I J C T A, 9(11) 2016, pp. 5377-5382

ENERGY EFFICIENT ALGORITHM FOR DETECTION OF BLACK HOLE ATTACK IN MANET

Manmohan Sharma[*], Baljinder Singh[**] , Anurag Singh Tomar[***]

Abstract: A collection of two or more devices (Mobiles, PDA's and Laptop) with multi-hop wireless communication is called mobile ad hoc network (MANET). The communication in MANET happens among different nodes within transmission range and outside the transmission range. Due to MANET's fundamental characteristics like flexibility, without any fixed infrastructure and any node can leave or join the network at any time without any confirmation resulting into various types of security issues. One of them is black hole attack, a malicious node in this attack fakes itself as node having the shortest path from source to destination. This paper provides the usage of energy in an efficient way with help of clustering and by using various types of verification of the route reply nodes to improve the security against the black hole attack.

Key Words: MANET, Balck hole attack, Energy efficient, Distance_time, node value, Cluster head.

1. INTRODUCTION

MANET [1] is a temporary network where the collections of wireless mobile nodes are present without the usage of a predefined infrastructure and centralized administrator. Communication between two nodes performed via radio links. The main objection in constructing a MANET is each mobile device easily equips the changes which monotonously maintaining information. MANET is a type of Wireless ad hoc network that has a routing management on the link layer. MANETs consist of an auto-configuring network, which has ability to make point to point links and further stores itself into a routing table.

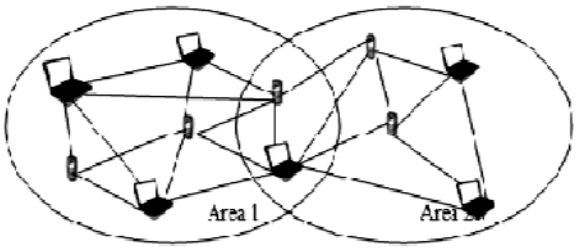

Figure 1- Mobile ad hoc network

[*] Department of Computer Science and Engineering Lovely Professional University Phagwara, Punjab, India
Email: manmohan_er@yahoo.co.in

[**] Department of Computer Science and Engineering Lovely Professional University Phagwara, Punjab, India
Email: sidhuekam32@gmail.com,

[***] Department of Computer Science and Engineering Lovely Professional University Phagwara, Punjab, India
Email: aunragtomar3105@gmail.com.

MANET is an open network, which is easy to attack as compared to wireless or wired network, so security [10] is main concern in. There are two types of attacks are possible on MANET: Internal attack is performed by any node or attacker from the inside the network and external attacks are performed from outside the network. Two main categories are present of attacks: Active and Passive attacks. Active attack like Black hole attack [2][7][9], it is a major security attack in MANET, and in this network malicious node behaves like an original node which has truly shortest path to the destination node. Malicious node drop all the packets are called black hole attack. Transmission of the packets are done with the help of routing protocols, Routing in MANET [2] is very different from other networks like wireless network. Routing in the MANET is depends on some factors like route request, route reply and topology. In MANET every node act like router, every node can send the data or receive the data without using of any router. We use the term energy efficient which means less usage of the energy to send the packets from source to destination. By using this we increased the lifetime of the network. We use the concept of clustering [6] which means a natural arrangement of nodes in the groups. One node become the cluster head from multiple nodes based on the energy, serve time, connected links etc. This is very extensive that every node in the MANET should have enough energy to send and receive the packets. We make clusters on basis of area. Many algorithms related to energy efficiency [8], detection of attacks [11] and black hole nodes which are based on different parameters like weight based clustering algorithm, detection of black hole using watchdog technique etc.

We use the various step verifications for detecting the black hole attack in the MANET with energy efficient. In this paper, various cases are made on basis of requirements of the users like more secure communication with energy efficiency, less secure with energy efficiency, more security without energy efficiency and minimum security without energy efficiency.

Related work

Neha and Manmohan Sharma [1] proposed an algorithm for the detection of black hole attack in the mobile ad-hoc network. In the first step check the malicious table and match the id of node which is send the route replies with the malicious table. In the second step of the verification sender node ask the next node about the true path to the destination, if the next node verified the path then the sequence number and node id is stored in the RREP table else if node does not verified the path the id and sequence number of that node is stored in malicious table then Select the one sequence number from the RREP table and compare with all other. Abbas Afsharfarnia and Abbas Karimi [4] proposed the clustering algorithm for decreasing the usage of energy in MANET. In this paper weight of each node has been calculated by using various parameter like neighborhood degree of sharing, speed and energy of the particular link. Ritul Kumar and Ruchika Monga [5] described the clustering based algorithm for increasing the lifetime of the network. The dynamic formation of clustering has been done by after checked the battery power, mobility and from the serve time for increasing the lifetime of MANET. Mandeep Singh, Mr.Gagangeet Singh [6] described the study of different cluster head algorithms for MANET which is reduced the energy consumption, increase the security of network and raise the lifetime of the network. The selection of cluster head is divided into two methods first is distance constrained selection and second is size constrained selection. Nodes select the cluster head on the basis of maximum energy level

Proposed work

In our proposed work, we detect the black hole attack from MANET with energy efficiency. In the previous work, we understand that in the MANET problem of energy efficiency is still there and the security of our data packets is big issue. There are several techniques which are used in

detection the black hole attack and to save the energy of network but our algorithm is able to detect the malicious at various levels with the usage of energy efficiency by using clustering model.

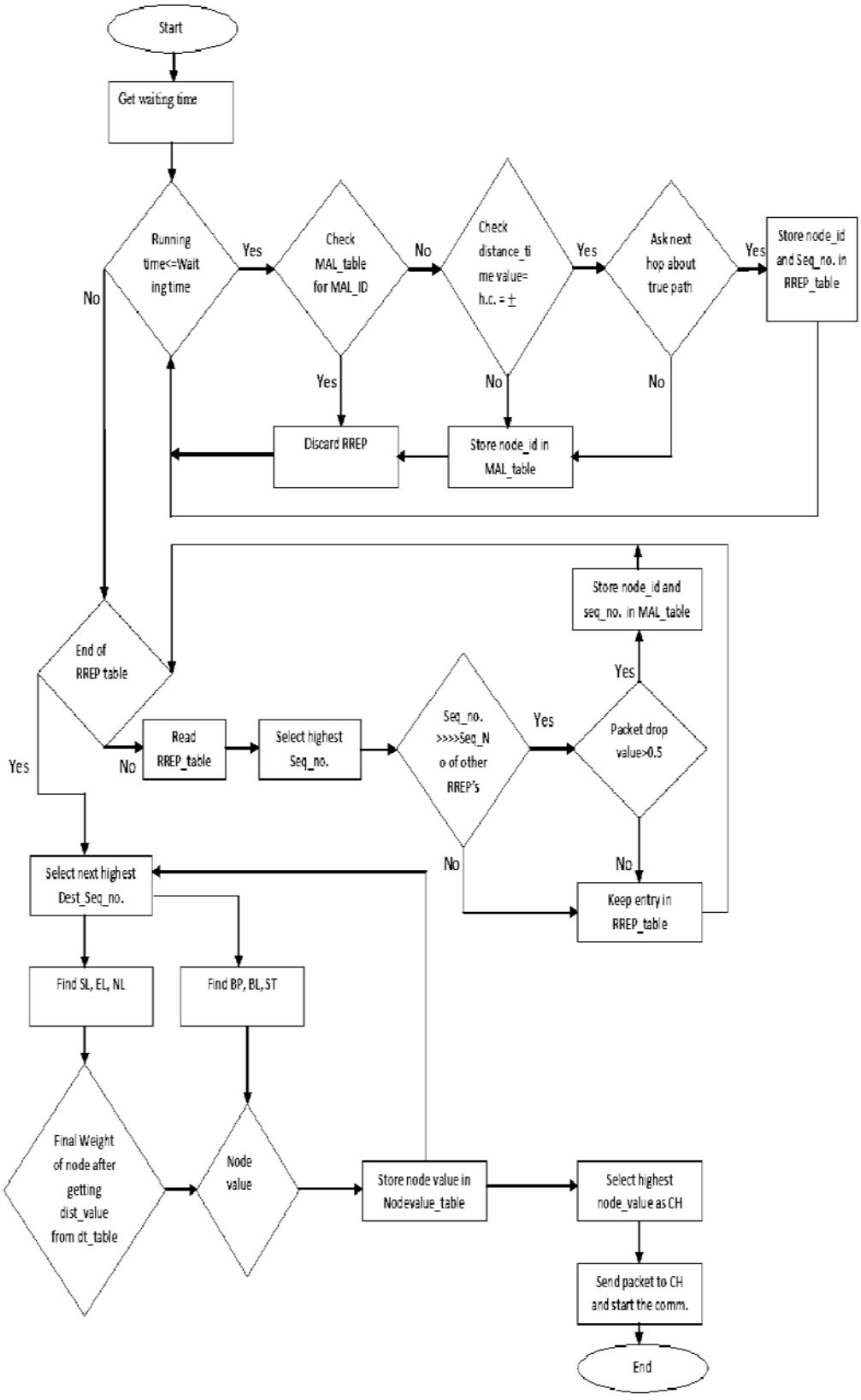

Figure 2- Flow chart of proposed algorithm

Step 1: Get current time (Time at which route request message is sent)

Step 2: Get waiting time (WT).

Step 3: While (RT<=WT).

Verification of route reply messages are done by various step verifications.

Step A: Check for malicious node.

(i) After getting route replies from intermediate nodes, check the malicious_table for malicious node_id which is formed on the basis of previous traffic.

(ii) If node_id is matched with the malicious_table, then discard the route reply.

(iii) If node_id is not found in the malicious_table, then go to step ii.

Step B: Check the distance_time value.

(i) If distance_time value matches with expected hop count value, then store that value in dt_table and go to step C.

(ii) Else discard the route reply.

Step C: In this sender node ask the next hop that node replied for the route request message has a path to destination or not.

(i) If next hop confirms that replying node has path, then node_id and seq_no. is stored in RREP_table.

(ii) Else node_id and seq_no. is stored in malicious_table.

Step D: Once the running time (RT) is greater than waiting time (WT) all verifications are done of route reply messages.

Now select one seq_no. from the RREP_table. While (End of RREP_table is not reached) do two step verification.

(i) Compare the selected seq_no. with all other seq_no. which are present on the RREP_table, if seq_no. is exceptionally high than do next step verification and go to step D (ii).

(ii) In this, the value of packet drop is checked here, if it is greater than 0.5 then store that node_id in malicious_table otherwise node_id keep in RREP_table and go to step E.

Step E: Once the all seq_no. are verified then select one highest seq_no. from the RREP_table. While (End of RREP_table is not reached), find the cluster head.

(i) Find the final weight of node using speed of link (SL), energy of link (EL) and neighborhood links (NL) and distance_time value which is getting from dt_table.

Final weight of node = (F1 * SL) + (F2 * EL) + (F3 * NL) + distance_time value.

$SL = \frac{S_a+S_b}{2}[4]$, $EL = \frac{E_a+E_b}{2}[4]$

a and b are two connected nodes. S_a and S_b are their speed.

E_a And E_b is the consumed energy by two nodes.

E_a is the energy of node A and E_b is the energy of node B.

F1, F2, F3 are weight factors.

F1 + F2 + F3 = 1.

(ii) Then find the battery power (BP), buffer length (BL) and serve time (ST) and go to step F.

Step F: Find the node value by adding the final weight of node and all the components of step E (ii).

Node value = Final weight of node + BP + BL + ST.

And store the node value in node_value_table.

Step G: Select one highest node value from the node_value_table and make that node cluster head then send the packets to that cluster head. Cluster head will select from neighbor nodes of the sender.

Step H: Delete all other seq_no. from RREP_table.

2. CONCLUSION-

This paper provides an introduction of MANET and black hole attack. In this, work is done to increase the energy efficiency to secure the MANET with having the values like distance_time value, node value and packet drop value. Further the work can be done to reduce the overhead of this algorithm. By doing so less will be the energy consumption and more reliable, secure will be the network.

References

[1] Neha and Manmohan Sharma, "Step Verification for Detection of Black Hole Attack in MANET", International Journal of Applied Engineering Research (IJAER), vol. 3 number 55 (2015), pp. 2887-2891.

[2] H. Deng, W. Li, D.P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazines, vol. 40, no. 10, October 2002.

[3] Priyanka Goyal, Vinti Parmar, Rahul Rish, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[4] Abbas Afsharfarnia, Abbas Karimi, "A New Clustering Algorithm Using Links' Weight to Decrease Consumed Energy in MANETs", TELKOMNIKA, Vol.12, No.2, June 2014, pp. 411~418.

[5] Ritul Kumar1 and Ruchika Monga, "CLUSTER BASED ENERGY EFFICIENT PROTOCOL TO INCREASE NETWORK LIFETIME IN MANETS", Special Issue, Vol. 1, No. 2, July 2015 National Conference on "Emerging Trends in Electronics & Communication" (ETEC-2015) © 2015 IJEETC.

[6] Mandeep Singh, Mr.Gagangeet Singh, "Secure and Efficient Cluster Head Selection Algorithm for MANET", Journal of Network Communications and Emerging Technologies (JNCET), Vol. 2, Issue 2, June (2015).

[7] Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4 Apr 2011, pp. 2832-2838.

[8] Yonghui chen, chunfeng zhang, zhiqin liu, "Energy Efficient Routing Protocol Based on energy of node and Stability of Topology", Third International Conference on Information and Computing, 2010.

[9] Alfy Augustine and Manju James, "Black Hole Detection using Watchdog", International Journal of Current Engineering and Technology, Vol. 5, No. 4 (Aug, 2015).

[10] Luhach, A.K., Dwivedi, S.K. and Jha, C.K., " Applying SOA to an E-commerce system and designing a logical security framework for small and medium sized E-commerce based on SOA", Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on (pp. 1-6), IEEE.

[11] Kumar, A., Luhach, A.K. and Pal, D., "Robust digital image watermarking technique using image normalization and discrete cosine transformation", International Journal of Computer Applications, 65(18).