Techniques Of Detection Of The Hidden Node In Wireless Ad Hoc Network

MOSTEFA Fatima zohra, MEKKAKIA Maaza zoulikha, KHELIFA Said

***Abstract*—In the wireless ad hoc networks, every node is assured by an individual battery which the consumption for the communication and the calculation of data must be optimized to avoid the problem of energy consumption. In the wireless ad hoc network, MAC protocol synchronizes the access of nodes to the channel. The access to the medium collides with two classic problems in wireless , hidden node problem which provoke collisions of packet and the exposed node problem but our paper treats the problem of hidden node. The active detection and the passive detection allow to resolve the problem of the hidden node. In the passive detection a mechanism RTS / CTS is used. The paper treats the power consumption provoke by RTS/CTS mechanism to detect hidden node for every node to have a better knowledge of the topology of the network and preserving its energy consumption**

***Index Terms:* RTS, CTS, Ad hoc, hidden node.**

I. INTRODUCTION

The wireless ad hoc networks are networks which get organized automatically and be deployable quickly, without fixed infrastructure with decentralized control. Every mobile node in MANET (Mobile Ad hoc NETwork) works as a relay to establish a communication multi hop between two nodes. hidden and exposed node problem is a common phenomenon due to the multi hop which acts negatively on the MAC (Medium Acces Control) protocol. The mobile ad hoc networks are characterized by a dynamic topology, a limited bandwidth, constraints of energy and a limited physical security.

II. THE CLASSIC PROBLEMS IN HERTZIAN COMMUNICATION

A. Hidden node problem

Suppose that the node A is in transmission with the node B. if the node C decides to send data to the node B, by listening to the channel it will suppose it free. The node C starts a transmission towards B and makes a collision at the node B. In this scenario which is in Figure 1, the node C is a hidden node from the node A [10].

MOSTEFA Fatima zohra is with the Science computer Departement,University of Sciences and Technology of Oran Mohamed Boudiaf USTO-MB, Oran, Algeria (e-mail: fati.mostefa@hotmail.com).

MEKKAKIA Maaza zoulikha is with the Science computer Departement,University of Sciences and Technology of Oran Mohamed Boudiaf USTO-MB, Oran, Algeria (e-mail: mekkakia@univ-usto.dz).

KHELIFA Said is with the Science computer Departement,University of Sciences and Technology of Oran Mohamed Boudiaf USTO-MB, Oran, Algeria (e-mail: said.khelifa@yahoo.fr).

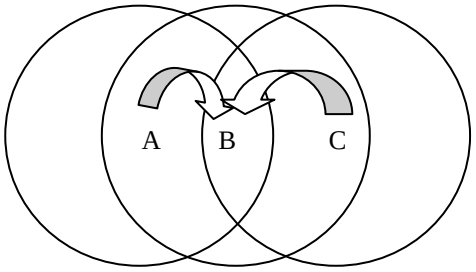

Fig. 1. The hidden node problem

III. HIDDEN NODE DETECTION

A. Active detection

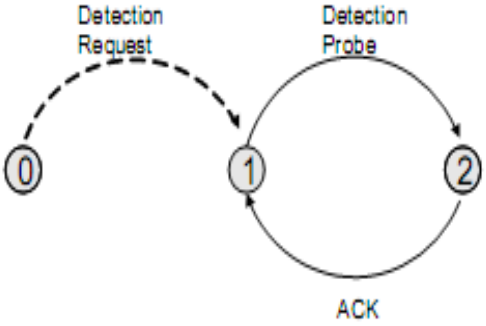

Fig. 2. Active detection mechanism

Figure 2 illustrates the active detection mechanism, where node 0 is the detecting node. Two new types of packets, referred to as ‘detection request’ and ‘detection probe’ packets, have been introduced. With active detection, each node that wishes to know its potential hidden terminals will actively generate a detection request to all its one-hop neighbors. (Neighbor information can be obtained by for instance exchanging Hello messages defined in ad hoc routing.) .All neighbor nodes that receive this request will then start sending a sequence of unicast probe packets to their neighbors, for a time interval specified in the detection request. The detecting node will then perform measurements on the traffic generated by the neighbors. Based on the received packets, the detecting node is able to establish a complete list of all its hidden terminals, including those that may not be discovered by passive detection [10].

ISBN: 978-988-19251-4-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

B. *Passive detection*

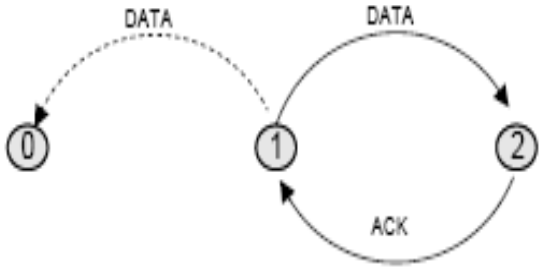

Fig. 3. Passive detection without RTS/CTS

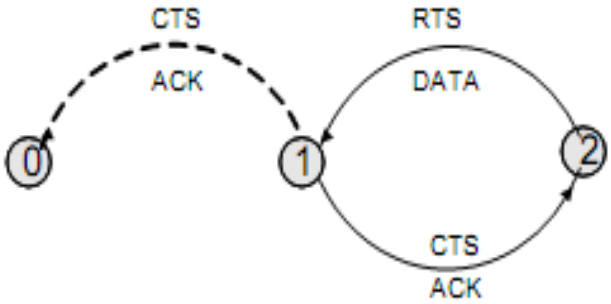

Fig. 4. Passive detection with RTS/CTS

Figures 3 and 4 show two different cases of passive detection, depending on whether RTS/CTS is being used or not by the transmitting neighboring nodes. In both figures, nodes 0 and 2 are hidden terminals to each other. When RTS/CTS is disabled (Figure 3), the detecting node (node 0) is able to hear the DATA frame sent by its immediate neighbor (node 1), but not the ACK frame sent by node 2. (According to 802.11, a node that has successfully received a unicast DATA packet destined for it, must reply with an ACK.) Since it does not receive the ACK, node 0 suspects that node 2 is a hidden terminal to it. Node 2 is confirmed as a hidden node after having recorded several subsequent missing ACKs by node 0. The MAC address of the hidden terminal is extracted from the receiver field of the DATA frame.

Figure 4 illustrates the other case where RTS/CTS is used in the neighborhood of the detecting node. Here node 2 is attempting to send DATA packets to node 1. As depicted in the figure, the detecting node (node 0) can only hear the CTS and the ACK frames sent by node 1, which are supposed to arrive after the RTS and DATA frames. Based on this information, node 0 concludes that there is a hidden terminal in its vicinity and extracts correspondingly the MAC address of the hidden terminal. If the background traffic is initiated from node 1 and destined at node 2, the detecting node receives the RTS and DATA frames, but not the CTS and ACK frames. The hidden terminal can also be easily detected in the same way [10].

IV. RTS/CTS MECHANISM IN 802.11-DCF

To prevent collisions as a result of the hidden terminal problem additional control packets were introduced to the DCF(Distributed Coordination Function) to access to the channel: The request to send (RTS) packet is sent in the beginning of the transmission (after the channel was idle for at least DIFS) by the sender and contains a duration field. This states the duration for CTS, Data and ACK packet (inclusive all inter frame spaces). All receiving stations set their Net Allocation Vector (NAV) to this value illustrate in figure 5 . The NAV describes the point of time until the medium will be busy. The receiver answers the RTS with the clear to send (CTS) packet after SIFS containing a duration field too with the time interval for data, ACK and interfame spaces (IFS). Every station which receives the CTS sets its NAV to the duration field. With this RTS/CTS mechanism all stations in the coverage of sender and receiver are informed about the duration of this transmission and should not disturb. As the RTS packet can be sent at least after a DIFS-idle medium the RTS/CTS mechanism does not prioritize stations. As collisions can only occur with a RTS-packet the mechanism is an excellent collision protection for big frames. The main disadvantage is the overhead of RTS/CTS which leads to a waste energy of each blocked node [12].

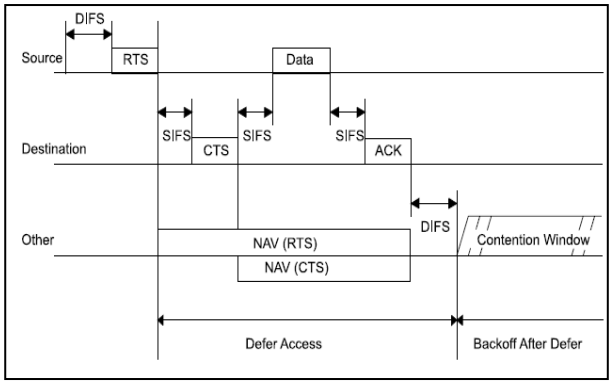

Fig. 5. RTS/CTS in 802.11-DCF

V. PROBLEMS WITH RTS/CTS MECHANISM

A. *Inhibiting non-interfering parallel transmissions*

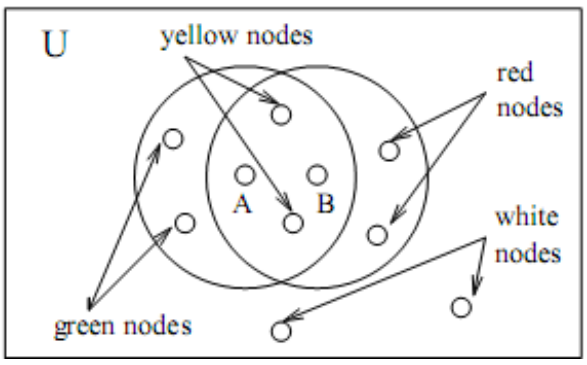

Fig. 6. Inhibing non-interfering parallel transmissions

Suppose that A is transmitting to B (Figure 6). If a green node, (being outside the range of B) decides to transmit to a white node, its transmission will cause no damage at B; however, the green node is within the range of A, so it won't be able to receive anything while A is transmitting. Similarly, a red node (located within the range of B but outside the range

ISBN: 978-988-19251-4-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

of A) is technically able to receive (from the white nodes) while B is receiving from A. Only the yellow nodes are truly restricted: they must not transmit, and they are also unable to receive. A node can determine its color with respect to an ongoing transmission as the involved nodes go through the RTS/CTS mechanism. In our sample scenario (Figure 6), when A sends the RTS packet, it will be received by all green and yellow nodes. When B responds with CTS, all red and yellow nodes will be able to hear it. Thus, a node recognizing the RTS packet will paint itself green, a node recognizing the CTS packet will paint itself red, and a node that overhears them both will be painted yellow.

In summary, the RTS/CTS mechanism, aimed at the elimination of hidden nodes, introduces a new problem: it hinders some non-interfering transmission that could be carried out in parallel [11].

B. *False blocking*

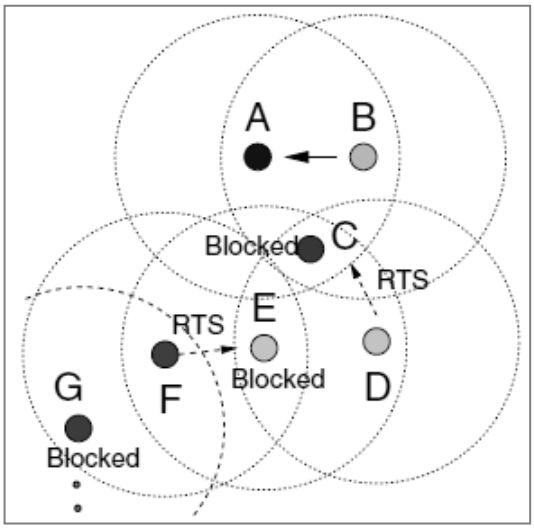

Fig. 7. False blocking

We suppose that the node B sends a data to the node A thus the node C is blocked. Whereas the node C is blocked, the node D sends packet RTS to the node C but the node C does not answer. However, the node E receives packet RTS and refrains from itself of the transmission. The node E is thus a false blocked. The problem of blocking is located to the neighbours of the blocked node by producing a reduction of the performance of the network and increase the energy consumption for the blocked nodes because the overhead is to high [11].

C. *Virtual jamming*

This problem consists to sending a false RTS packet by malicious node to maximizing the duration of sending in time to live fields to block node without any transmission of data and to lose energy for the mobile node [11].

VI. OUR APPROACH EXPLANATION

This paper treats the problem of energy consumption when the nodes are blocked with RTS/CTS mechanism used in the passive detection of hidden node. In figure 4,to reduce the energy consumption in the passive detection with RTS/ CTS by putting all the neighbors of node 1 in sleep mode except the destination node when they hear CTS packet. These nodes will be in sleep mode until the ending of time of sending the data packet then became in wake up mode at the end of communication, in Figure 4 when the node 1 send the CTS packet to the node 2, the neighbors of the node 1 listen to the CTS packet and they can extract The MAC address of the node 2 by CTS packet which represents the hidden node from the node 0.

VII. SIMULATION RESULT

The simulation for hidden terminal detection are carried out using ns2.29 (network simulator) with some code modifications in the file mac-802_11(.h,.cc) to detect a hidden node with passive detection using RTS/CTS mechanism in the case when each two nodes in the network try to send data at the same receiver in the same time .We modify some lines in the function void Mac802_11:: recv_timer() in the file mac-802_11.cc the following lines:

```
  if(subtype == MAC_Subtype_ACK && dst != index_) {add_hidden_node(dst);}

    void Mac802_11::add_hidden_node(int noeud)
    { if(noeud==index_){printf("\n                                    \n
**********\n\n"); goto il_existe;}
    printf("========%d=====add                    ===> %d\n",index_,noeud);
      struct table_n_cach *temp;
      if(table==NULL) {
            table = (struct table_n_cach*)malloc(sizeof(struct table_n_cach));
            table->val = noeud;
            table->next = NULL;
            goto il_existe;}

      else {

  if(table->next==NULL){if(table->val==noeud){printf("\n IL EXISTE\n");goto il_existe;}
            else{table->next=(struct table_n_cach*)malloc(sizeof(struct table_n_cach));
        table->next->val = noeud; table->next->next=NULL; goto il_existe;}
                  }
temp = table;

while (temp != NULL) { if(temp->val==noeud) {printf("\nIL EXISTE\n"); goto il_existe;}
                  //printf("  %d\n",temp->val);
                  temp=temp->next;
                  }

struct table_n_cach *temp2;
temp2 = (struct table_n_cach*)malloc(sizeof(struct table_n_cach));

    temp2->val=noeud;
    temp2->next = (struct table_n_cach*)malloc(sizeof(struct table_n_cach));
    temp2->next=table; table=temp2;
```

ISBN: 978-988-19251-4-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

```
        }

il_existe :
    //PRINTING
          struct table_n_cach *tempR; int i=1;
          tempR = (struct table_n_cach*)malloc(sizeof(struct
table_n_cach));
          tempR = table;
    while(tempR != NULL) { printf("|%d
  %d\n",i,tempR->val); i++; tempR=tempR->next; }
    }
```

And we add two functions sleep_mode() and wakeup_mode() in the file mac-802_11(.h,.cc) to put the node in sleep and wake up mode :

```
void Mac802_11::sleep_mode()
state_=SLEEP;
radioState_=RADIO_SLP;
phy *p;
p=netif_;((wirelessPhy*)p->node_sleep();

void Mac802_11::wakeup_mode()
state_=IDLE;
if(radioState_=RADIO_SLP)
radioState_=RADIO_IDLE;
phy *p;
p=netif_;((wirelessPhy*)p->node_wakeup();
```

TABLE 1 Simulation parameters

Routing protocol	AODV
Transmission range	200m
Traffic	CBR/UDP
Packet size	350 bytes
Transmission interval inter packets	0.05 second
Simulation duration	100 seconds

The table 1 gives the simulation parameters use in NS2 in Tcl file.

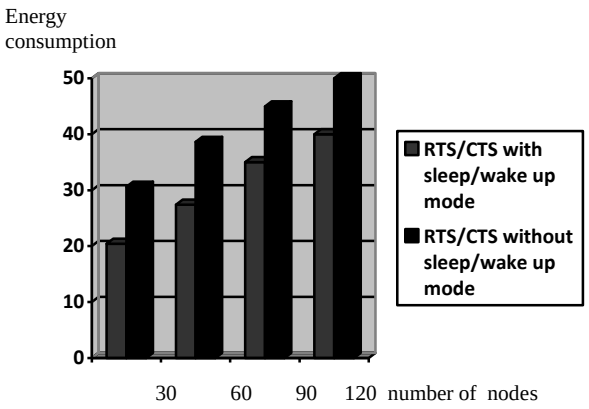

Fig. 8. Simulation result

The figure 8 illustrate the comparison with passive detection (RTS/CTS without sleep/wake up mode) with passive detection(RTS/CTS with sleep/wake up mode) and we see the power consumption in MAC 802.11 in passive detection (RTS/CTS with sleep/wake up mode) to detect a hidden node is low to compare with power consumption in passive detection (RTS/CTS without sleep/wake up mode) when the number of node increase in the network .

VIII. CONCLUSION AND FUTURE WORK

The problem of hidden node and the problem of energy are well-known problems in wireless ad hoc network, two mechanisms of detection of hidden node are introduce, active detection to produce a high consumption in bandwidth, passive detection give not all hidden nodes in the network but active detection indicates all hidden nodes. The combination with active detection and passive detection (with RTS/CTS sleep/wake up mode) is possible in future work to have a global topology of network to detect all hidden node and to reduce energy consumption.

REFERENCES

[1] N. Abramson : The ALOHA system—another alternative for computer communications, in Proceedings of the Fall Joint Computer Conference, NJ, vol. 37, pp. 281–285 ,(1970).

[2] F. A. Tobagi and L. Kleinrock, : Packet Switching in Radio Channels: Part II—The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution," IEEE Transactions on Communications, vol. 23 (12), pp. 1417- 1433, (1975).

[3] P. Karn : MACA - A new channel access method for packet radio, In proceedings of the ARRL/CRRL Amateur Radio 9th computer Networking Conference (1990).

[4] Sunil Kumar, Vineet S. Raghavan, Jing Deng : Medium Access Control protocols for ad hoc wireless networks: A survey, Vineet S. Raghavan b, Jing Deng Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13699, United States ELSEVIER (2004).

[5] A. D. Vaduvur Bharghavan, Scott Shenker,Lixia Zhang,: MACAW a media access protocol for wireless LAN's, In proceedings of the Communications architectures, protocols and applications (1994).

[6] C.L. Fullmer, J.J. Garcia-Luna-Aceves : Floor Acquisition Multiple Access (FAMA) for packet-radio networks, in: Proc. ACM SIGCOMM, Cambridge MA, August 28– September 1, (1995).

[7] C. Yu, B. Lee, S. Kalubandi, M. Kim, Medium access control mechanisms in mobile ad hoc networks, in: I. Mahgoub, M. Ilyas (Eds.), Mobile Computing Handbook, CRC Press, Boca Raton, FL (2004).

[8] Frank Y. Li, Arild Kristensen, ,Paal Engelstad : Hidden Terminal Detection in 802.11-based wireless Ad Hoc Networks University Graduate Center, University of Oslo, N-2027, Kjeller Norway (2006).

[9] ANSI/IEEE Std 802.11 – 1999: Wireless LAN Medium Access Control (MAC) and Physical(PHY) Specifications,(1999).

[10] m. j. saeed, m. merabti, r. j. askwith: hidden and exposed nodes and medium access control in wireless ad-hoc networks , school of computing and mathematical sciences liverpool john moores university byrom street, Liverpool l3 3af, uk (2006)

[11] Saikat Ray, Jeffrey B. Carruthers and David Starobinski :RTS/CTS-Induced Congestion in Ad Hoc Wireless LANs.

[12] sven wietholter,Christian hoene: design and verification of an IEEE 802.11e ECDF simulation model in NS2.26,technical university of Berlin telecommunication network group (2003).

ISBN: 978-988-19251-4-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)