Middle-East Journal of Scientific Research 23 (7): 1358-1360, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.07.106

An Efficient Neighbor Node Detection Using AODV in MANET

C. Aparna and C. Nelson Kennedy Babu

Thamirabharani Engineering College,Tirunelveli (Tamilnadu), India

Abstract: MANET is a self configuring and centralized multi hop wireless network. Adhoc achieve efficient routing but due to high mobility network can change the structure dynamically so route may be disconnected and route selection, route combinations are not an easy issue to solve. Especially detecting vulnerable node to both internal and external attacks are challenging and major issue in the Adhoc network. This problem affects routing efficiency and performance of the network. In this paper, suggest for ADOV routing protocol based on signal to noise ratio, intensity, flow capacity and set the relative position of the node in MANET. By adding this extra parameter we can easily detect both internal and external attacks. Proposed approach provides optimal secure routing to give the appropriate solution against neighbor attacks in MANET. The performance of proposed system is simulated by NS2.

Key words: MANET · AODV · Flow capacity · Node position · Signal velocity and intensity · Adhoc routing

INTRODUCTION

To increases the performance of the network, we considering a node which are good and reliable one. In this paper categorized good node and bad nodes depends upon their transmission range, packet size signal velocity and flow capacity, Moreover we can test each node how fast they can perform and complete the task with in a time slot. Detecting a neighbor node signal strength is calculated based on fixed transmission range of the network is 250 meter [1]. In an addition AODV[2,3] routing protocol is used to analyzed by proposed approach. This prototype simulated by ns-2, implemented by Linux-5.3 and tested it over an IEEE 802.11a based on adhoc mode approach. In our proposed system enforcing mechanism, node can discover the routing process.

The paper is organized as follows: We discuss the effect of neighbor nodes in AODV in section II. Motivate the research work in section III. In section IV suggest for proposed method. Simulation results are described in Section V. Finally Section VI concludes with future work.

ADHOC on Demand Distace Vector Routhing: AODV enables self-starting, multi hop and dynamic routing protocol. Nodes can establish and maintain the network during the discovery process only on demand. If any link faults then failure node send this notification to their upstream neighbors and so on. Until it reaches to the source. Source can re-route this discovery process only on demand. There is a two main progress in ADOV they are,

Route Discovery: Source node broadcast a route request message (RREQ) to the neighbors. If any nodes request a new route immediately send a reply (RREP) to the source node. Suppose the node does not have a route reply then rebroadcast the (RREQ).

Node Connectivity: Source node can maintain the routing table. Node can periodically send a message to the neighbor node. Source Table updated that information and assigns the lifetime for the responding node.

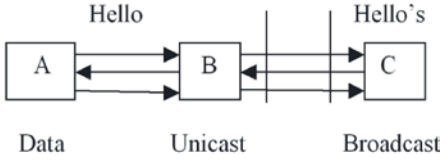

Fig. 1: Topology testing for route Discovery.

Corresponding Author: C.Aparna, Thamirabharani Engineering College, Tirunelveli (Tamilnadu), India.

Motivation and Related Work: When route discovery process is initiated we need to test the network range then Hello message is send periodically to the neighbors. when network changes the hello message is not received within a period of time the route expire in the network as discussed in section II. [4] has Proposed neighbor detection using signal to noise ratio [SNR]. [5] has suggested stability and hop count based approach for route computation and discussed life time of the link. [6, 7] calculate the probability rate for signal strength and packet delivery rate for every network transmission [Ntr]. For that it can analyzed capacity of the network to achieve maximum throughput.

Proposed Work: We proposed to detect good neighbor node in adhoc routing, so differentiate good neighbor and bad neighbor node in MANET. In a route discovery initiate total number of nodes in the network and also calculate transmission range. Hello broadcast message send to the neighbors (RREQ) after getting reply (RREP) calculate time and reach hello message. Compare network transmission range (NTr) with Total Transmission range (TTr). For this calculation we can measure signal strength of hello message and time period between two successive hello packets and link connectivity.

Measure signal intensity then calculate threshold value, if maximum threshold value is evaluated then set timer and judge relative position. Further we can calculate flow capacity of a node if the flow capacity is good store the address otherwise remove the address in the routing table. Figure 2 shows detailed process flow of proposed approach.

In our experiment initially node defines required quality of the link i.e., using the link SNR values shows the range suppose SNR range is vary then node is not moving, For that we can differentiate between good and bad neighbor node easily. This method minimizes the energy consumption and increases the battery life.

In this approach we suggest some parameter to detect good neighbor in MANET. This method increases the size the routing table same as in AODV but these parameter individually detect the attack in every stage. [8] Has suggested a distributed intrusion detection system for AODV. It has some limitation which can't detect impersonate, when the mobility is high, so that accuracy is decreased automatically.[9] has proposed the number of necessary nodes for adhoc network areas, ensure that the limitation of covering and collecting data from an arranged network. Our proposed method analyzed all criteria and their complexities, which are suitable for the effective 0.communication, are discussed in Section V.

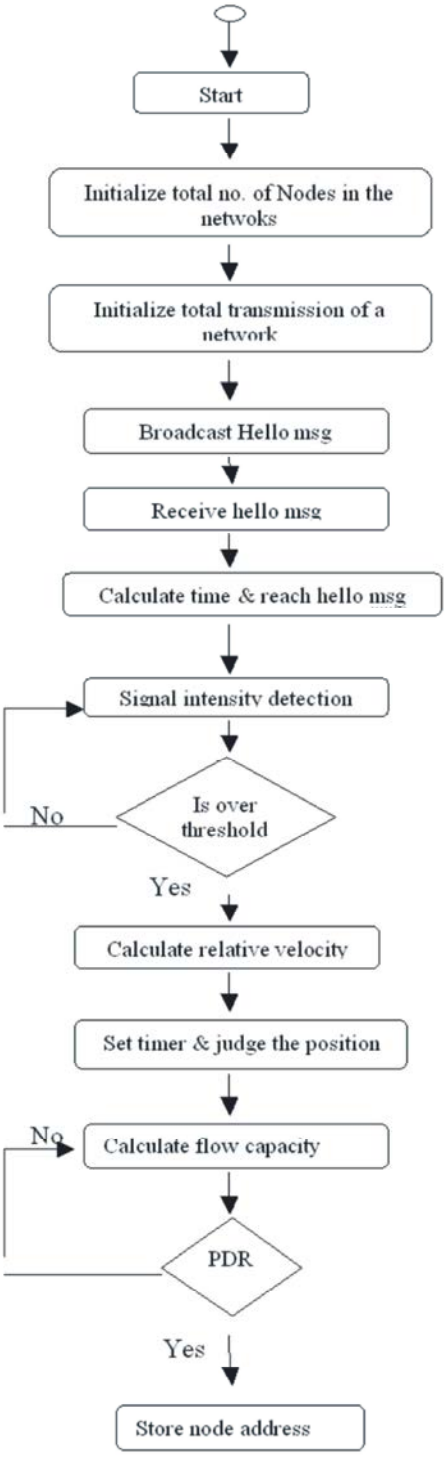

Fig. 2: Process flow of proposed system.

Simulation: Proposed approach compares its results with existing protocols along with limited parameter.Initially it has been assumed their own parameter values with dynamic movements.

Simulation Parameter	Values
No.of.Nodes	5-10
Simulation time	100sec
MAC layer	IEEE 802.11
Packet size	512
Pause Time	I0-100 sec
Packet Rate	4 m/s
Area	670*670
Tx power and Rx Power	0.15,0.04
Transmission threshold power	0.28
Transmission Range	250m
Delta_SNR	5-10db

In this approach used IEEE802.11 as a MAC Layer and original AODV developed by using Linux-5.3 and ns-2.33.The simulation parameters are summarized as follows in Table 1.

In our simulation had provided a significant improvement. This Results shows to increasing the parameter values how the routing overhead can be reduce gradually one by one. Finally it demonstrates good quality of packet delivery ratio and also achieve maximum throughput which is almost 90-95% where as the existing AODV routing protocol performance between 80%-85%.

CONCLUSION

In our proposed approach all related information are covered only detection of good neighbor in adhoc routing protocol. Our experimental result shows the improvement of network performance and also achieve maximum throughput for both fixed and dynamic transmission. We look forward the further development of the ADOV protocols, its performance will be improved in future by reducing delay in communication.

REFERENCES

1. Singh Umang, B.V.R. Reddy and M.N. Hoda, 2011. GNDA: Detecting good neighour nodes in adhoc routing protocol, International Conference on information Technology.
2. Perkins, C.E. and E.M. Royer, 1998. Ad hoc on demand distance vector (AODV) routing," Internet-Draft, draft-ietf-manet-aodv-02.txt.
3. Krco Srdjan and Marina Dupcinov, 2003. Improved Neighbor Detection Algorithm for AODV Routing Protocol, IEEE Communications Letters, 7(12).
4. Li, Qing, Cong Liu and Hang Hong Jiang, 2008. The Routing Protocol of AODV Based on Link Failure Prediction, ICSP2008 Proceedings, 978-1-4244-2179-4/08/$25.00 ©2008 IEEE.
5. Sridhar, K.N. and Mun Choon Chan, 2005. Stability and Hop-Count based Approach for Route Computation in MANET, 0-7803-9428- 3/05/$20.00 © IEEE.
6. Gupta, P. and P.R. Kumar, 1998. Critical Power for Asymptotic Connectivity in Wireless Network" In W.M. McEneany, G. Yin and Q, Zhang, editors, Stochastic Analysis Control, Optimization and Applications, pp: 547-566, Birkhauser, Boston, MA.
7. Gupta, P. and P.R. Kumar, 2000. The Capacity of Wireless Networks, IEEE Transactions on Information Theory, 46(2): 388-404.
8. Trang Cao Minh, Hyung, Yun Kong and Hong Hee Lee, 2006. A Distributed Intrusion Detedtion System For AODV, IEEE, 1-4244-0574-2/06.
9. Kim, Youngrag, Shuhrat Dehkanov, Heejoo Park, Jaeil Kim and Chonggun Kim, 2007. The Number of Necessary Nodes for Ad Hoc Network Areas, IEEE Asia-Pacific Services Computing Conference.