International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-2, Issue-2, March-2014

An Enhanced AODV Routing Protocol to detect and isolate selfish nodes in Manets

Yogesh Bansal

Abstract - **The fact that security is a critical problem when implementing mobile ad hoc networks (MANETs) is widely acknowledged. One of the different kinds of misbehaviour a node may exhibit is selfishness. A selfish node is a node which avoids the forwarding activity due to its current low power status or it feels so over utilized in the forwarding activity and fears that it will drain so much power that it will not have enough energy to send or receive its own packets in the future. This selfish behaviour problem is quite common in ad hoc networks. One way of preventing selfishness in a MANET is a detection and exclusion mechanism. In this paper, we have proposed an Enhanced AODV routing protocol to detect and isolate selfish nodes from the network in MANETs. The strategy assumes that the selfish nodes are not malicious and obligated to speak truth about their current energy level.**

Index Terms – **AODV, EAODV Routing Protocol, Mobile Adhoc Network, Selfish Nodes.**

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are distinguished from other communication networks by many features. First, mobile nodes in MANETs may move freely in the absence of a fixed infrastructure. Therefore, frequent changes in routes may happen due to unpredictable topology changes and link disconnections. Second, nodes in MANETs have limited resources such as energy, bandwidth, and computational power. Finally, MANETs have no trusted centralized authority. The initial routing protocols in MANETs such as AODV [1], DSR [2], TORA [3] etc. were devoid of security features and assumed that the all the nodes in the network will behave in the rational manner and extend the desired cooperation required for the multihop routing. Later it was found that it is wrong to assume that all the nodes would behave rationally and selflessly forward the packets for other nodes [4]. It may be due to malicious or non-malicious (for example, low residual power) [5] nature of nodes. It is quite possible that a node which was earlier trustworthy may no longer continue to be so as it may become selfish due to its energy constraints. Such a node is not basically malicious but is unwilling to spend its residual energy for forwarding the data packets of other nodes. As the time passes by, there is an increase in such type of nodes which can have disruptive effect on the activities of the network and may bring the network activity to near halt. There arises the need to detect and isolate such nodes so as to avoid the degradation of the performance of the network.

This paper is organized as follows. Section II summarizes the literature survey of the related work. Section III introduces the concept of EAODV protocol. Section IV describes the proposed routing mechanism. Section V specifies the simulation parameters that have been used for simulation. Performance metrics has been described in Section VI. The results of the simulations of both protocols are presented in section VII. Finally, conclusions and future scope are given in Section VIII and IX.

Manuscript Received March 23, 2014.

Yogesh Bansal, Assistant Professor in Computer Science/Information Tech. Baddi University of Emerging Sciences and Technology, Baddi. India.(e-mail: er.yogesh.it@gmail.com)

II. LITERATURE SURVEY

The ad hoc networks provide ubiquitous connectivity without the need of fixed infrastructure. This makes them very suitable choice when the communication has to be provided temporarily such as in case of battle field, disaster hit area or to create a network between members of an interim group. Such a network is composed of mobile nodes which are powered by the battery. Therefore energy is a precious resource for all the nodes participating in the communication process and has to be used very carefully spent by every node who intends to stay alive in the network. The communication in the ad hoc network takes place using the concept of forwarding where a source node sends a packet to a far off destination node using intermediate relay nodes. This mechanism of transmission through relay node leads to the better connectivity and lower cost of power transmission than in case of direct transmission over large distance. Since the traffic in an ad hoc network is through the relay nodes hence it is desirable that every node participating in the network faithfully forwards the packets which it receives but are meant for some other node as destination. If such cooperation is received from every node in the network it would be an ideal situation. But like all other aspects of real life here also the conditions are not ideal and there exists non cooperative nodes in the network. These nodes may have two reasons for their non cooperation: malicious attitude or selfish attitude.

The malicious attitude of a node can be due to the opponent's intervention in the network where it intends to sabotage the network activity. The selfish attitude may be due to the various reasons where a legitimate node in the network starts avoiding the forwarding activity due to its

current low power status or it feels so over utilized in the forwarding activity and it fears that it will drain so much power that it will not have enough energy to send or receive its own packets in the future. The communication in the ad hoc networks suffers a lot because of the selfish attitude of the participating nodes and a lot of research work has been carried out to mitigate this type of attitude of the nodes and how to maintain the connectivity with such behaviour persisting [6][7].

The selfish behaviour of the participating nodes leads to the increased retransmission and thereby the overall decrease in the throughput of the network. As the number of selfish nodes increase, the efficiency of the network keeps on decreasing which ultimately leads to the near or total shut down of the network. In this paper, the literature on ad hoc networks contains a lot of papers [8]-[14] which provide strategies or mechanisms to deal with or cope up with such nodes. The subsequent part of this section explains some of these strategies and their relative merits and demerits.

The strategies used to tackle the selfish nodes can be categorized into two basic categories: Motivation / incentive based approach and detect and exclude approach. The motivation/ incentive approach tries to motivate the users of the ad hoc network to actively participate in the forwarding activities. Such a system involves certain amount of money transfer to the relay nodes, on behalf of source or destination, to motivate them to forward messages [8]-[10]. One of the motivation/ incentive based approach [11] is based on a virtual currency called nuglet. Every network node has an initial stock of nuglets. Either the source or the destination of each traffic connection use nuglets to pay the relay nodes for forwarding the traffic. The cost of a packet may depend on several parameters such as required total transmission power and the battery status of the intermediate nodes. Packets sent by or destined to nodes which do not have a sufficient amount of nuglets are discarded. The major drawback of this approach is the demand for trusted hardware to secure and maintain the record of the currency at central level. One such protocol, the ad hoc VCG [12] is based on the monetary transfer and discovers an energy-efficient path between the source and the destination. However, the number of messages that must be exchanged in order to find the route to the destination is quite high in the order of O(n3), where n is the number of network nodes.

Vikram Srinivasan [15] have proposed a random strategy to tackle the nodes which are not having enough battery. They introduced the concept of sympathy factor for each path on the basis of energy left in the intermediate nodes. If the sympathy factor is low for a certain path that means the relaying nodes do not have enough energy to participate in the route discovery phase. The path having maximum sympathy factor is selected and the data packets are routed from that path.

Detect and exclude approach avoids the selfish nodes from the routing paths. In this scheme two types of trust are developed first and second hand trust. First hand trust: The nodes personal observation about the neighbouring node. Second hand trust: The observation of neighbouring node for the other neighbours. The Watchdog and Pathrater is a mechanism [6] based on detect and exclude principle to deal with the selfish nodes. It has been designed to optimize the forwarding mechanism in the Dynamic Source Routing protocol [2]. It has two components: Watchdog and Pathrater. The Watchdog is responsible for detecting selfish nodes that do not forward packets. For this purpose each node in the network buffers every transmitted packet for some time. During this interval, the node places its wireless interface into the promiscuous mode in order to overhear whether the next node has forwarded the packet or not. The Pathrater assigns different rating to the nodes based upon the feedback that it receives from the Watchdog. These ratings are then used to select routes consisting of nodes with the highest forwarding rate. The protocols CONFIDANT [16] adds trust manager and reputation index to the above mechanism. It maintains two lists to deal with the selfish nodes. The node which behaves rationally are kept in the friends list and the nodes which drops the packets or tampers it is kept in the black list by the other nodes. The list is exchanged by each node with its neighbouring nodes. Based on these list trust of a particular node is calculated. Whenever the trust value for a particular node falls below a certain threshold the protocol stops forwarding packets of that node. In [13][14] Y. Zhang has described a distributed intrusion detection system (IDS) for MANETs that consists of the local components data collection, detection and response and of the global components cooperative detection and global response. Their architecture is very promising in dealing with the selfish nodes but they neglect the aspect how their local data collection should find out on incidents like dropped packets, concealed links, etc. Another system is the Collaborative Reputation Mechanism or CORE [17]. It is similar to the distributed IDS by Zhang et al. and consists of local observations that are combined and distributed to calculate a reputation value for each node. Based on this reputation, nodes are allowed to participate in the network or are excluded. In their work, the authors specify in detail how the different nodes should cooperate to combine the local reputation values to a global reputation and how they should react to negative reputations of nodes. For the actual detection of selfish nodes, they only refer to the work of Marti [18]. The protocols SORI [19] is also based on detect and exclude mechanism. It makes two record, the local evaluation record (First hand trust) and the overall evaluation record based on the reputation index given by the nodes about their neighbours are very much similar to above mechanism. Each node in the network maintains tables of first and second hand trust of their neighbouring nodes. Based on these tables the trust of a node is calculated and then action is taken against the selfish nodes.

III. E-AODV (ENHANCED AODV ROUTING PROTOCOL)

E-AODV is an enhanced AODV routing protocol. It is an energy aware AODV routing protocol which incorporates the power status concept in the hello request and reply messages to know the current power status of the neighbouring nodes and excludes those with low power status.

In this routing protocol, Energy/Power Status of each

node can be known whether it is participating in the communication process or not.

It Keeps track of energy calculations of each node with respect to simulation time. Once energy level of each node has been checked, nodes with low battery/power status avoid the forwarding activity causing the major disruption in the network and thus needs to be detected and isolated.

Isolation of such nodes from the network will avoid in the degradation of the network and help in the performance of the network as is shown in the results.

Table 1: Differences between AODV and E-AODV Routing Protocol

S.No.	AODV Routing Protocol	E-AODV Routing Protocol
1	Simple standard AODV routing protocol.	Enhanced AODV routing protocol.
2	No Energy concept is there in the hello request and reply messages.	Energy concept has been incorporated in the hello request and reply messages.
3	No Energy calculation exists of any node participating in the network.	Energy/Power Status of each node can be known whether it is participating in the communication process or not.
4	No check has been made to track the energy of each node with respect to simulation time.	Keeps track of energy calculations of each node with respect to simulation time.
5	No question of isolating the selfish nodes as they are not detected.	Selfish nodes are being detected and isolated.

IV. PROPOSAL

The Communication in an ad hoc network is done using intermediate nodes. Main objective in an ad hoc network environment is to find a suitable route for better communication. It is necessary that every node must be aware of its immediate neighbours at every moment. To remain aware about its neighbour nodes, a node in the network keeps on broadcasting hello requests on the periodic basis and keeps on receiving the hello replies as well. Using these hello request and replies a node in the ad hoc network constructs and maintains a table of its neighbours known as neighbour table. Since the nodes in the ad hoc networks are mobile, the neighbour table keeps on changing with time. Our proposal begins with the format for hello request packet as shown in Fig. 1. The hello request packet has three fields. packet type, source address and power status.

Packet Type	Source Address	Power Status

Fig 1: Hello Request Packet

Packet type field denotes that it's a hello request packet, source address field is the identifier of the node in the network which generated the hello request and power status field indicates the current status of the power of the sender node.

Packet Type	Source Address	Destination Address	Power Status

Fig 2: Hello Reply Packet

The format of hello reply packet is shown in Fig. 2. It has four fields: packet type, source address, destination address and power status. The packet type field here is hello reply, source address field contains the identification of the node from which the reply packet originated, destination address field is the identification of the node to which the packet has to be sent and the power status field provides the current power status of the sender node. The proposed routing mechanism in this paper has modified the conventional hello request and reply mechanism to include a new feature called power status. This feature keeps a node aware about the power status of neighbouring nodes. Thus the neighbour table of a node, in the proposed routing protocol will have an additional entry in the form of power status of the neighbouring node.

V. SIMULATION ENVIRONMENT

Network simulator provides a scalable simulation environment for large wireless and wired communication networks. The nodes are distributed randomly in the simulation area of 1000*1000 sq. unit size. ns-2.34 simulator has been used to analyze the routing protocols AODV and E-AODV.

Table 2: Simulation Parameters

SNo.	Parameters	AODV	E-AODV
1	Simulation Area	1000*1000	1000*1000
2	Number of nodes	50	50
3	Mobility Model	Random waypoint	Random waypoint
4	Simulation Time	200 s	200 s
5	MAC Type	IEEE 802.11	IEEE 802.11
6	Traffic Type	CBR	CBR
7	Energy	NA	100 joules

VI. PERFORMANCE MEASURES

Following metrics [20] are used to analyse and compare the performance of AODV and E-AODV routing protocols. Metrics are as follows: - Average Throughput, Jitter and Packet Delivery Ratio.

A. *Average Throughput*

It is defined as the total amount of data per time unit that is delivered from one node to another via a communication link.

B. *Jitter*

It is defined as the variation in time between arrivals of packets. It is deviation from ideal delay or latency.

C. *Packet Delivery Ratio*

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.

VII. SIMULATION RESULTS

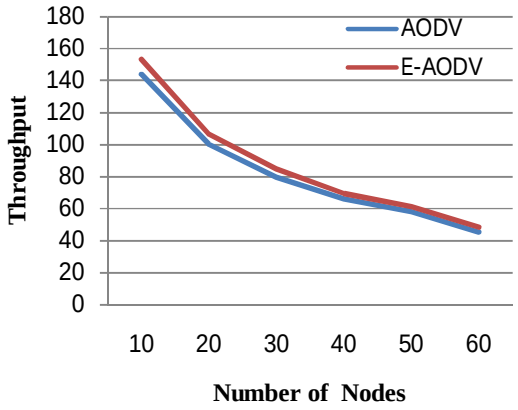

Fig 3: Throughput vs Nodes

Figure 3 shows the graph between throughput and nodes. X-Axis denotes the number of nodes from 10 to 60 and Y-Axis denotes the throughput and values ranges from 35 to 145. Blue line indicates E-AODV and Red line indicates AODV protocol.

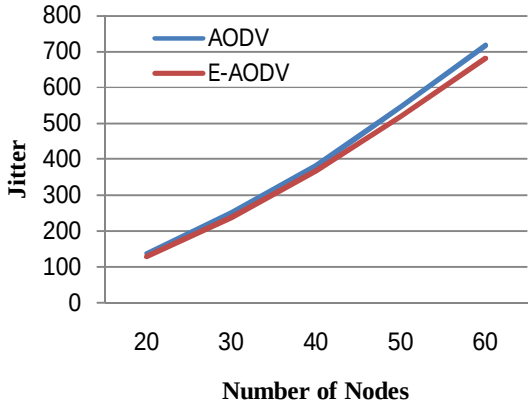

Fig 4: Jitter vs Nodes

Figure 4 shows the graph between Jitter versus number of nodes. In this Xgraph X-axis represents nodes from 20 to 60 and Y-axis represents the jitter values from 150 to 700. Blue line indicates E-AODV and Red line indicates AODV protocol.

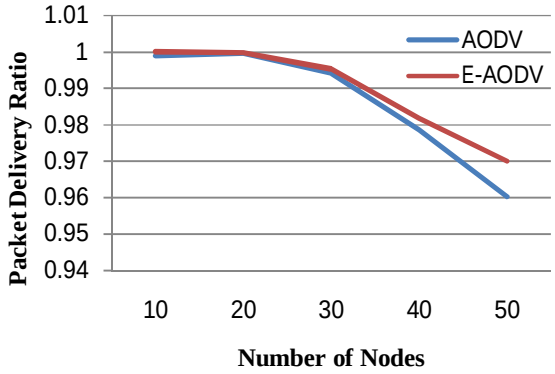

Fig 5: Packet Delivery Ratio vs Nodes

Figure 5 shows the graph between Packet Delivery ratio versus number of nodes. In This Xgraph X-axis represents the number of nodes from 10 to 100 and y-axis represents the value of packet delivery ratio ranging from .993 to .997

VIII. CONCLUSION

In this thesis work, a further enhancement has been done to the existing standard routing protocol AODV. The energy concept has been incorporated in the hello, request and reply messages of existing AODV routing protocol to know the current power status of the neighbouring nodes and excludes those with low power status. A comparison has been made between AODV and E-AODV routing protocol using three parameters i.e. average throughput, jitter and packet delivery ratio.

A. *Average Throughput*

As the number of nodes increases, throughput decreases.
In AODV: - Due to the non cooperative nature of the selfish nodes, they will not forward the packets to other nodes and keep dropping the packets which will increase the retransmission of the packets and thus less amount of data per unit time is delivered from one node to another node.
In E-AODV: - Due to the isolation of selfish nodes from the network, more data per unit time can be delivered from one node to another node.
So, throughput is more in E-AODV than in AODV.

B. *Jitter*

As the number of nodes increases, jitter increases.
In AODV: - Since the selfish nodes are not being detected isolated, so their presence in the network will lead to increased retransmission and thus packets will be delivered to destination in much more time.
In E-AODV:- Since selfish nodes are being detected isolated, packets will be delivered easily to other nodes and less time will be taken to route the packets to the destination.
So, Jitter is less in E-AODV than in AODV.

C. Packet Delivery Ratio

As the number of nodes increases, packet delivery ratio decreases.
In AODV: - Since the selfish nodes do not forward the packets to other nodes, so the packets received will be much less than the packets delivered/sent.
In E-AODV: - Since selfish nodes are isolated from the network, packets sent will easily be received by other nodes to reach to the destination.
So, packet delivery ratio is more in E-AODV than in AODV.

IX. Future Scope

From conclusions, it is concluded that E-AODV is better than AODV. But we can still make improvisations to this work. Some sort of incentive mechanism may also be incorporated in the network to enforce cooperation among all the nodes in MANET to improve the overall network performance. It will help to resist selfishness and misbehaviour in the network by motivating the nodes to enhance cooperation and thus improve the network performance. We can implement this work by considering network partitioning concept. It is essential to strive for perfection in the field of research. However, some of the objectives were beyond the scope of current research.

REFERENCES

[1] C.E. Perkins and E.M. Royer. Ad hoc on demand Distance Vector routing, mobile computing systems and applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, 1999, p90 - p100.
[2] D. Johnson, D. A. Maltz, Dynamic source routing in ad hoc wireless networks, in Mobile Computing (T. Imielinski and H. Korth, eds.), Kluwer Acad. Publ., 1996.
[3] V. Park, and S. Corson, Temporally-Ordered Routing Algorithm (TO- RA) Version 1 Functional Specification. IETF Internet draft, 1997.
[4] K. Mandalas, D. Flitzanis, G. F. Marias, P. Georgiadis "A Survey of Several Cooperation Enforcement Schemes for MANETs" International Symposium on Signal Processing and Information Technology IEEE, 2005.
[5] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J.P. Hubaux, J. Y. Le Boudec, "Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes" IEEE Communications Magazine, Vol. 39, No. 6, June 2001.
[6] A. A. Pirzada, C. McDonald and A. Datta, " Performance Comparison of Trust Based Reactive Routing Protocols" IEEE transaction on mobile computing, Vol. 5, No. 6, June 2006, pp 695-710
[7] Shin Yokoyama†, Yoshikazu Nakane Osamu Takahashi, Eiichi Miyamoto, "Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods", Proceedings of the 7th International Conference on Mobile Data Management (MDM'06).
[8] L. Buttyan and J. Hubaux, "Stimulating Cooperation in Self Organizing Mobile Ad Hoc Networks", ACM/Kluwer Mobile Networks and Applications, Vol.8, No.5, October 2003.
[9] L. Buttyan and J. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs", in Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, August 2000.
[10] N. Ben Salem, L. Buttyan, J.P. Hubaux, M. Jakobsson, "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks", in Proc. ACM MobiHoc 03, pp. 13–24, 2003.
[11] L. Buttyan and J. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized ad hoc networks", in Technical Report EPFL, DSC, 2001.
[12] L. Anderegg, S. Eidenbenz, "Ad hoc-VCG: A Truthful and Cost Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents", Proc. ACM Mobicom, pp. 245–259, 2003.
[13] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless Adhoc networks. In Mobile Computing and Networking, pages 275–283, 2000.
[14] Yongguang Zhang, Wenke Lee, and Yi-An Huang. Intrusion Detection Techniques for Mobile Wireless Networks. to appear in ACM Wireless Networks (WINET), 9, 2003.
[15] Vikram Srinivasan, Pavan Nuggehalli, Carla F. Chiasserini, Ramesh R. Rao, "Energy Efficiency of Ad Hoc Wireless Networks with Selfish Users".
[16] Buchegger S, Le Boudec JY. Performance analysis of the CONFIDANT protocol. In Proceedings of 3rd ACM International Symposium, on Mobile Ad Hoc Networking and Computing, June 2002.
[17] Michiardi P, Molva R. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of 6th IFIP Communication and Multimedia Security Conference, September 2002.
[18] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. Sixth Ann. Int'l Conf. Mobile Computing and Networking (MobiCom), pp. 255-265, 2000.
[19] He Q, Wu D, Khosla P. SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks. In Proceedings of IEEE WCNC2004, March 2004.
[20] S. Corson, and J. Macker, Mobile Ad hoc Networking: "Routing Protocol Performance Issues and Evaluation Consideration" rfc 2501, jan 2003.

Yogesh Bansal, Assistant Professor in Computer Science/Information Tech. Baddi University of Emerging Sciences and Technology, Baddi. Working in this university since last 3 years. Masters in Computer Science was completed in 2011from UIET, Panjab University (Chandigarh). My research interests are networking, simulation, software testing. Presented a paper in national conference on **"Detecting and Isolating Selfish nodes in MANETS",** in National conference on innovative Projects (ncip), held at Baddi University of Emerging Sciences and Technology, Baddi, 2011.