Secure admission control based opportunistic routing scheme in WSN

Rashmi Kolekar[1] Mamta Nhavkar[2] Manasi Chakote[3]
[1,2,3]Department of Computer Engineering
[1,2,3]TSSM's Bhivarabai Sawant College og Engineering and Research, Narhe, Pune

Abstract— QoS in ad hoc wireless networks. In traditional routing scheme, if a node on the optimal path is broken due to lack of power available, the entire route will break, and the source must modify the redrawn. opportunistic routing is introduced to solve this problem that improves system performance. It is very difficult to provide better quality of service in the operating room because of the uncertainty of bypass roads. Most existing protocols or rarely consider the service for different types of flows. Opportunistic existing routing scheme uses admission control (ORAC) of nodes for different types of flows. ORAC scheme manage a new scheme flow admission control based on bandwidth, traffic and accumulation of the residual energy of the nodes to select candidates forwarding. Network security is also a subject of current research in WSN. Existing work in O considered one of QoS and security. In the proposed system we have taken security problem on the account while the program is adopted ORAC. To solve the security problems we have used the value of the confidence of network nodes.

Key words: WSN; SACOR

I. INTRODUCTION

In multi-hop wireless ad hoc networks, packets can be forwarded via 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 reroute again, and end-to-end QoS is difficult to guarantee. OR 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 . So that, the network throughput can be improved and the transmission delay can be reduced by using the OR scheme. Because OR has many characteristics, several representative works on OR have been proposed

II. RELATED WORK

MAC-Independent opportunistic routing and Coding (MAS), is an intra-session encoding scheme, CCACK network adopts a cumulative acknowledgment scheme coded receipt that allows network nodes recognize encrypted traffic to its previous nodes. Simple opportunistic adaptive routing (SOAR) adaptively selects forwarding nodes and uses timers based on the priority of maintaining multiple simultaneous streams in wireless mesh networks.

Network security is also a research topic on routing. WangBo et. Alabama. "TOR aims to offer a new solution to solve security problem by defining a new metric called E2TX (reliability 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 the classical opportunistic routing "Ergin et al. It presents a mechanism for admission control and routing for wireless mesh in multiple speeds, and admission control scheme is based on the estimate of available bandwidth. Moreover, Gao et al. discussed the multi-speed routing any routing scheme, which provides bandwidth reservation for traffic.In addition, bandwidth consious proposal or consideration.

III. METHODOLOGY

A. *Trust calculation and Updating:*

As a metric of the wireless link, the value of trust is used to indicate the reliability of the transmission behavior through the link.

confidence value of a node is calculated using the following equation,

$$T_j(k\ n)=R_{kj}(n)/F_{kj}(n) \quad (3.1)$$

Tj (k, n) = confidence value assigned node j / k calculated by the node during the nth cycle topology. Where RKJ (n) and FKJ (n) is the number of packets that have been received by and transmitted from j k at time t, respectively, and $0 \leq T(k, t) \leq 1$.

confidence value of a node is updated after each change of topology using following mathematical equation.

$$T_j(k, n) = \alpha . T_j(k,n-1)+(1-\alpha).T_j(k, n) \quad (3.2)$$

When Tj (k, n) is the value of node j confidence measured during the umpteenth update cycle topology. $0 < \alpha < 1$ is a weighting factor used for trade between the current measurement and the previous estimate.

The value of the combined metric routing node j is true only if the node j satisfies a precondition: $Tj \geq TThreshold$.

Where TThreshold is the threshold value of the confidence of the entire network, definition5 means that if the j node is not a node trust, that is, can be a selfish and malicious node, so we ignore the node and is not allowed its membership in the network.

B. *Flow admission control model in ORAC:*

Flow Admission Control with Opportunistic Routing is introduced, 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 a directed graph G(V,E), 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, hence,
V={n1; n2; n3; . . . ; ni; n_i+1; . . . ; n_n}

C. Available bandwidth:

Suppose a typical node in a wireless ad hoc network has a bandwidth C limited to service flows inbound traffic. We denote an incoming packet of a particular flow qkj data rate, where j is the priority class of flow and k is the number of the current. There m classes of flows in the network, the total set of classes denoted {1, 2 ,. . . , J ,. . ., M}. Suppose the class j is pj existing flows in a no intermediate node, flows whole class j can be expressed as {1, 2, ..., k, ..., pj} in or node. When a new stream you want to access a node- or intermediate transmission during the discovery phase of opportunistic path must satisfy the following condition.

$$q_{j+1}^{new} + \sum_{j-1}^{m}\sum_{k-1}^{\rho_j} q_j^k \leqslant C \qquad (3.3)$$

Where, q_j^{new} denotes the data rate of the new flow belonging to class j + 1 $\sum_{j-1}^{m}\sum_{k=1}^{\rho_j} q_j^k$ 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 congested node when in flows are more than you can cope . Therefore , a node can it be congested when it has a low bandwidth (due to sharing bandwidth with several neighbors or poor network status , etc.) and tail length is long is i.e , the packets are not able to be transmitted fast enough) . To provide better service quality , we also consider delay traffics in the buffer. The second criterion is to avoid congestion and to provide a better guarantee for a flow delay . Suppose , at any time , an intermediate node or contains bits total waiting in its buffer , WKJ is the number of bits waiting in a queue that belongs to a class k j flow . For the NI intermediate node when a new flow is admitted , it must satisfy the following inequality

$$C - \sum_{j=1}^{m}\sum_{k=1}^{\rho_j} \frac{w_j^k}{D_j - T_j^k} \geqslant 0 \qquad (3.4)$$

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.

$$T_j^k = \sum_{\omega=1}^{n_i} T_j^k(\omega) \qquad (3.5)$$

where $T^k_{j\,(w)}$ is the successfully transmission time of data flow from node x to next hop x1 for flow k of class j, which can be expressed.

$$T_j^k(\omega) = \sum_{l=1}^{L} T_j^k(l) \times p_j^k(l) \qquad (3.6)$$

Where,

$l\ (1 \leqslant l \leqslant L)$ 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.

$$T_j^k(l) = AIFS_j + T_{backoff_j}(l) + T^k_{j-Data} + R_\omega * T_{ACK} + R_\omega * SIFS \qquad (3.7)$$

where SIFS is the short inter-frame spaces, $AIFS_j$ is the arbitration inter-frame space defined in the IEEE 802.11e EDCA standard, $T_{backoff_j}(l)$ 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_{kj}-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 lth attempt for flow k of class j, denoted by p^k_j (*l*), which can be calculated as

$$p_j^k(l) = (1 - \delta_j^k)^{l-1} \times \delta_j^k \qquad (3.8)$$

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

The energy consumption of wireless ad hoc networks are a special type of wireless networks, which allow a group of nodes to configure and maintain a temporary network themselves, without the support of any fixed infrastructure. In the ad hoc wireless networks, the battery power of many nodes is limited. Therefore, we must consider the energy of these devices, the estimated energy consumption of them in packet transmission. We assume that the packet size is the same for different types of flows, and power sending nodes is constant, so that consumption of energy expended in the forwarding or receiving packets is also the same for different types flow. The power consumption of one or intermediate node for successful transmission of a packet to its downstream node, denoted IHD, which is composed of three parts: the energy EiF consumed to forward a packet, energy EiR is consuming to receive a package, and EiAck energy is consumed to send a confirmation packet. In this power module, the main energy consumption of nodes is used to transmit packets, and some other factors, such as energy attenuation nodes; we do not consider them [1]. Therefore, we

$$E_{iC} = E_{iF} + E_{iR} + E_{iAck} \qquad (3.9)$$

We assume that EIT indicates the total energy of a node NI . In addition , according to the mechanism OR, or node must send an acknowledgment to the upstream node when a packet is received . Therefore , the residual energy EIR node NI front packets belonging to the queue buffer existing class j can be expressed

$$E_{ir} = E_{iT} - \sum_{j=1}^{m}\sum_{k=1}^{\rho_i} \frac{w_j^k}{pktsize}(E_{iF} + E_{iR} + E_{iACK}) \quad (3.10)$$

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

$\sum_{j=1}^{m}\sum_{k=1}^{\rho_i} \frac{w_j^k}{pktsize}$ 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.

$$E_{ir} - r_{j+1}^{new} \times (E_{(j+1)F} + E_{(j+1)R} + E_{(j+1)ACK}) \geqslant 0 \quad (3.11)$$

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 entering the consumption model available bandwidth , traffic delay and energy , we give our scheme admission control key idea is that a node can admit a new flow if you have enough bandwidth , energy and buffer space . And then , we can select it as forwarding nodes in the discovery phase of opportunistic route. Therefore , any intermediate node or support a new stream of class j + 1 containing r_{j+1}^{new} packets with data rate q_{j+1}^{new} when it satisfies the following inequality.

$$\begin{cases} C - \sum_{j=1}^{m}\sum_{k=1}^{\rho_i} q_j^k - \sum_{j=1}^{m}\sum_{k=1}^{\rho_i} \frac{w_j^k}{D_j - T_j^k} - q_{j+1}^{new} \geqslant 0 \\ E_{ir} - r_{j+1}^{new} \times (E_{(j+1)F} + E_{(j+1)R} + E_{(j+1)ACK}) \geqslant 0 \end{cases} \quad (3.12)$$

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.

F. Forwarding scheme in SACOR:

In this section , we introduce our ORAC diversion scheme for different types of flows in detail. The SACOR schema contains three components : the candidate selection set forward , prioritization of candidate and opportunistic diversion scheme . The first two parts determine the methods of selecting candidates and political forwarding prioritization of candidates forwarding , and the second provides a diversion scheme containing to determine when a node updates its list of candidates and how to provide different QoS for different types of flows . Then we introduce respectively.

F. Forwarding candidates set selection:

Selecting appropriate metrics to determine forwarding candidates set is very important. In the SACOR protocol, a new method for selecting candidates forwarding established, which is based on admission control flow and the value of trust node in the set of candidates is proposed. The details are expressed as follows.

Earlier algorithms, the distance between any two network nodes must be calculated using the location service module. This can be easily performed because the network topology is static. And for Ni network node, neighbors jumped can be determined when we established the transmission range of nodes. Select the nodes that the distance between them and the destination node is shorter than the distance between the node and and destination within neighbors jumped and then collect these nodes in a set, denoted by the set temporary, TSi. (TSI = {n1, n2, ..., Nr}). Moreover, the value of available bandwidth, traffic delay, the residual energy and confidence of the nodes that are at stake TSi is calculated. First, we check that the nodes are more trustworthy for their confidence value in the cycle of the current network topology.

If T (n) ≥ Tthreshold then add the node Si.Then TSi to check that the nodes in the set if have sufficient resources to admit a new flow according to the formula .After that , store nodes that satisfy the formula

set $Q_i = \{n_1, n_2, \ldots, n_\psi\}\ (Q_i \subseteq S_i, \psi \leq r)$ & T(n) ≥ $T_{threshold.}$

where Q_i is the forwarding candidates set of node n_i.

H. Candidate selection using SACOR:

[1] When the node joins the network first, the confidence value is assigned to the 0.5 / calculated, meaning node is not a malicious node.
[2] Once the first cycle of confidence value is calculated concluded.
[3] In each confidence value is updated topology cycle.
[4] Calculate the distance of each node from other nodes in the network using the location service module.
[5] After calculating the distance each node calculated its temporary candidate TSi established based on the confidence value of the nodes of the range.
[6] Calculate the bandwidth available and necessary for the incoming flow.
[7] Calculate the current traffic backlog and incoming traffic for the node.
[8] Calculate requires energy and the residual energy of the node.
[9] Check if sufficient resources are available, if the node has sufficient resources then add that node to the set of Si.
[10] If Node to establish Qi if the node itself satisfies T (n) ≥ Tthreshold

IV. Routing Algorithm

```
Route_Packet(P)
{
Receive_Packet(P);
S ← Get_Src(P);
D← Get_Dest(P);
If(D==NodeID)
{
Process_Packet();
}
Else
{
L=Get_NeighborList(NodeID);
```



```
For(all nodes in list L)
{
Calculate_Trust();
Check_Bandwidth();
Check_BackLogTraffic();
CheckAvail_Energy();
}
Candidate_selection();
Prioritizatio();
Send_Packet(p);
        }
}
```

In WSN network, for routing the packet firstly packet is created and then the packet is send from source to destination. For this purpose SACOR protocol is used, in this protocol new admission control is created. In this some parameters are checked those are to calculate trust, the value must be greater than threshold value. To calculate bandwidth, in this parameter the network must has limited bandwidth C to service incoming traffic flows. To check backlog traffic, in this parameter for providing better QoS consider backlog traffics in buffer. To check available energy, the node must have sufficient energy to send and receive packet. After checking all this parameter candidate selection is done in which the node is selected. Then prioritization is done and finally packet is send.

V. FIGURES

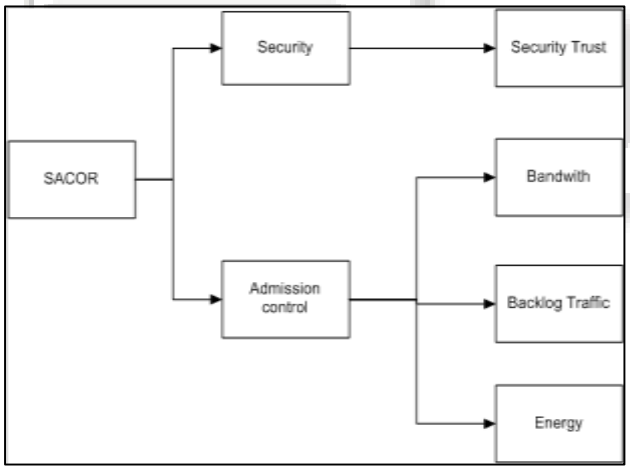

Fig. 1: Proposed model

In this figure, SACOR protocol is used. There are two main parameters, those are security and admission control. In security parameter, security trust is calculated. In admission control parameter, bandwidth, backlog traffic and energy are calculated.

VI. CONCLUSION

To provide better QoS in wireless ad hoc networks is a challenging issue, and how to explore an efficient routing scheme to service for different priority flows is a difficult but meaningful work. In this method, we propose opportunistic routing scheme joint with admission control named as SACOR for different priority flows in wireless ad hoc networks with security.

REFERENCES

[1] Yang Qin, Li Li , Xiaoxiong Zhong "Opportunistic routing with admission control in wireless ad hoc networks " ,0140-3664/2014 Published by Elsevier B.V.
[2] Lyes Khoukhi , Hakim Badis , Leila Merghem-Boulahia & Moez Esseghir "Admission control in wireless ad hoc networks", Khoukhi et al. EURASIP Journal on Wireless Communications and Networking 2013.
[3] WangBo HuangChuanhe YangWenzhong WangTong "Trust Opportunistic Routing Protocol in Multi-hop Wireless Networks" 978-1-4244-5849-3/10/$26.00 ©2010 IEEE.
[4] Ismail Butun and Ravi Sankar "A Brief Survey of Access Control in Wireless Sensor Networks", Department of Electrical Engineering, University of South Florida, Tampa, FL, USA 2009.
[5] Anatolij Zubow, Mathias Kurth, and Jens-Peter Redlich "Considerations on Forwarder Selection for opportunistic Protocols in Wireless Networks", Humboldt University, Germany 2008.
[6] S. Nelakuditi, Z. Zhang, R.P. Tsang, et al., Adaptive proportional routing: a ocalized QoS routing approach, IEEE/ACM Trans. Network. 10(2002) 790–804.
[7] Y. Xiao, H. Li, Local data control and admission control for QoS support in wireless ad hoc networks IEEE Trans. Veh. Technol . 53 (2004) 1558–1572.
[8] X. Yang, N. Vaidya, Priority scheduling in wireless ad hoc networks, Wireless Netw. 12 (2006) 273– 286
[9] S. Toumpis, A.J. Goldsmith, Performance, optimization and cross-layer design of media access protocols for wireless ad hoc networks, in: IEEE International Conference on Communications (ICC'03) Anchorage, Alaska, USA, 2003, pp. 7092234–2240.
[10] M. Conti, G. Maselli, G. Turi, et al., Cross-layering in mobile ad hoc network design, IEEE Comput. 37. (2004) 48–51

