Devised Opportunistic Routing With Congestion Control Policy In Wireless Adhoc Networks

Roopalakshmi S [1], Noor Basha [2], Anil Kumar[3]

[1]Asst. Professor, Computer Science & Engineering, Vemana Institute of Technology, Bengaluru-34, India.

[2]Asst. Professor, Computer Science & Engineering, Vemana Institute of Technology, Bengaluru-34, India.

[3]Asst. Professor, Computer Science & Engineering, Vemana Institute of Technology, Bengaluru-34, India.

Abstract: *The rapid advances in wireless Ad-hoc environment enables a profound of users. The data transmission via multi-hop networks creates huge traffic in opportunistic routing. To overcome from this issue, a devised opportunistic routing with congestion control policy is studied. We have proposed OR based DTMC scheme that deals with behavioral study of cooperative and non-cooperative nodes. The task of opportunistic routing is to deliver the packets in reliable and secured manner. The objective is to design routing protocols that supports non-cooperative nodes of wireless environment. We estimate packet drop ratio to observe the action of nodes and detect the congestion establishing nodes. The set of each node is selected and various parameters are considered to improve the possibility of delivering packets to their final endpoint. An experimental outcome shows the efficacy of the proposed system.*

Keywords: Wireless Adhoc networks, Multi-hop networks, Opportunistic routing, Non-Cooperative nodes and Packet drop ratio

I. INTRODUCTION

Opportunistic routing for multi-hop wireless ad-hoc networks has been a current research attention to overcome demerits of predictable routing [1]–[5]. Opportunistic routing moderates the effect of weak wireless links by showing the features of wireless transmissions and the route diversity. It works on principles based routing systems. Each packet transmission can be listened by a random subgroup of receiver nodes among which the subsequent dispatch can be selected opportunistically. More accurately, the routing judgments are made on the go by choosing the subsequent dispatch based on the actual transmission outcomes as well as a rank ordering of nearby nodes. The main challenges in the design of an opportunistic routing strategy includes the condition based on which the subsequent dispatch is selected and the increased overhead associated with opportunistic selection of the relay. Let us first consider the dispatch selection problem. To ensure a small average latency, the dispatch selection condition need to balance the commutation between many routing packets along the shortest paths and distributing traffic throughout the network. When multiple casecade of packets are to traverse the network, however, it might be necessary to route some packets along longer paths, if these paths eventually lead to links that are less congested. As noted in [6], [7], the opportunistic routing schemes cause severe congestion and unbounded delay.

In contrast, backpressure [8] which is a simple routing policy, ensures bounded expected delay for all stabilizable arrival rates. In the opportunistic context, Diversity Backpressure Routing (DIVBAR) [6] provides a generalization of backpressure which incorporates opportunism and diversity in the wireless context. Backpressure-based routing policies in [8] and [6] chooses metric different from [1]–[3]; rather than any parameter of closeness (or cost) to the destination, receiver which is selected has the largest positive variance backlog to ensure throughput optimality. In other words, routing decisions are made on the dynamic queue backlogs which form a time-varying relay selection criterion. However, the less latency performance is due to overlooking the cost to the destination which will become the misery (see [6], [7]). In higher version of DIVBAR (E-DIVBAR), a summation of queue backlogs and expected number of transmissions is used as the selection criterion. This routing policy, unfortunately, can lead to worst delay performance as shown in [7]. Instead, in our earlier work, we combined the congestion information with the shortest path calculations proposed in [4] to provide an Opportunistic Routing with Congestion Diversity (ORCD).

The paper is organized as follows: Section II describes the related work; Section III describes the proposed work; Section IV describes experimental results and concludes in Section V.

II. RELATED WORK

The author in [5] proposed ExOR, which differs from traditional routing that it does not use predetermined path for sending packets. Instead it uses broadcast nature of Wireless networks to forward packets through the network. It broadcasts all the packets to the nodes in the network. ExOR uses a potential forwarders list to reach the destination. Upon reception each nodes will check the list available in the header and forwards it. Likewise 90% of the packets will be delivered to the destination; the remaining 10% of the packets will be delivered using traditional unicast routing. Trial outcomes shows that ExOR throughput performance is improved 2x times than the traditional routing.

The author in [6] MCExOR which is a Multi-channel protocol and extends ExOR by utilizing several RF channels in multi hop wireless networks. Large amount of transmissions each end-to-end delivery combined with meddling are the main reasons for the low capacity of multi-hop networks. It reduces the number of transmissions by opportunistically avoiding nodes in a packet's forwarding path. MCExOR needs one RF transceiver per device and selection of RF channels is independent of the routing function. The simulation results show that it outperforms AODV.

The author in [7] stated a proactive Link state routing protocol. It produces better results than ExOR by utilizing the components: adaptive forwarding path to avoid duplicate transmissions, priority based timers, Local loss recovery scheme and adaptive rate control. SOAR effectively supports multiple simultaneous flows by improving both throughput and fairness.

The author in [8] which is designed to achieve the following as goals to reduce routing update overhead, resilience against link's loss/failure and improving throughput. The above goals are achieved by reducing routing updates through building runtime mesh on the fly, improving throughput by exploiting instantaneous channel variations and Randomized forwarding by exploiting different data rate and loss rate.

The author in [9] which uses network coding approach to opportunistic routing. The OR protocols exploits the broadcast nature of the wireless medium to increase throughput. The important of MORE is that through intermediate nodes forward packets they hear without consulting with each other; they do not generate spurious Transmissions. (i.e.) intermediate nodes forward random linear combinations of packets going to the same destination. This approach does not need any co-ordination among nodes and maximizes network throughput.

The author in [10], an Opportunistic Routing (OR) protocol that is free from identical communication. OR utilizes overheard packets and takes many routes into consideration simultaneously. Economy utilizes token passing along a route that relays can listen one another to eliminate identical communication. When a token reaches, the dispatch is allowed to transmit unacknowledged packets according to the acknowledgement information of the token received. Economy prevents duplicate transmission while keeping the advantages of OR. Simulation outcomes show that while previous OR schemes suffer from duplicate transmission, economy can exploit the potential of OR and perform up to 100% better than traditional routing.

The author in [NC based OR protocol. The NC based OR protocol [11] approach has minimal coordination overhead but they suffer performance deprivation in dynamic wireless environments with continuously changing levels of channel gains, interference and background traffic. The scheme allows nodes to report network coded traffic to their upstream nodes in a modest way, with reduced loss rates and with almost zero surcharges. The compared to MORE this protocol improved throughput and fairness by up to 3.2x and 83% respectively for different number of concurrent flows based on results.

III. PROPOSED WORK –DEVISED OPPORTUNISTIC ROUTING MODEL

This section depicts the functioning of devised opportunistic routing process. The purpose of the work being carried is to detect the black hole attacks via devised opportunistic routing protocols. The behavior of the node is monitored for detecting the malicious node. Every node in the network sends and receives the data packets. Black hole attack is an attack that continuously drops the data packets. Devised opportunistic routing protocols with EXOR algorithm is proposed in this paper. A hop by hop routing process is instantiated with OR protocols in better coordinated nodes. Initially, the link quality between transmitters and receivers using OR protocols are checked. A perfect coordination mechanism is needed among the nodes. Routing operations in OR protocols can modeled by DTMC.

Candidate nodes are mutually communicated under its network systems. In this method packet is sent continuously i.e. several retransmission need to be done till it is delivered to destination. Using DTMC, the routing operations gets modeled in OR methods. In general, DTMC system is independent i.e. dispose its past states. It exhibits only if current hops transfer the next hop without using its previous hop. And also different state values arrive for different DTMC states. Along with OR protocols, DTMC supports two states, namely, success state and fail state. DTMC is derived in tuple form that contains node identifier and no.of retransmissions states.

The theme of the proposed work is to detect the black hole attacks. In this OR based mesh network is deployed over the wireless environment. Several nodes in the wireless system may not participate for communication. These nodes may be malicious node or normal nodes. The non-cooperative nodes are identified using OR based DTMC schemes. Let us consider the following symbols and is presented in table 1.

Symbols	Details
N	No. of nodes in network
M	No. of malicious nodes
K	No. of retransmissions states
C	No. of candidate sets
CS_i	Candidate set for node i at intended destination
ID	Node identifier
$Link_{prob}$ (x,y)	Link delivery probability between node x and y

Table 1. Symbols and its details

The proposed steps are as follows:

i) A linear topology is defined and shown in Fig.1

ii) Let us assume that distance between source and destination nodes is equal.

iii) Each node is specified with ID, to identify the black hole attacks. Black hole attack is an attack that continuously drops the received packets.

iv) Each node continuously sends/ receives the data packets until it moves to absorbing states.

v) Consider node 3 as malicious node. The node 3 process until it reaches the state (3,0). By eqn.1, the no. of states is estimated as:

$$S= (N-M-1) *(K+1) +M+2 \quad (1)$$

vi) After the DTMC is computed, the transition probability matrix is established for predicting the no. of retransmissions and its probability values.

vii) Packet Drop ratio calculation is done for more accurately predicting the black hole attack.

viii) Packet drop ratio is defined as the no. of packets received by non-cooperative nodes and maliciously dropped. It is given as:

$$Drop\ ratio = \sum_{i=1}^{M} Drop\ BH_i$$

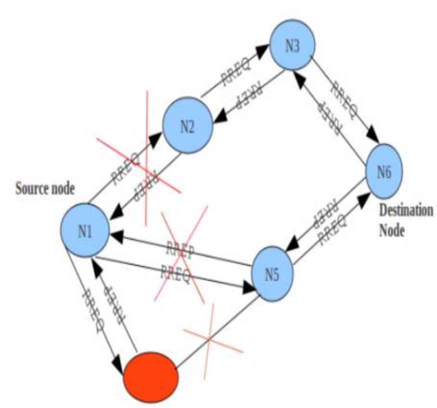

Fig. 1. Proposed architecture

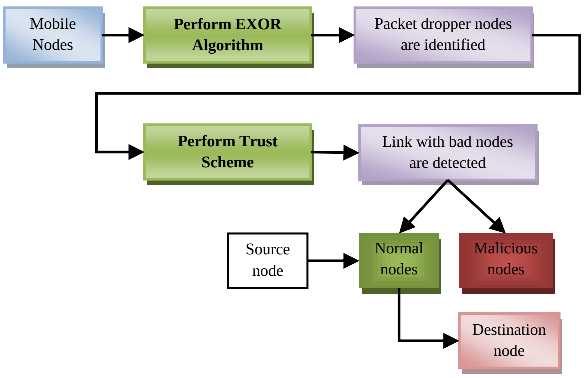

Fig.2. Block diagram of proposed algorithm

IV. EXPERIMENTAL ANALYSIS

This section depicts the experimental validation of our proposed algorithm.

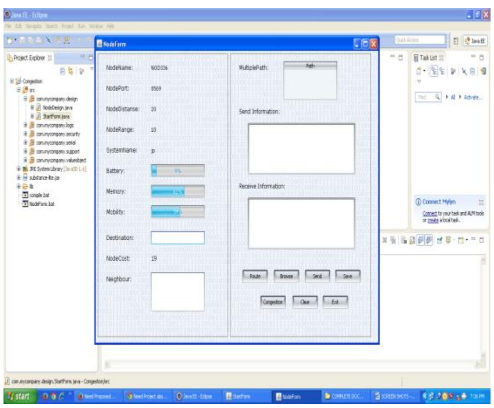

Fig.3. Nodes creation by getting the details like port, distance, range, battery level, memory, mobility, cost and its neighbor nodes

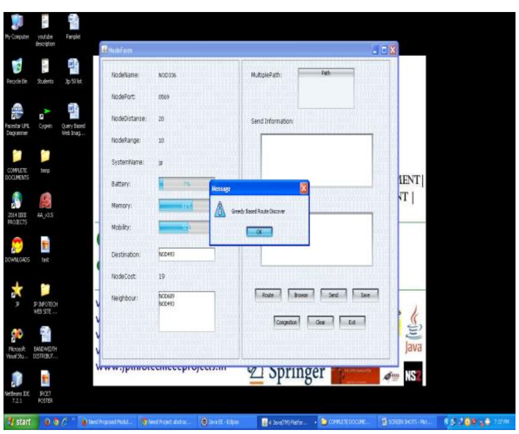

Fig.4. Greedy based discovery route that concludes the source node and destination node.

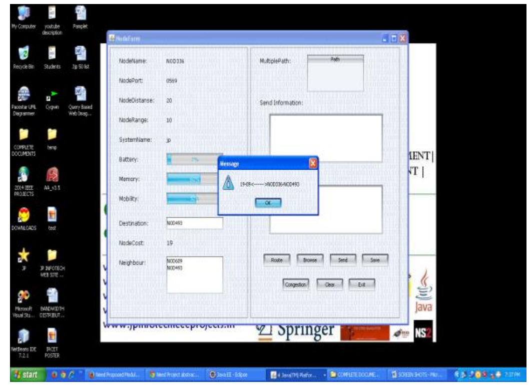

Fig.5. Estimating the neighboring nodes and its intermediate path.

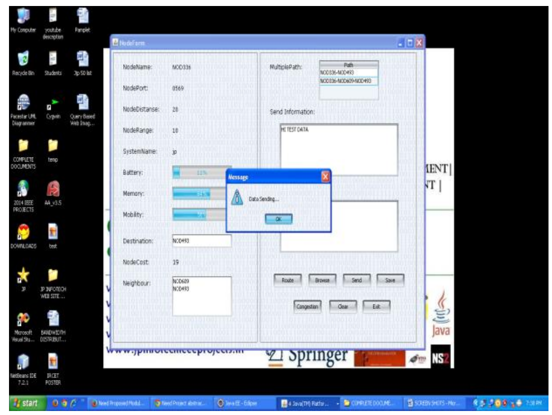

Fig.6. Generation of the multiple path and then sending the data packets.

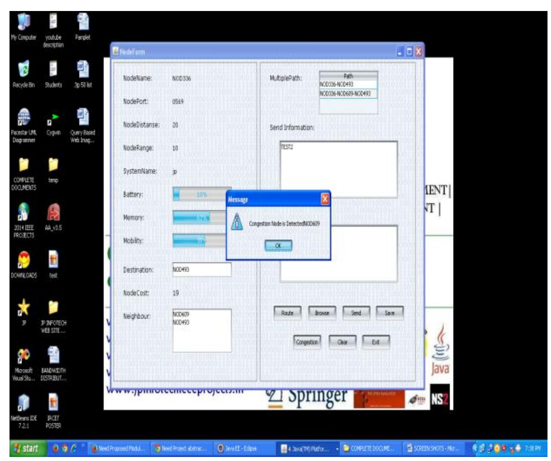

Fig.7. Detection of congestion node

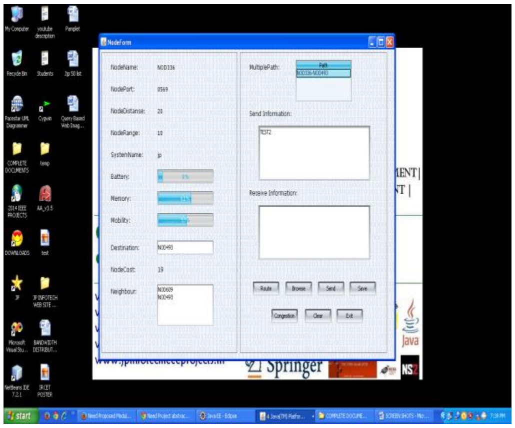

Fig.8. Broadcasting the congestion node to its other nodes in opportunistic routing systems.

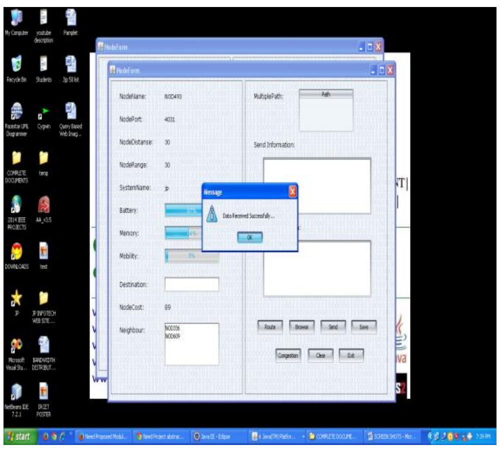

Fig.9. Then forwarding the data packets to all its nodes.

V. CONCLUSION

This paper concentrates on adversial effects of the non-cooperative nodes in opportunistic routing system. The objective of the paper is to design a routing model that capable of sending the message in delayed performance over prior opportunistic routing. By considering all candidate nodes are mutually communicated with each other towards the networks, the behavior of the nodes are studied. A novel Discrete Time Markov Chain (DTMC) model is designed with OR protocols that effectively studies the behavior of the candidate nodes. We also calculated the packet drop ratio which estimates the no.of malicious nodes. An experimental result shows the effectiveness of the systems.

REFERENCES

[1] C. Lott and D. Teneketzis, "Stochastic routing in ad hoc wireless networks," in Proc. 39th IEEE Conf. Decision Control, 2000, vol. 3, pp. 2302–2307, vol. 3.

[2] P. Larsson, "Selection diversity forwarding in a multihop packet radio network with fading channel and capture," Mobile Comput. Commun. Rev., vol. 2, no. 4, pp. 47–54, Oct. 2001.

[3] M. Zorzi and R. R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks:Multihop performance," IEEE Trans. Mobile Comput., vol. 2, no. 4, pp. 337–348, Oct.–Dec. 2003.

[4] M. Zorzi and R. R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Transactions on Mobile Computing, vol. 2, no. 4, 2003.

[5] S. Biswas and R. Morris, "ExOR: Opportunistic Multi hop Routing for Wireless Networks," ACM SIGCOMM Computer Communication Review, vol. 35, pp. 3344, October 2005.

[6] C. Lott and D. Teneketzis, "Stochastic routing in ad hoc networks," IEEE Trans. Autom. Control, vol. 51, no. 1, pp. 52–72, Jan. 2006.

[7] E. M. Royer and C. K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Pers. Commun., vol. 6, no. 2, pp. 46–55, Apr. 1999.

[8] T. Javidi and D. Teneketzis, "Sensitivity analysis for optimal routing in wireless ad hoc networks in presence of error in channel quality estimation," IEEE Trans. Autom. Control, vol. 49, no. 8, pp. 1303–1316, Aug. 2004.

[9] J. N. Tsitsiklis, "Asynchronous stochastic approximation and Q-learning," in Proc. 32nd IEEE Conf. Decision Control, Dec. 1993, vol. 1, pp. 395–400.

[10] J. Boyan and M. Littman, "Packet routing in dynamically changing networks: A reinforcement learning approach," in Proc. NIPS, 1994, pp. 671–678.

[11] J. W. Bates, "Packet routing and reinforcement learning: Estimating shortest paths in dynamic graphs," 1995, unpublished.