International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 12, December-2014

A Survey On Admission Control and Trust Based Opportunistics Routing in Wireless ad hoc Networks

Pallavi S. Shinde
ME Second Year,
PVPIT, Pune

Mr. N. D. Kale
Department of Computer Engineering,
PVPIT, Pune

***Abstract*—Providing QoS in wireless ad hoc networks is a difficult task. The multi-hop nature of the network affects QoS in wireless ad hoc networks. In traditional routing scheme, if one node at the optimal path is down due to lack of available energy, the whole path will be broken, and the source must re-route again. Opportunistic Routing is introduced to solve this issue which improves performance of the system. It isquite difficult to provide better QoS in Opportunistic Routing due to the uncertainty of forwarding paths. Most of the existing Opportunistic Routing ie OR protocols rarely consider providing service for different types of flows. Existing Opportunistic Routing scheme uses Admission Control (ORAC) of nodes for the different types of flows. The ORAC scheme manage a new flow admission control scheme which is based on bandwidth, backlog traffic and residual energy of nodes to select forwarding candidates. Network security is also a current research topic in WSN. The existing work in OR considered either of QoS and security. In the proposed system we have taken security issue in to account while adopting the ORAC scheme. To solve issues of security we have used the trust value of the nodes in the network.**

Keywords—Wireless ad hoc networks routing, bandwidth, traffic, energy.

I. INTRODUCTION

In multi-hop wireless ad hoc networks, packets can be forwarded using intermediate nodes from the source to the destination without centralized coordination. And many traditional routing protocols fail to use the broadcast nature of wireless networks and spatial diversity by choosing a fixed path as similar to wired links. When the current path is broken, the source will re-route again, and then end to end QoS is difficult to guarantee. Opportunistic Routing gives way to utilize the broadcast nature of wireless links to achieve cooperative communication at the link layer and networks layer of static multi-hop wireless networks. Thus the network throughput can beimproved and the transmission delay can be reduced by using the OR scheme. Because OR has many characteristics, multiple representative works on OR have been proposed.

II. RELATED WORK

The network throughput can be improved and the transmission delay can be reduced by using the OR mechanism. Biswas and Morris [3] "first explained the ExOR, which integrates routing and MAC protocol to increase the throughput in multi-hop wireless networks. Extremely OR's forwarding paths can easily spread from its central point, and the metric which is for selecting candidate nodes only employs Expected Transmission."

Then, MAC-Independent Opportunistic Routing and Encoding i.e. MORE, MORE[4] is an intra-session network coding scheme, CCACK adopts a cumulative coded acknowledgment scheme that allows nodes to acknowledge network coded traffic to their upstream nodes. Simple Opportunistic Adaptive Routing (SOAR) [5] adaptively selects forwarding nodes and uses priority-based timers to service for multiple simultaneous flows in wireless mesh networks.

Network security is also a hot research topic on routing. WangBoet. al. [2] "TOR gives a new solution to solve security issue by defining a new metric called E2TX(trustworthiness and ETX). Using this metric, TOR also considers the two key issues for a new routing protocol called TOR: candidate selection and prioritization of relays in classical opportunistic routing."

In [7], Ergin et al. presented an admission control and routing mechanism for multi-rate wireless mesh networks and their admission control scheme is dependent on available bandwidth estimation. Moreover, Gao et al. [8] discussed the multi-rate any path routing scheme, which gives details about a bandwidth reservation for traffics. In addition, Zhao et al. [9] mentioned Bandwidth-aware OR with considering Admission Control named BOR/AC in mesh networks.

In [1] Yang Qin et. al. "propose a novel OR scheme joint with admission control for different priority flows in wireless ad hoc networks, named as ORAC (Opportunistic Routing with Admission Control). By considering the node's available bandwidth, residual energy and backlog in buffer before selecting the candidates, ORAC is able to improve the network performance for different traffics."

III. PROPOSED MODEL

As shown in fig 1, proposed TORAC considers two major issues in wireless ad hoc network. Proposed model provides security by using trustworthiness of a node in the network. Initially trust value is assigned or calculated and then trust value is updated in each cycle. In proposed model, concept of admission control is put with help of three main parameters like bandwidth, backlog traffic, and Energy of the node.

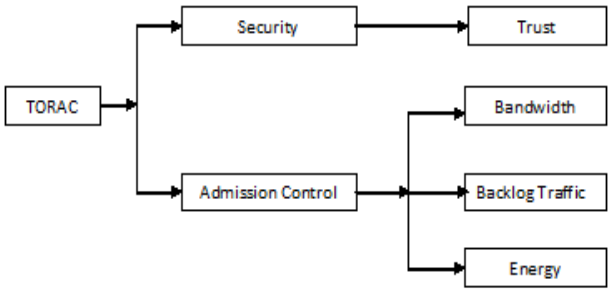

Fig. 1 Proposed TORAC model

IV. METHODOLOGY

A. Trust calculations and updating

As a metric of the wireless link, trust value is used to indicate the trustworthiness of the transmission behaviors over the link.

Trust value of a node is calculated by using following equation,

$$T_j(k,n)=R_{kj}(n)/F_{kj}(n) \quad (1)$$

$T_j(k,n)$ =Trust value of node j assigned/calculated by node k during n^{th}topology cycle. Where$R_{kj}(n)$ and $F_{kj}(n)$are the number of packet that have been received by k and forwarded from j at time t respectively, and$0 \leq T(k,t) \leq 1$.

Trust value of a node is updated after every topology change using following mathematical equation.

$$T_j(k,n) = \alpha . T_j(k,n-1)+(1-\alpha).T_j(k,n) \quad (2)$$

Where, $T_j(k,n)$ is node$j^{'s}$trust value measured duringn^{th}topology updating cycle. $0<\alpha<1$ is a weighting factor used to trade-off between current measurement and previous estimation.

Definition 5. The combined routing metric value of node j holds true, only if node j satisfies a precondition: $T_j \geq T_{Threshold}$.

Where $T_{Threshold}$ is the trust threshold value of the whole network, definition5 means if the node j is not a trustworthy node, namely, it may be a selfish and malicious node, so, we disregard the node and don't allow its joining in the network.

B. Flow admission control model in ORAC

Flow Admission Control with Opportunistic Routing is introduced [1], to provide a proper method to select forwarding candidates for a new incoming flow by using flow admission control during the routing discovery.

1. Current available bandwidth is compared with requested flow rate arrived to decide whether the new flow can be admitted by the node.
2. If there is large number of backlogs in node's buffer, new flow will be rejected by the node.
3. The nodes must consume energy for receiving, forwarding packets, thus, the residual energy of nodes in multi-hop networks is also an important factor that affects admitting of a new flow.

If the above three criteria available bandwidth, enough buffer space and residual energy are satisfied for a node, the node will participate in the route discovery phase and will become node of the forwarding candidates set

In this, we consider a wireless ad hoc network, whose topology is static, denoted by G(V,E) a directed graph, where V is the set of nodes and E is the set of virtual links in wireless ad hoc networks. Assume there are n nodes in the network and V={n1; n2; n3; . . . ; ni; n_i+1;ni+2; . . . ; n_n}

C. Available Bandwidth

Assume that a typical node in a wireless ad-hoc network has a limited bandwidth C to service incoming traffic flows. We denote an incoming packet of a particular flow with data rate q^k_j, where j is the priority class of the flow and k is the number of the flow. There are m classes of flows in the network, the set of total classes denotes {1, 2, . . . ,j, . . ., m}. Assume class j has p_j flows existing in an intermediate node n_i, the flows set of class j can be expressed as {1, 2, ..., k, ..., p_j } at node n_i. When a new flow wants to access an intermediate forwarding node n_i during the opportunistic route discovery phase, it should satisfy the following condition.

$$q^{new}_{j+1} + \sum_{j-1}^{m} \sum_{k-1}^{pj} q^k_j \leq C \quad (3)$$

Where, q_j^{new}denotes the data rate of the new flow belonging to class j + 1.

$\sum_{j=1}^{m} \sum_{k-1}^{pj} q^k_j$ denotes the total data rate of flows that have been admitted by node n_i from different priorities of classes. Considers the bandwidth allocation for the flows based on the average rate.

D. Backlog traffic

In OR, we define a node as a congested node when it's in flows are more than it can cope. Thus, a node may be congested when it has a low bandwidth (due to sharing of bandwidth with multiple neighbors or poor network condition, etc.) and its queue length is long (i.e., packets are not able to be transmitted fast enough). For providing better QoS, we also consider backlog traffics in the buffer. The second criterion aims to avoid congestion and to provide better delay guarantee for a flow. Assume that at any time, an intermediate node n_i contains $\sum_{j=1}^{m} \sum_{k=1}^{pj} w^k_j$ bits in total waiting within its buffer, w^k_j is the number of bits waiting in a queue belonging to a flow k of class j. For the intermediate node n_i, when it admits a new flow, it should satisfy the following inequality.

$$C - \sum_{j=1}^{m} \sum_{k=1}^{pj} \frac{W^k_j}{D_j - T^k_j} \geq 0 \quad (4)$$

where $D_j$is a soft delay bound parameter of class j in order to ensure more weight given to higher priority traffic, T^k_j is the consumed time that spends on transmitting the flow k of

class j from source to intermediate node n_i, which can be expressed.

$$T_j^k = \sum_{\omega=1}^{ni} T_j^k(\omega) \quad (5)$$

Where,

$T^k_{j(w)}$ is the successfully transmission time of data flow from node x to next hop x þ 1 for flow k of class j, which can be expressed.

$$T_j^k(\omega) = \sum_{l=1}^{L} T_j^k(l) \times p_j^k(l) \quad (6)$$

Where,

$l(1 \le l \le L)$ is the number of retry, and L is the retry limit defined in the IEEE 802.11 standard, pk_j^k (l) is successful probability of the l_{th} attempt for flow k of class j, $T^k_j(l)$ is time required for l_{th} attempt of data flow k of class j transmission in node w, which can be expressed.

$$T_j^k(l) = AS_j + T_{boffj}(l) + T_{j-data}^k + R_\omega * T_{ACK} + R_\omega * SS \quad (7)$$

where SIFS is the short inter-frame spaces, AS_j is the arbitration inter-frame space defined in the IEEE 802.11e EDCA standard, $T_{boffj}(l)$is the average back off time consumed in the l^{th}attempt for the flow of class j, R_w is the number of candidates of node w, T_j^k_Data is the time for transmit data frame of data flow k within class j, and T_{ACK} is the time for transmit ACK frame.

We assume that transmission attempts are independent from each other, and the successful probability for each class of traffic is different because of their different priority. Then, the successful probability of the l^{th} attempt for flow k of class j, denoted by $p^k_j(l)$, which can be calculated as

$$p_j^k(l) = (l - \delta_j^k)^{l-1} \times \delta_j^k \quad (8)$$

wherep^k_j is the success probability of each attempt for flows of class j.

Energy consumption Wireless ad hoc networks are a special kind of wireless networks, which allow a group of nodes to setup and maintain a temporary network by themselves, without the support of any fixed infrastructure. In wireless ad hoc networks, the battery energy of many nodes is limited. Hence, we must consider the energy of these devices, estimating energy consumption of them in packets transmission. We suppose that **packet size is the same** for different types of flows, and the sending power of nodes is constant, so, the energy consumption that spends on forwarding or receiving packet is also the same for different types of flows. The energy consumption of an intermediate node n_i for successful transmitting one packet to its downstream node, denoted by E_{iC} , which is composed by three parts: the energy E_{iF} is consumed to forward a packet, the energy E_{iR} is consumed to receive a packet, and the energy E_{iAck} is consumed to send an acknowledgment packet. In this energy module, the main energy consumption of nodes is used to transmit packets, and some other factors, such as energy attenuation of nodes; we do not consider them [1]. Thus, we have

$$E_{ic} = E_{iF} + E_{iR} + E_{iACK} \quad (9)$$

We suppose that E_{iT} denotes the total energy of a node n_i. Moreover, according to the mechanism of OR, node n_i should send an acknowledgment to its upstream node when it receives a packet. Hence, the residual energy E_{ir} that the node n_i forwards existing packets belonging to the buffer queue of class j can be expressed.

$$E_{ir} = E_{iT} + \sum_{j-1}^{m} \sum_{k-1}^{\rho j} \frac{w_j^k}{pktsize} (E_{iF} + E_{iR} + E_{iACK}) \quad (10)$$

Where

- pktsize denotes the number of bits occupied by a packet size.

  $\sum_{j-1}^{m} \sum_{k-1}^{\rho j} \frac{w_j^k}{pktsize}$denotes the number of packets in the buffer queue of class j for node n_i. The above formula expresses the consumed energy that node $_{ni}$ spends to receive and forward existing packets in the buffer.

Suppose that a new flow belonging to class j+1 contains r_{j+1}^{new} packets, hence, the node n_i can admit the new flow, it need to satisfy the following inequality.

$$E_{ir} - r_{j+1}^{new} \times (E_{(j+1)F} + E_{(j+1)R} + E_{(j+1)\_ACK}) \ge 0 \quad (11)$$

Where $r_{j+1}^{new} \times (E_{(j+1)F} + E_{(j+1)R} + E_{(j+1)\_ACK})$ denotes the consumed energy that node n_i spend to receive and forward a new flow of class j +1.

E. Flow admission control scheme

After introducing the available bandwidth, backlog traffic and energy consumption model, we give our admission control scheme from [1]. The key idea is that a node can admit a new flow if it has sufficient bandwidth, energy, and buffer space. And then, we can select it as forwarding nodes in the opportunistic route discovery phase [1]. Hence, any intermediate node n_i admits a new flow of class j+1 which containsr_{j+1}^{new} packets with data rate q_{j+1}^{new} when it satisfies the following inequality.

$$C - \sum_{j=1}^{m} \sum_{k=1}^{\rho j} q_j^k - \sum_{j=1}^{m} \sum_{k=1}^{pj} \frac{W_j^k}{D_j - T_j^k} - q_{j+1}^{new} \ge 0 \quad (12)$$

$$E_{ir} - r_{j+1}^{new} \times (E_{(j+1)F} + E_{(j+1)R} + E_{(j+1)\_ACK}) \ge 0$$

The advantage of this scheme is that it is able to strike a balance indirectly between admitting more flows and facing congestion, and provide better QoS for different requirements.

V. ALGORITHM

A. Forwarding scheme in TORAC:

In this section, we introduce our forwarding scheme of TORAC for different types of flows in detail. The TORAC scheme contains three components: forwarding candidates set selection, candidate's prioritization, and the opportunistic forwarding scheme. The former two parts determine the methods of selecting forwarding candidates and prioritization policies of forwarding candidates, and the latter gives a forwarding scheme which contains to determine when a node updates its candidates list and how to provide different QoS for different types of flows. Next, we introduce them respectively.

a. Forwarding Candidate Set Selection

How to select proper metrics for determining forwarding candidates set is very important. In TORAC protocol, we propose a new method for selecting the forwarding candidates set, which is based on flow admission control and trust value of the node in candidate set. The details are expressed as follows.

At the beginning of algorithms, the distance between any two nodes in the network should be calculated using location service module. This can be realized easily because the network topology is static. And for node n_i in the network, its one-hop neighbours can be determined when we set the transmission range of nodes. We select the nodes that the distance between them and destination node is shorter than the distance between n_i and destination node within the one-hop neighbors, then, collect these nodes in a set, denoted by temporary set, TSi.

(TSi = {n1; n2; . . . ; nr}). Moreover, we calculate the available bandwidth, backlog traffic, residual energy and trust value of the nodes which are in set TSi. First we check that which nodes are more trustworthy by its trust value in the current network topology cycle.

If $T(n) \geq T_{threshold}$ then add node from TSi to the Si.Then we check that which nodes in set Si have sufficient resources to admit a new flow according to formula .After that, we store the nodes that satisfy formula in set Q_i={n1, n2, ……, nφ}

$(Q_i \subseteq S_i \varphi \leq r) \& T(n) \geq T_{threshold.}$

where Q_i is the forwarding candidates set of node n_i.

b. Candidate Selection Using TORAC

1. When node joins the network firstly its trust value is assigned to the 0.5 / calculated, which means node is not a malicious node.
2. After completion of first cycle its trust value is calculated.
3. In every topology cycle trust value is updated.
4. Calculate the distance of each node from other nodes in the network using location service module.
5. After calculation of distance each node will calculate its temporary candidate set TS_ibased on trust value of nodes in the range.
6. Calculate the available and required bandwidth for incoming flow.
7. Calculate the current backlog traffic and incoming traffic for the node.
8. Calculate required energy and residual energy of the node.
9. Check for sufficient resources are available, if node has sufficient resources then add that node to the set S_i.
10. Node from S_i to set Q_i if node in S_i satisfy the

$T(n) \geq T_{threshold.}$

```
Route_Packet(P)
{
        Receive_Packet9P0;
        S <- Get_Src(P);
        D <- Get_Dest(P);
        If(ID==NodeID)
        {
                Precoss_Packet();
        }
        else
        {
                L=Get_NeighborList(NodeID);
                for(all nodes in list L)
                {
                        Calculate_Trust();
                        Check_Bandwidth();
                        Check_BacklogTraffic();
                        CheckAvail_Energy();
                }
                Candidate_Selection();
                Candidate_Prioritization();
                Send_Packet();
        }
}
```

c. Candidate Prioritization

After selecting the forwarding candidates set, we give a prioritization policy to determine the priorities for these candidates. In TORAC scheme, we use the priority metric $\delta_i$to decide the priorities of node n_i when it admits a new flow with class j, which can be defined as follows.

$$\delta_i = \alpha \times \frac{C - \sum_{j=1}^{m} \sum_{k=1}^{\rho j} q_j^k - \sum_{j=1}^{m} \sum_{k=1}^{pj} \frac{W_j^k}{D_j - T_j^k} - q_{j+1}^{new}}{C} + \beta \times \frac{E_{ir} - r_{j+1}^{new} \times (E_{(j+1)F} + E_{(j+1)R} + E_{(j+1)\_ACK})}{E_{iT}} + \gamma \times \frac{(p_{if} + p_{ir})}{2} + \varphi \times \frac{d_{SD} - d_{iD}}{d_{SD}} \quad (13)$$

where p_{if} is the forward delivery ratio of node ni, which indicates probability that a data packet successfully arrives at the recipient, p_{ir} is the reverse delivery ratio, which is the probability that the ACK packet is successfully received by node n_i, d_{SD} is the distance from source to the destination node, d_{iD} is the distance from current node n_i to the destination node, α,β,γ and φ are the weight factors, which can determine according to the requirements of application, such as, pay more attention to bandwidth, energy, link delivery ratio requirements or the distance to the destination, and satisfying the condition

$\alpha + \beta + \gamma + \varphi = 1.$

When computing the node's priority metric within the forwarding candidates set according to above formula, we can obtain a priority queue by sorting the priority metric Qi in descending order, the larger priority metric Qi, the higher priority for forwarding packets. And this priority queue is the candidate list.

CONCLUSION

To provide QoS for wireless ad hoc networks is very difficult and how to provide an efficient routing to deal with different priority flows. In this we proposeTORAP scheme contains forwarding candidates set selection, candidate's prioritization, and the opportunistic forwarding scheme. The former two parts determine the methods of selecting forwarding candidates and prioritization policies of forwarding candidates, and the latter gives a forwarding scheme which contains to determine when a node updates its candidates list and how to provide different QoS for different types of flows.

ACKNOWLEDGMENT

It is my privilege to acknowledge with deep sense of gratitude to Computer Engineering Department for their support and helpand cooperation.

REFERENCES

1. Yang Qin, Li Li , XiaoxiongZhong "Opportunistic routing with admission control in wireless ad hoc networks " ,0140-3664/2014 Published by Elsevier B.V.
2. WangBoHuangChuanheYangWenzhongWangTong "Trust Opportunistic Routing Protocol in Multi-hop Wireless Networks" 978-1-4244-5849-3/10 ©2010 IEEE
3. S. Biswas, R. Morris, ExOR: Opportunistic multi-hop routing for wireless 716networks, in: Proceedings of the 2005 Conference on Applications, 717Technologies, Architectures, andProtocols for Computer Communications 718SIGCOMM'05), Philadelphia, PA, USA, 2005, pp. 133–144. 719
4. S. Chachulski, M. Jennings, S. Katti and other., Trading Structure for Randomness in 720wireless opportunistic routing, in: Proceedings of the 2007 Conference on 721Applications, Technologies, Architectures, and Protocols for Computer 722Communications (SIGCOMM'07), Kyoto, Japan, 2007, pp. 169–180.
5. E. Rozner, J. Seshadri, Y.A. Mehta, et al., SOAR: Simple opportunistic adaptive 730routing protocol for wireless mesh networks, IEEE Trans. Mob. Comput. 8 731(2009) 1622–1635.
6. M.A. Ergin, M. Gruteser, L. Luo, et al., Available bandwidth estimation and 745admission control for QoS routing in wireless mesh networks, Elsevier 746Comput. Commun. 31 (2008) 1301–1317. 747
7. X. Gao, F. Wu, X.F. Gao et al., BREW: A bandwidth reservation protocol for 748multirateanypath routing in wireless mesh networks, in: Proceedings of IEEE 749Wireless Communications and Networking Conference (WCNC'13), Shanghai, 750China, 2013 pp. 1327–1332. 751
8. P. Zhao, X. Yang, J. Wang et al., BOR/AC: bandwidth-aware opportunistic 752routing with admission control in wireless mesh networks, in: Proceedings of 75331st IEEE INFOCOM, Orlando, FL, USA, 2012, pp. 2701–2705