Collision Avoidance Mechanism In Wireless Ad Hoc Networks Through Distributed Mac Protocol

Dr. B.Vijaya Babu[#1], **G. Kiran Kumar**[*2]
[#]*CSE Department, KL University Guntur-IND*

Abstract-In this paper we are going to analyse Medium Access Control Protocols for high performance in Ad hoc Networks by increasing reliability in data transmission. In the mean while we can reduce collision among the nodes while transmitting information, by using collision avoidance Techniques. Medium access control (MAC) has been one of the important issues in wireless networks; CSMA/CA has been used in many high-speed and low-speed networks because of its robustness and simplicity. Performance of the medium degrades due to heavy collision among nodes and due to hidden-node problem.To achieve high-performance MAC is still an important issue in ad-hoc networks.Wireless networks are divided into one-hop or multi hop networks. Depending on the number of wireless nodes over which a packet is relayed. Most of the existing networks are one-hop, that is simple network and the complex network.

Keywords— MAC, CAIN, CSMA/CA, Complex network

I. INTRODUCTION

An Ad Hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to keep the network connected. Ad hoc networks may be formed or merged together into separate networks on the fly [1], without necessarily depending on a fixed infrastructure to manage the operation. Nodes of Ad hoc networks are often mobiles, which also implicates that they apply wireless communication to maintain the connectivity, in this case the networks are called as mobile ad hoc networks (MANET). Mobility is not a requirement for nodes in ad hoc networks. In ad hoc networks they may contain static and wired nodes, which may use services offered by fixed infrastructure. Ad hoc networks may be different from each other, depending on the area of application [4][1].

As ad hoc networking somewhat varies from the more traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in ad hoc networks [2][3]. While the basic security requirements such as confidentiality and authenticity remain, the ad hoc networking approach somewhat restricts the set of feasible security mechanisms to be used, as the level of security and on the other hand performances are always somewhat related to each other. The performance of nodes in ad hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained .

Wireless ad hoc networks are an important platform for bringing computational resources to diverse contexts. These networks are characterized by limited devices, deployed in novel environments in an ad hoc fashion (that is, typically, no a priori knowledge of the environment or connection topology is assumed). Direct communication is possible only with neighbours through the use of local radio broadcast. Devices in ad hoc networks are commonly low-cost (to ease the expense of large, rapid, and temporary deployments), they are prone to unpredictable crash failures [3]. Similarly, their local clocks can operate at varying rates depending on temporal environmental effects such as temperature, complicating the task of maintaining synchronized clocks.

Many solutions have been proposed to mitigate some of this uncertainty. For example, the most widely used MAC layers in wireless ad hoc networks make use of physical carrier sensing and exponential back off to help reduce contention on the channel.

II. LITERATURE SURVEY

Calvin Newport In his study, considered the fault-tolerant consensus problem in Ad hoc networks with crash prone nodes. We develop lower bounds and matching upper bounds for this problem, in single-hop wireless networks, where all nodes are located within broadcast range of each other. In a novel break from existing work, we introduce a highly unpredictable communication model in which each node may lose an arbitrary subset of the messages sent by its neighbors during each round. This model better matches behaviour observed in studies of these networks.

Jaume Barcelo et.al, proposed, in some wireless Ad-hoc networks it is not possible to depend on carrier-sensing mechanisms to prevent collisions. We suggest a MAC protocol that reaches collision-free operation in sparse ad-hoc wireless networks when all the stations are decomposed. Each participating stations can make its own backoff parameter after collecting information from its neighbourhood. The system enters in a transient-state until collision free operations are reached. We assume the duration of the transient-state and other performance metrics with an example scenario and finally we make two options to incorporate reception acknowledgements.

Vesa Kärpijoki done a work on ad hoc networks the communicating nodes does not rely on a fixed infrastructure, which makes new challenges for the necessary security architecture they apply. Ad hoc networks are designed for specific tasks and may have to function with full availability even in more difficult conditions, security solutions applied in more traditional networks may not directly be suitable for protecting them [5]. A short literature study over on ad hoc networking shows that most of the new generation Ad hoc networks are not yet able to address the security problems they face. Environment specific implications on the required approaches in implementing security in such dynamically changing networks have not yet fully realized.

Yu Wang J. J. Garcia-Luna-Aceves Three collision-avoidance protocols are analysed .It uses Omni-directional packet reception together with Omni directional transmissions, directional transmissions or a combination of both. A simple model is introduced to analyse the performance of these collision avoidance protocols in multi-hop networks. The results of this analysis show that collision avoidance using a narrow antenna beam width. For both transmissions of all control and data packets achieves the highest throughput among the three collision avoidance schemes. Simulation experiment of the IEEE 802.11 protocol and its variants based on directional transmissions and Omni-directional packet reception validate the results in the analysis. Its show that the advantage of spatial reuse achieved by narrow-beamwidth transmissions outweighs that of conservative collision avoidance schemes featured by the omnidirectional transmission of some control packets.

EXISTING SYSTEM

The Radios which are used in previous mechanisms of collision avoidance in Ad-hoc Networks uses half-duplex and which can tune only one channel at a time. So it is very difficult to find the collisions at all the channels or nodes.

PROBLEM DEFINITION

In the proposed system for collision avoidance in Ad-hoc networks uses Distributed Mac protocols and which will work on the Carrier Sense and Collision Avoidance Principle. Here it overcomes the hidden node problem at the intermediate nodes. The chances of collision occurrence is high at the intermediate nodes so if we decrease the collision at that instance automatically the transmission rate of the information increased by 75 percent. Here we use two collision Avoidance Mechanisms namely Out of band approach and Hand shaking Approach.

SYSTEM MODEL:

Most distributed MAC protocols are based on the principle of carrier sensing & collision avoidance (CSMA/CA). Hidden terminals play very dominant role in CSMA/CA based protocols

Collisions that occur at the destination may not be heard by the sender Therefore receiver has to send some kind of feedback to sender. There are mainly two types of approaches for collision avoidance they are,

1. Out-of-band Approach
2. Hand Shaking Approach

Out-of-band approach:

In Ad-hoc networks Hidden node plays a prominent role because it is one reason for occurring collision so by finding the hidden node in the network we can avoid collision at the intermediate nodes. Out-of-band approach uses Busy Tone Multiple Access (BTMA) (Tobago & Kleinrock, Haas) protocol uses out of band signalling to solve hidden terminal problem[2][3]. For this busy tone a separate channel is required for all the node in the Network. Any node hearing ongoing transmission transmits busy tone. All nodes hearing busy tone will remains silent. All nodes in 2R radius of the transmitter keep silence. Avoids interference from hidden terminals.

In the Network the receiver first initiates the busy tone and sends it to all the nodes which are in the range of R. It Avoids interference from hidden terminals and Eliminates hidden nodes, and increases exposed nodes [2].

The idea is to transmit a signal on different frequency to notify an on-going data transmission. If hearing an on-going transmission, transmit a busy tone, If hearing a busy tone, do not initiate any transmission. BT eliminates the hidden node problem, while increases the number of exposed nodes. This Require different frequencies for data and Out-of-band signalling.

Algorithm [CAIN] Collision Avoidance at Intermediate Nodes in Out of band Signalling:

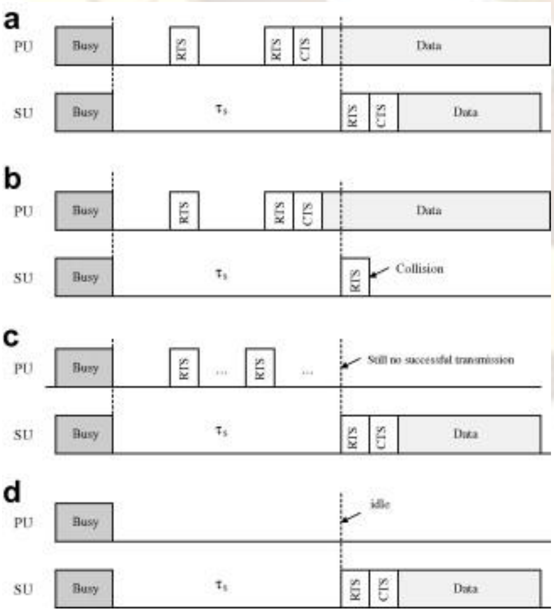
Function 1
handle_collision()

```
if (pkt_CTRL == NULL) then
  p = random(0,1);
  if (p < P_RRTS) then
    if (inc_NAV == TRUE) then
      NAV(RRTS) = DIFS + k·CW_min + RTS + SIFS + CTS;
      timeout = TX(RRTS) + δ + DIFS + k·CW_min + TX(RTS) + δ;
    else
      NAV(RRTS) = DIFS + CW_min + RTS + SIFS + CTS;
      timeout = TX(RRTS) + δ + DIFS + CW_min + TX(RTS) + δ;
    end if
    pkt_RRTS = create_RRTS(BDCST, NAV(RRTS));
    defer(EIFS);
    backoff(CW_min);
    transmit(pkt_RRTS);
    set_timer(timeout);
  end if
end if
```

In out of band signalling mechanism we use busy tone and CAIN algorithm for collision avoidance in Out of band signalling.

Hand Shaking Approach:

The idea is based on three-way handshaking to deal with hidden node. A node with a packet to transmit sends a short request-to-send (RTS) message to the destination. Upon receiving RTS, the corresponding destination responds by a clear-to-send(CTS) message [2][3]. Nodes receiving either of the above mentioned messages defer their transmission for the duration of the transfer included in both RTS and CTS. This duration is called Network Allocation Vector (NAV), Sender transmits the date to the destination.



From the above diagram the RTS message has been sent by the sender, and the CTS has been sent by the receiver to get the information from the sender. The algorithm represents the prehand shaking mechanism for collision avoidance.

Algorithm 1 PHED-GR (Pre-Handshaking):

1: if $A_f = 1$ then. A has successfully sent M_d
2: A will keep silent in TR and exit.
3: end if
4: Node A decides and send M_s by probability $1/A_n$ and keep listening by probability $1- 1/A_n$.
5: if A sends M_s Then .A hopes to send M_d in TR.
6: if A does not receive M_s during GR then
7: A will transmit M_d in TR;
8: else. A receives M_s from other nodes
9: A will transmit M_d in TR by probability 1/2.
10: end if
11: else. A does not send M_s
12: if A does not receive M_s during GR then
13: A will transmit M_s in TR by probability $1/A_n$;
14: else A receives M_s from other nodes
15: A will keep silent in TR.
16: end if
17: end if.

In In-band signalling we are using pre handshaking algorithm instead of handshaking mechanism .Here we can also use INSIGNIA mechanism for quality of service and collision avoidance in wireless ad hoc networks.

CONCLUSION

In this paper we are analysing collision avoidance in wireless ad hoc networks using CAIN algorithm and busy tone in out of band signalling, and Pre-Hand shaking algorithm in In-band signalling for collision avoidance and Quality of Service.

REFERENCES

[1] J. I. Chhoi, M. Jain, K. Srinivasan, P.Levis, and S.Katti. "Achieving, Single Channel, Full Duplex Wireless communication". In Proc. Of ACM MobiCom.
[2] M. Jain, J. I. Chhoi, T. M. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha. "Practical, Real-time, Full Duplex Wireless".In Proc. of ACM MobiCom, 301-312, 2011.
[3] M. J. McGlynn and S. A. Borbash. "Birthday Protocols for Low Energy Deployment and Flexible Neighbor Discovery in Ad Hoc Wireless Networks". In Proc. of ACM MobiHoc, 137-145, 2001.
[4] S. Vasudevan, D. Towssley, D. Goeckel, and R. Khalili. "Neighbour Discovery in Wireless Network and the Coupon Collector's Problem". In Proc. of ACM MobiCom 181-192, 2009.
[5] W. Zeng, X. Chen, A. Russell, S. Vasudevan, B. Wang, and W. Wei. "Neighbour Discovery in Wireless Network with MultiPacket Reception". In Proc. of ACM MobiHoc