+1+1) = 0.333333

1--------4---------5-------10-----13------17-----20

VR(P2) = (0-1) + (1-1) + (2-1) + (1-2)+ (2-1)+ (2-1) +(1-1) / (0+1+1+1+2+1+1) = 0.143

VR (P3) = 0.4322

Step 3: Then apply Evolutionary game theory for best path selection and identify path between source and destination

$$p_i = \frac{p_i(y_j) - I_i}{\sum_{l=1}^{m}\left(p_l(y_j) - I_l\right)}; \qquad j = 1, 2, \ldots, d$$

$$p_i(y_j) = p_1(y_1) + p_1(y_2) + p_1(y_3); \qquad i = 1, j = 3$$

Here, the possible paths involved with 8 nodes only… so i= 0, 1, 2, 3, 4, 5, 6, 7, 8 and the j= 1, 2 (computed metrics)

P1 (1) = 0.75+0.3333 = 1.0833
P2 (2) = 0.72+0.143 = 0.8633
P3 (3) = 0.74+0.4322 = 1.1722
Then

P1 = (1.0833 – 1) / ((1.0833-1) + (0.8633 – 1) + (1.1722-1) = 0.7

P2 = (0.8633 – 1) / ((1.0833-1) + (0.8633 – 1) + (1.1722-1) = -1.15 (value will be in negative so it will subtract from 1) now we get = 0.15

P3 = (1.1722-1) / ((1.0833-1) + (0.8633 – 1) + (1.1722-1) = 1.449

Then it will check with the following function

$$f(i, j) = \sum_{i=1}^{n}\left[p_i^2 - 10\cos(2\pi\, \mathrm{p}_i) + 10\right]$$

f 1(1, 20) = (0.72 – 10 cos (2 *PI* 0.7) +10) = 0.521
f 2(1, 20) = (0.152 – 10 cos (2 *PI* 0.15) +10) = 0.0245
f 3(1, 20) = (1.4492 – 10 cos (2 *PI* 1.449) +10) = 2.225601

Step 5: To find the optimal path apply Pareto-talented Nash Equilibrium game theory, with the usage of Hi-Lo game model, compute the paths.

i). Choose path 1, 2

		L	R
I	U	0.72, 0.143	0.521
	D	0.0245	0.75, 0.333

ii). Choose path 1, 3

		II	
		L	R
I	U	0.74, 0.4322	2.225601
	D	0.521	0.75, 0.333

We get the optimal path by using co-operation rate and path vacant rate for each node and the best path will be taken for transferring of data packet between source and destination nodes. The resultant best path which we get as per our model are shown in figure 2.

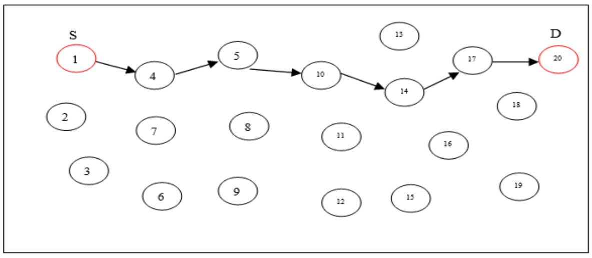


Figure 2 The resultant path

VI CONCLUSION

In this paper, we discussed analytical approach to eliminate black hole attack in OLSR. The work comprises of OLSR routing protocol with secured features like co-operation rate and path vacant rate along with evolutionary game theory which provide security to the network model. The proposed work is efficient in terms of delay, routing overhead and throughput.

VII REFERENCES

[1] Hongmei Deng, Wei Li and D. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, 2002.

[2] C. Brill and T. Nash, "A comparative analysis of MANET routing protocols through simulation", 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), 2017.

[3] Thomas Clausen et.al, "Optimized Link State Routing Protocol", http://www.ietf.org/internet-drafts/draftietf-manet-olsr-11.txt , July 2003.

[4] Hamela K, Kathirvel Ayyaswamy, Identifying various routing attacks in Optimized Link State Protocol, International Journal of Scientific & Engineering Research –IJSER, Volume 8, Issue 5, May-2017 29 ISSN 2229-5518

[5] Hamela K, Kathirvel Ayyaswamy, Measuring performance of OLSR and EOLSR during routing attack, International Journal of Innovative Research in Computer and Communication Engineering. ISSN(Online) :2320-9801, Vol.5, Special Issue 2, April 2017, PG 171 - 177

[6] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless Communications, vol. 14, no. 5, pp. 85-91, 2007.

[7] H. Amraoui, A. Habbani, A. Hajami and E. Bilal, "Security-Based Mechanism for Proactive Routing Schema Using Game Theory Model", Mobile Information Systems, vol. 2016, pp. 1-17, 2016.

[8] S.Sankara Narayanan and Dr.S.Radhakrishnan, "Secure AODV to Combat Black Hole Attack in MANET", 2013 International Conference on Recent Trends in Information Technology (ICRTIT), ISBN:978-1-4799-1024-3/13/$31.00 ©2013 IEEE, Pg 447 - 451

[9] Shashi Gurung, Siddhartha Chauhan,"A dynamic threshold based approach for mitigating black-hole attack in MANET",Wireless Networks, Volume 24 Issue 8, November 2018, Pages 2957-2971

[10] J. Kumar, M. Kulkarni, D. Gupta and S. Indu, "Secure route discovery in AODV in presence of blackhole attack", CSI Transactions on ICT, vol. 3, no. 2-4, pp. 91-98, 2015.

[11] Hamela K, Dr. A.Kathirvel, "Alleviating black hole attack in olsr protocol adopting an evolutionary game theory approach for manet", Journal of Adanced Research in Dynamical and Control Systems, Vol 9, Sp-17/2017,pp. 666-678.

[12] F. Shi, W. Liu, D. Jin and J. Song, "A cluster-based countermeasure against blackhole attacks in MANETs", Telecommunication Systems, vol. 57, no. 2, pp. 119-136, 2013.

[13] M. Burmester and B. de Medeiros, "On the Security of Route Discovery in MANETs", IEEE Transactions on Mobile Computing, vol. 8, no. 9, pp. 1180-1188, 2009.

Hamela K was born in Chennai, India, received her MCA degree from Bharathidasan University, Tiruchirappalli, India in 2002, MPhil degree from Mother Teresa Women's University, Kodaikanal, India in 2004 and MBA degree from Alagappa University, Karaikudi, India in 2010. She is currently pursuing Ph.D in the area of "Mobile Ad Hoc Network" at Mother Teresa Women's University, Kodaikanal, since August 2014. She is working as Assistant Professor in Computer Science department, Government First Grade College, Malur, Karnataka, India.

Dr.A.Kathirvel - born in Erode, Tamilnadu, India, received his B.E. degree from V.M.K.V. Engineering College, University of Madras, Chennai, in 1998, M.E. degree from Crescent Engineering College, University of Madras, Chennai, in the year 2002 standing 7th rank in the University. He got University medalist and Best Project Award in his PG Degree studies. His Doctoral Degree from Anna University, Chennai in 2010. He has got teaching, research and administrative experience of more than 20 years in various engineering colleges, autonomous institutions and universities. He is currently working as Professor and Head in Computer Science and Engineering at Misrimal Navajee Munoth Jain Engineering College, Chennai. He has worked as Lecturer, Senior Lecturer, Assistant Professor, Associated Professor, Professor, and Professor & Head in various institutions. He has published more than 100 papers in national and international conferences and in international journals. He is working as scientific and editorial board member of many journals. He has reviewed dozens of papers in many journals. He has author of 11 books. He has also published a research monograph from the LAP Lambert Academic Publishing GmbH & Co., Germany, Europe based on his Ph.D thesis titled "Umpiring Security Model and Performance improvement on MANETS", costing 110.35 Euros. His other two books are Introduction to GloMoSim and Prevention of Attacks using Umpiring Security Model for MANETS, LAP Lambert Academic Publishing GmbH & Co., Germany. Europe. He is a Life member of the ISTE (India), Senior Member IACSIT (Singapore), Life Member IAENG (Hong Kong), Member ICST (Europe), IAES, Member IEEE and ACM. He has given several guest lecturers/expert talks and seminars, workshops and symposiums. He has visited Dubai, Abu Dhabi and Oman for presentation of his research papers in various international conferences. His biography was published in 29th edition of Marquis's Who's Who in the World in 2012 issue. He has also guided more than 3 dozen projects (B.E/B.Tech/M.E/M.Tech/MCA) in various engineering colleges. He has given many keynote/invited talks/ plenary lecturers in various national and international conferences and chaired many sessions. His research interests are protocol development for wireless ad hoc networks, security in ad hoc network, data communication and networks, mobile computing, wireless networks and Delay tolerant networks.