Pure Contention-Based MAC Layer Protocols to avoid The Hidden Node Problem – A Review

Navpreet Kaur
Student, Department of IT
UIET, PANJAB UNIVERSITY
Chandigarh, UT
nvprtkr7@gmail.com

Mrs. Inderdeep Kaur Aulakh
Head of the Department
UIET, PANJAB UNIVERSITY
Chandigarh, UT
ikaulakh@yahoo.com

Abstract- One of the problems in Cognitive radio is the hidden node problem which as a result of sightless collisions leads to packet loss, degrading the QOS of the network, delays in transfers and many more problems. In this paper we discuss the advancements made in contention-based protocols to avoid the hidden node problem. We arrange them in three classes, which are Sender-initiated, Receiver-initiated and Hybrid protocols. In the end, we discuss the challenges associated with hidden node problem.

Keywords-*hidden node problem, protocol categorization, sender-initiated, receiver- initiated, hybrid*

*****

I. INTRODUCTION

Multiple Access Control (MAC) protocols play a very crucial role in performance of the networks. Adequate methods of bandwidth sharing and accessing channels must be described. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the well-known MAC protocol in which each node performs carrier sensing mechanism before initiating any communication with other networks or nodes. If the sensed channel is not idle, the node delay its communication and if the channel is idle, the node is allowed to communicate. Nevertheless, the presence of hidden nodes within the network may lead to collisions. [1]

In 1975, Kleinrock and Tobagi described the hidden node problem [2]. Figure1. depicts the
hidden node problem. Assume that node X is in communication with node Y but not with node Z. Node Y can hear communications from both node X and node Z as any node situated in sensing range of the other node is able to hear it's packets conveniently. However, collision will take place if node X and node Z communicate simultaneously in the same interval of time with node Y, as nodes X and Z cannot sense each other's transmission . Hence nodes X and Z are the hidden nodes.

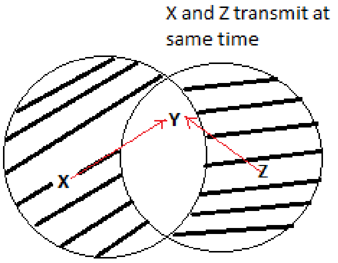

Figure 1. Hidden node scenario

In general, three circumstances can make a node behave as a hidden node. Firstly, scenario in which all nodes behave as hidden nodes and this leads to least throughput. Secondly, in this scenario best throughput is achieved as all nodes are visible and compete with each other for resources. Finally, in this both the nodes hidden as well as the competing nodes come into sight together [3].[7]

Hidden node problem in network degrades the performance, minimize the throughput, delays the transmission and effects many more network factors [4]. Packet loss is one of its worst effects.

We check into thoroughly the hidden node scenario and define the mechanisms of different pure contention-based protocols starting from 1990 to the latest 2012. Section 2 describes the mechanisms of different protocols. Finally, Section 3 concludes the paper.

II. PURE CONTENTION-BASED PROTOCOLS

Contention-based protocols are the protocols that find the solution to a collision after it has occurred. Collision resolution protocol is executed by these protocols after the collision takes place. [5]

Merits [1]

- Requires basic hardware along with single transreciever.
- If basic frames of RTS and CTS are used, these are compatible with IEEE 802.11.

Demerits [1]

 ISSN: 2321-8169
6317 - 6322

- Immense signaling overhead.
- Reserving a channel is slow process.
- Not appropriate for real-time networks.

2.1 Sender-initiated protocols

2.1.1. Multiple Access with Collision (1990)

Multiple Access with Collision Avoidance (MACA) [6] is a protocol in which two fixed –size RTS (Request-to- send) and CTS (Clear-to-send) signal frames are used to mitigate the problem of hidden node. Sender node initiates

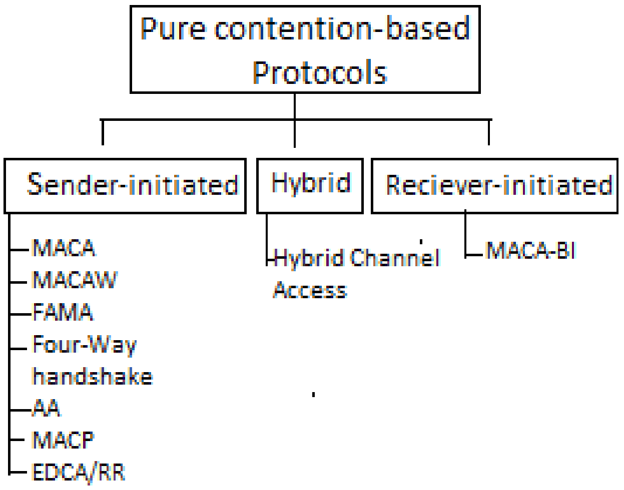

Fig. 2. Pure contention-based protocols

the transmission by sending the RTS frame to the receiver node and during that time interval if the nodes in the sender's neighborhood sense the RTS, then they must delay their transmission. The CTS frame is sent by the receiver node as a reply to the frame sent by the sender node. Similarly, if the nodes in the receiver's neighborhood sense the CTS, then they must delay their transmission. Also, the CTS contains the time interval for which the channel will remain busy, to notify other nodes in the neighborhood. After the transmission is over, the receiver node must return an Acknowledgement (ACK) frame as to assure that the sent data was accepted. However, if collision takes place between the two RTS packets, then the sender node must delay its transmission until the *Backoff* interval chosen randomly. Figure 3. depicts the above scenario.

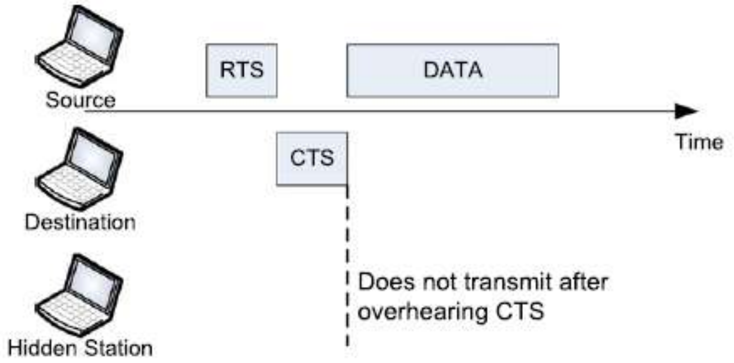

Figure 3. MACA [1]

2.1.2. MACA for Wireless (1994)

MACAW [8] in addition to RTS/CTS packets uses the DS (Data Sending) packet, which notifies the other suspended nodes about the effective RTS/CTS exchange and the consecutive DATA frame length.

Another frame RRTS (Request for RTS) is sent when an RTS packet is received by the node suspending its transmission. RRTS frame is sent to the RTS sender which instantly answers back by sending RTS packet. However, all other nodes sensing RRTS packet must delay their transmission for large interval of time so as to sense the successful RTS/CTS exchange [1]. Figure 4 depicts the above scenario.

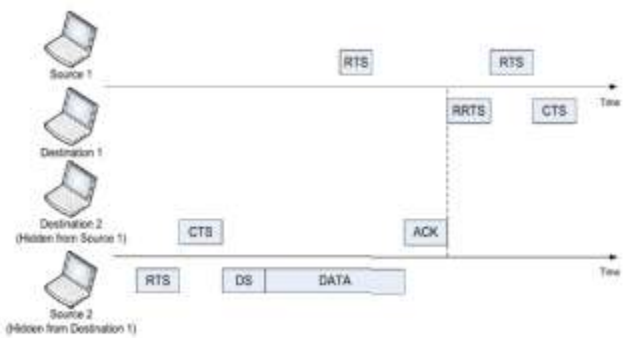

Fig 4. MACAW scenario [1]

2.1.3. Floor Acquisition Multiple Access (1997)

FAMA is furthur divided into two protocols that require the sender to acquire the access of the floor (medium). FAMA with Non-persistent Carrier Sensing (FAMA-NCS) and FAMA for Non-persistent Packet Sensing (FAMA-NPS) [9].To acquire the medium control RTS is sent by the sender after it performs one of the mechanisms which include: packet sensing (MACA) or carrier sensing (CSMA).The receiver responds by sending the CTS packet with length long enough to avoid the hidden node transmission. Figure 5 depicts the FAMA protocol scenario.

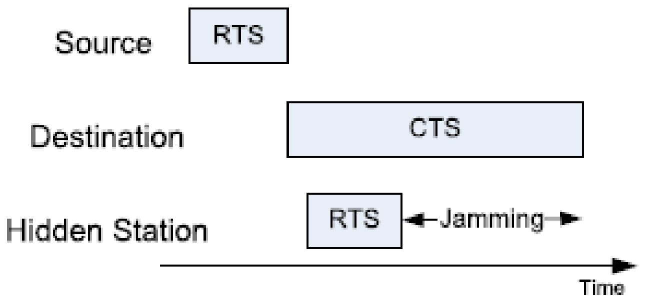

Fig 5. FAMA scenario [1]

2.1.4. Four-way handshake mechanism (1999)

For predefined time interval medium has to be sensed idle before a node needs to transmit data. If the medium is not idle, *Backoff* timer is set by the node and when this timer expires the four-way handshake procedure is initiated by the node. For the Distributed Coordination Function (DCF), nodes wait for the DCF Inter-Frame Space (DIFS) time interval and for the Enhanced Distributed Channel Access (EDCA, standardized in 2005) they wait for the Arbitration Inter Frame Space (AIFS) time interval [1]. RTS/CTS packets inform other nodes about the duration of the transmission. Consequently, nodes are allowed to set a counter that determines for a how long a node should suspend from acquiring the channel and this counter is known as NAV (Network Allocation Vectors). Figure 6 depicts the scenario [1].

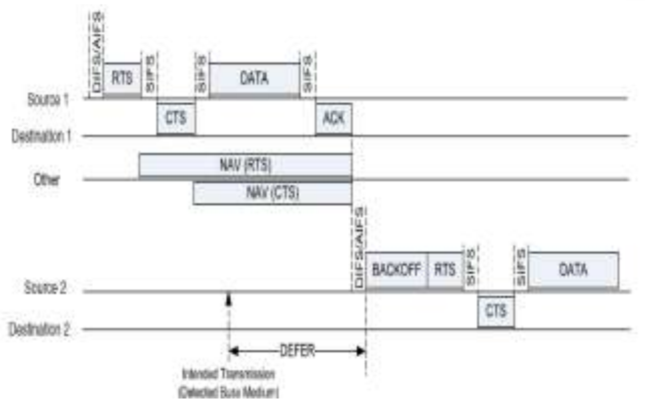

Fig 6. Four-Way Handshake Mechanism

2.1.5. Advance Access (2003)

Advance Access (AA) [10] contains RTS/CTS frames having special lag times that separate the DATA packet from its associated control packets. This protocol has a feature for allowing simultaneous transmissions. Figure 7 depicts this scenario.

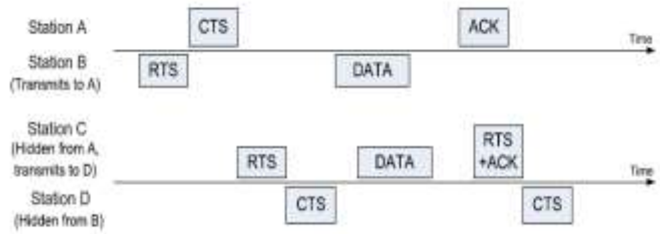

Fig 7. AA scenario [1]

2.1.6. Multiple Access Collision Prevention (2004)

In MACP [12] terminals compete with other terminals through DMBC (Distributed Multi-hop Binary Countdown) based on CSMA with Collision Prevention (CSMA/CP) using prohibiting signals [1-12]. Competition Numbers (CNs) are selected by the competing terminals in every round of DMBC. If the n-th bit of the terminal in the n-th time slot is equal to one, then the terminals can send buzz signal while in competition with other terminals. However, the transmission by the terminal is suspended if during sensing a buzz signal is heard. Terminal with the large value of CN wins the competition and after this the standard four-way handshake mechanism is used by MACP to transmit the DATA packets. MACP frame is divided in two slots the competition slots and second, the Detection slots. Detection slots are used to send a OTS (Object-to-Send) signal to stop hidden terminals from sending their control packets. Figure 8 depicts the MACP frame format.

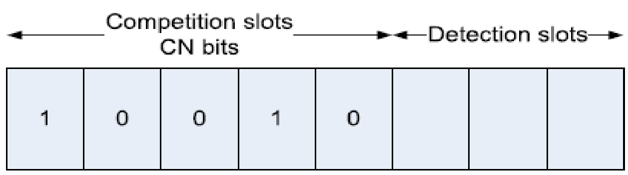

Fig 8. MACP frame format [1]

2.1.7. Enhanced Distributed Channel Access with Resource Reservation (2006)

In EDCA/RR [13], the method used for reservation is similar to the four-way handshake as to reserve the medium; it uses ADDTS (Add Traffic Stream) requests and ADDTS responses.

Traffic flow factors are described by TSPEC (Traffic Specification Field) and this field is the part of ADDTS requests. In this QOS provisioning is associated with awareness of hidden node [1]. Figure 9 presents the EDCA/RR scenario.

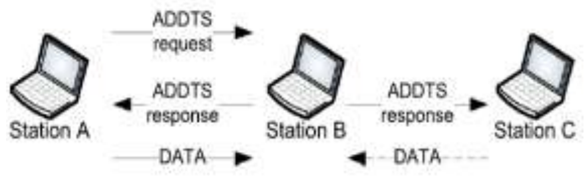

Fig 9. EDCA/RR scenario [1]

2.1.8. Adaptive QoS MAC Protocol (2009)

In AQMP, different priority classes can be assigned for different traffics, and nodes in the network can participate in channel contention adaptively, and nodes perform backoff mechanism adaptively. Analysis and simulation result show that compared with model MAC protocol, AQMP protocol provides better QoS support for higher priority traffics, solves hidden terminal problems, and also considers the fairness issues between different network nodes.[14]

In 2010 an advanced version of AQMP was proposed AMP (Adaptive QoS MAC Protocol). In AMP, the concept of transmission license is used, where only the node which holds transmission license can participate in the channel contention for changing the number of licenses according to the load of the network adaptively, controlling the number of the nodes that participate in the channel contention, and ensuring the nodes with licenses share the channels through contention. In addition, AMP assigns different priority classes for different traffic according to the special characteristics and performance types of the different networks,
and it sets the different contention parameters for the different priorities services for guaranteeing these services performances to have advantages in the channel contention. AMP not only can meet the QoS requirement with high priority in the networks but also can well solve the hidden terminal problems and the fairness issues between different network nodes; that is, it can satisfy the high efficiency, pertinence, spatial-reuse, etc. to the largest extent at the same time in limited channels. [15]

2.1.9. Fair QoS assured MAC Protocol (2011)

The fair QoS assured MAC protocol [16] is based on DCF. It differentiates three traffic classes. Every traffic class has a dissimilar set of CWmin and CWmax values. Frames are inserted in three different queues based on their types. Every node along the path from the source to the destination adds up the number of successful frame exchanges, independently for each flow. If two frames of the same priority but from different flows are inserted in a single queue the one which belongs to less served flow is deleted. Such a performance is obtained by altering CW values according to a scaling factor, which is the ratio of the number of successful frame transmissions for the current flow to the number of successful frame transmissions for any better served flow of the same priority. The projected mechanism can help hidden nodes to transfer the data because in the majority cases they will have poor ratio of successfully transferred frames in comparison to unhidden nodes. [1]

2.1.10. Solution to hidden node problem using Cloud (2012)

The design is that the cloud can accumulate the status of cognitive network, compute, reorganize, and make available the current state of cognitive networks for future decisions. Figure 11. illustrates that each node in the CRN is linked to cloud (CRNC). Each node in the CRN is linked to cloud and the nodes inform their status at cloud. The cloud software execute the condition of free channels in each node connected from sender node to the destination node and secure the free channels. The cloud software decides the channel in every connected node to transmit the packets. Further, if the primary user enters the network at any time, the cloud decides the alternating action of assigning the channel or stores the packets in its buffer till it finds the free channel to transmit the packets to the destination. The same provision will not be possible without cloud organization. For example, if the primary user enters (to use the channel) suddenly, the current data transfer on the channel used by secondary user must be stopped and wait for alternate channel. In CRNC, the free channels are available at each node in the cloud knowledgebase. The cloud software links the free channel to transmit the data without delay. Therefore, delay time is less in CRNC since it maintains the current channel states and does not require RTS/CTS.[17]

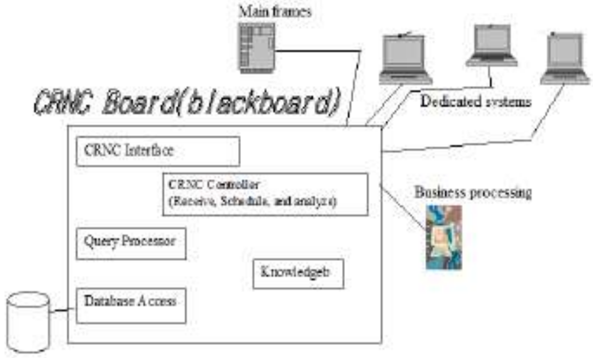

Fig 11. Architecture of CRNC [17]

2.2 Hybrid Protocols

2.2.1 Hybrid Channel Access Scheme (2004)

The hybrid channel access scheme for ad hoc networks [18] adjusts its channel access method and takes benefit of either sender-initiated (SI) or receiver-initiated (RI) handshakes (Figure 12). By default the SI mode is set and merely if the SI mode fails the RI mode is activated. The authors say that their scheme fits within the IEEE 802.11 standard, is easy and does not initiates any fresh control frames. The source/destination pair decides on the RI mode when the sender transfers the same RTS frame for more than half of the time allowed by the IEEE 802.11 standard. In most cases, if the destination is not capable to send a response to the RTS frame the conflict around it is very adverse. Consequently, according to the authors, it is better to let the sender change to the RI mode. In this mode the sender sets the RI flag in each frame it transfers to the destination. In this way it requests the destination node to alter to the RI mode. If the sender does not receive a CTS frame from the destination it can suppose that the destination node is down. But, if the CTS frame is received, the sender enters the RI linked mode and sets the RI flag in each DATA frame it sends to the destination node. The RI flag can be cleaned simply when the sender does not have any more data to send. After the overload conditions are minimized, the sender/destination pair returns to the SI mode. The two most important advantages of the described behavior are the reduced number of collisions and shorter queuing delays. [1], [18].

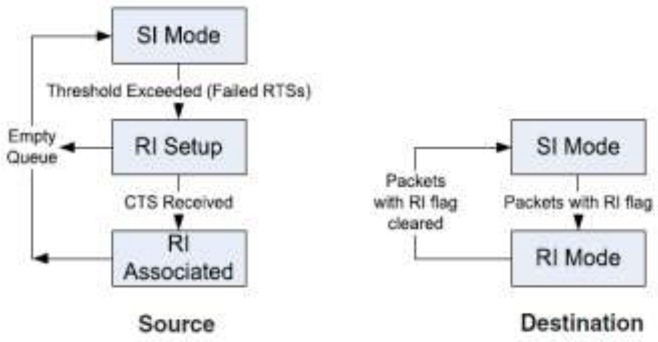

Fig 12. Status of Source and Destination [1]

2.3 Receiver-initiated Protocols

2.3.1. MACA by Invitation (1997)

(MACA-BI) MACA By Invitation [19] is an additional mechanism based on MACA. As an alternative to the RTS/CTS frames it uses a only Ready To Receive (RTR) frame, which contains the similar information as a CTS frame. It serves as a polling frame (Figure 13) and is sent by the destination node to the sender node. This allows informing possible hidden node in the transmission range of the RTR frame of the planned transmission. In MACA-BI a sender cannot transfer data before being polled, hence, the destination needs to have a integrated traffic prediction algorithm so as to know when to ask the sender for its data [20]. To attain this, the authors of MACA-BI propose piggy-backing the information concerning the frame queue length and data arrival rate in the sender's DATA frame. in addition, every time an RTR frame has not been received by the sender for a given time it can send an unambiguous RTS frame (in such a case the method changes into MACA). So, MACA-BI is appropriate for networks with expected traffic patterns as its performance decreases to MACA in case of periods of immobility, which are common for bursty traffic [20]. Moreover, the authors of MACA-BI pressure on the control frames may collide with each other and/or DATA frames and lead to protocol failures. Recovery from such a situation is possible only by using ACK frames, Yet, explicit acknowledgments are not implemented in MACA-BI.[1]

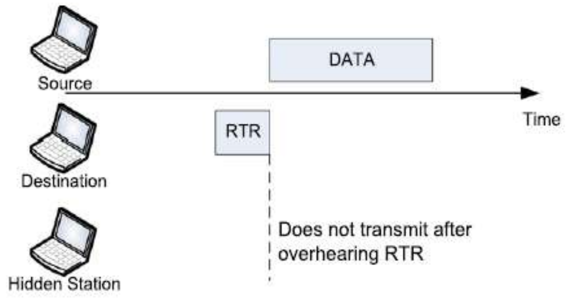

Fig 13. MACA-BI scenario [1]

III. CONCLUSION

In this paper we have described the mechanisms to mitigate the hidden node problem. We have differentiated these techniques in three categories namely: sender-initiated, receiver- initiated and hybrid protocols. Furthur, we have concluded that pure contention-based protocols use standard hardware along with single transreciever. Moreover, FAMA-NCS is more suitable than FAMA-NPS to minimize the hidden node effect.These protocols have large signaling overhead and reservation time is slow for these protocols. The researchers should focus there research on dynamic hidden node detection, as the nodes in the networks can move and cannot be easily detected as the hidden nodes change for mobile nodes.

REFERENCES

[1] Kosek-Szott, Katarzyna. "A survey of MAC layer solutions to the hidden node problem in ad-hoc networks." *Ad Hoc Networks* 10.3 (2012): 635-660.

[2] Tobagi, Fouad, and Leonard Kleinrock. "Packet switching in radio channels: Part II--The hidden terminal problem in carrier sense multiple-access and the busy-tone solution." *Communications, IEEE Transactions on* 23.12 (1975): 1417-1433.

[3] Ekici, Ozgur, and Abbas Yongacoglu. "Fairness and throughput performance of infrastructure IEEE 802.11

networks with hidden-nodes." *Physical Communication* 1.4 (2008): 255-265.

[4] Koubâa, Anis, et al. "H-NAMe: A hidden-node avoidance mechanism for wireless sensor networks." *8th IFAC International Conference on Fieldbuses and Networks in Industrial and Embedded Systems*. 2009.

[5] http://www.ece.tamu.edu/~reddy/ee602_00/bettati1.pdf

[6] P. Karn, MACA – a new channel access method for packet radio, in:Proc. of the ARRL/CRRL Amateur Radio 9th Computer Networking Conference, vol. 9, 1990, pp. 134–140.

[7] Boroumand, L., et al. "A review of techniques to resolve the hidden node problem in wireless networks." *SmartCR* 2.2 (2012): 95-110.

[8] V. Bharghavan, A. Demers, S. Shenker, L. Zhang, MACAW: a media access protocol for wireless LANs, in: Proc. of the ACM Conference on Communications Architectures, Protocols and Applications, 1994, pp. 212–225.

[9] Fullmer, Chane L., and J. J. Garcia-Luna-Aceves. *Solutions to hidden terminal problems in wireless networks*. Vol. 27. No. 4. ACM, 1997.

[10] C.H. Yeh, The advance access mechanism for differentiated service,power control, and radio efficiency in ad hoc MAC protocols, in: Proc. of the 58th IEEE Vehicular Technology Conference – IEEE VTC, vol. 3,2003,pp. 1652–1657.

[11] C.-H. Yeh, A new scheme for effective MAC-layer DiffServ supports in mobile ad hoc networks and multihop wireless LANs, in: Proc. of the IEEE Vehicular Technology Conference, 2004, pp. 2149–2155.

[12] You, Tiantong, Chi-Hsiang Yeh, and Hossam Hassanein. "A new class of collision prevention MAC protocols for wireless ad hoc networks."*Communications, 2003. ICC'03. IEEE International Conference on*. Vol. 2. IEEE, 2003.

[13] D. Level, Deliverable reference number: D-IA-8.3-7 Deliverable Title:Proceedings of the Third Workshop on Wireless and Mobility.

[14] Geng, Rong, Zhe Li, and Lei Song. "AQMP: an adaptive QoS MAC protocol based on IEEE802. 11 in ad hoc networks." *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*. IEEE, 2009.

[15] Geng, Rong, Lei Guo, and Xingwei Wang. "A new adaptive MAC protocol with QoS support based on IEEE 802.11 in ad hoc networks." *Computers & Electrical Engineering* 38.3 (2012): 582-590.

[16] Seth, D., Srikanta Patnaik, and Srikanta Pal. "A Faired Quality of service assured MAC protocol for mobile ADHOC network and its performance evaluation." *International Journal of Wireless and Mobile Networks* 3.2 (2011).

[17] Reddy, Y. B. "Solving Hidden Terminal Problem in Cognitive Networks Using Cloud Application." (2012): 19-24.

[18] Y. Wang, J.J. Garcia-Luna-Aceves, A new hybrid channel access scheme for ad hoc networks, ACM Wireless Networks Journal, Special Issue on Ad Hoc Networking 10 (4) (2004).

[19] Talucci, Fabrizio, Mario Gerla, and Luigi Fratta. "MACA-BI (MACA by invitation)-a receiver oriented access protocol for wireless multihop networks."*Personal, Indoor and Mobile Radio Communications, 1997. Waves of the Year 2000. PIMRC'97., The 8th IEEE International Symposium on*. Vol. 2. IEEE, 1997.