Vol. 1, Issue IV, May 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Reduce Delay in MACA Protocol by using Ant Colony Optimization and Bat Algorithm

Saniya Puri, Harwant Singh Arri

Lovely Professional University
Jalandhar, Punjab
saniya.saniya.puri@gmail.com, hsarri@gmail.com

Abstract: *The Ad hoc network is the self configuring type of network in which any node can leave or join the network when they want. Ad hoc network has many challenges like high packet loss, Packet collision, Hidden terminal problem and exposed terminal problem. Among the entire challenges hidden terminal problem is the most challenging problem to solve. The Hidden terminal problem is solved by the MACA protocol. The MACA protocol has many disadvantages like RTS, CTS packet collision, Delay which leads to high battery consumption and waste of network resources. In this paper, we proposed a new technique which is based on ant colony optimization and bat algorithm with the use of both the algorithms we can able to reduce the delay in MACA protocols. The simulation results show that proposed approach is much efficient than the existing one in terms of delay.*

Keywords: *MACA, Delay, Self configuring, Ant colony, Bat algorithms.*

1. INTRODUCTION

Mobile Ad-hoc Networks are future wireless networks consisting entirely of mobile nodes that communicate on-the-move without base stations. Nodes in these networks will both generate user and application traffic and carry out network control and routing protocols. Rapidly changing connectivity, network partitions, higher error rates, collision interference, and bandwidth and power constraints together pose new problems in network control particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements [1]. The routers are free to move randomly and organize themselves arbitrarily thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Sensor nodes consist of sensing, data processing, and communication components and typically form ad hoc networks.

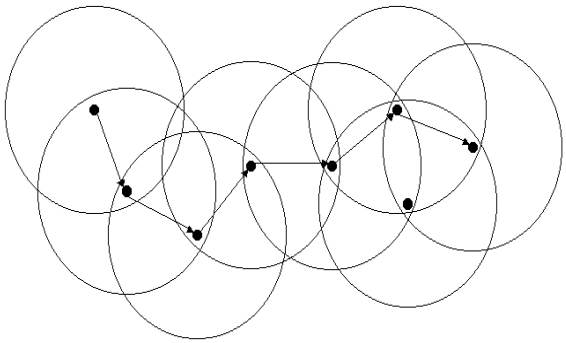

Figure1: Ad hoc networks

As shown in the figure 1 the independent mobile nodes can form the network on fly and communicate with each other without the use of any central controller. In such network the mobile nodes can start communicating with the proper channel sensing which leads to packet collision and network throughput can be reduced. To reduce packet loss and enhance the network throughput many protocol have been proposed like ALOHA, Slotted ALOHA, MACA etc.

Vol. 1, Issue IV, May 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

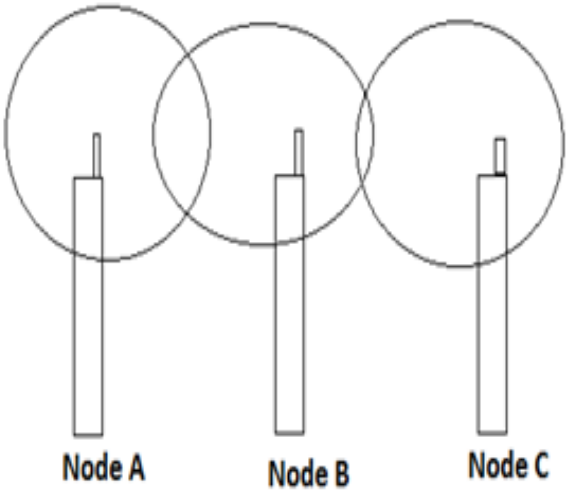

Figure 2: Hidden terminal Problem

As shown in the figure 2, Node A and Node B are in the range of each other .Node B and Node C are also in the range of each other. But Node A and Node C are not in the range of each other. Node A when wants to transmit data to Node B ,it sense the channel and channel is free at that time .At the same time Node C sense the channel to transmit the data to Node B. When Node C senses the channel, it is also free because both nodes are not in the range of each other. The Node A and Node B when simultaneously transmit data to node B; data will collide at Node B.MACA Protocol will solve this Problem.

The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not.

Passive attacks: A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overheard.

Active attacks: An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication. Both passive and active attacks can be made on any layer of the network protocol stack. This section however, focuses on network layer attacks only. Depending upon the various attacking behavior routing attacks can be classified into five categories: attacks using information disclosure, impersonation, modification, fabrication, and replay of packets.

In this paper, we will discuss Literature review in section 2.NAV attack will be discussed in section 3 Future and conclusion is written in section 4.

2. LITERATURE REVIEW

K. Sugantha et al proposed a static approach to detect NAV attack. NAV attack can be performed on the MAC protocol .Simulation results shows that proposed technique will be simple to detect NAV attack [2].

Zhong Zhou et al discussed about the hidden terminal problem .when the network is large ,then triple hidden terminal problem can also be raised. In this paper, they provide a solution for the hidden terminal problem which is raised in the underwater sensor network. They proposed a new technique called CUMAC to solve hidden terminal problem [3].

Sunil Kumar et al provide the comparative study of various MAC protocols like ALOHA, Un-slotted ALOHA, Slotted ALOHA, MACA and MACAW. In this paper they discuss that hidden terminal and exposed terminal problems were raised. To solve these problems and to increase the network throughput we use MAC protocols [4].

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Chane L. Fullmer et al proposed a new technique FAMA. In this technique a control is assigned to the single station, and this station will responsible for channel sensing and collision avoidance. Stimulation results show that FAMA is better than ALOHA and CSMA [5].

Lin Chen et al discussed the DCF protocol of wireless ad-hoc network. In ad-hoc network various selfish nodes exits which are responsible for various internal and external attacks. In this paper, they proposed a new technique for the detection of selfish nodes in the ad-hoc network .They had made certain changes in the DCF protocol and increase the back-off timer value to detect selfish nodes [6].

Sumit Khurana et al discussed about the hidden terminal and exposed terminal problems and there effects on the network performance. The simulation results shows that the throughput of network will degrade when hidden terminal problem will exits in the network [7].

Y.N SINGH discussed the solution to overcome of this problem the researcher will uses the RTS (REQUEST TO SEND) and CTS (CLEAR TO SEND).In this case when node1 will transmit the data to node 2 it will send RTS to NODE2 and node2 will send CTS to both 1 node and 3 node .so that it will be clear to the 3 node that at this particular time there is a communication going on in between node 1 and node 2.so that it will be in ideal state and hence it solve out the problem[8].

3. DELAY IN MACA PROTOCOL

In MACA protocol much delay is there to access the services which are the most common challenge to solve it will also leads to waste of network resources and battery of the mobile nodes. As Shown in the figure 3 there is a network with three mobile nodes. Node 1 wants to communicate with node 2 it send RTS packet to node 2 and node if free broadcast the CTS packet and all the mobile node which are in the network will get blocked for the certain period of time. After waiting for the certain period of time Node 3 and Node 5 again send an RTS packet to node 2. Node 2 will receive RTS packet from Node 5 first. Node 2 will gave channel access to Node 5 and Node 3 again goes to waiting state.

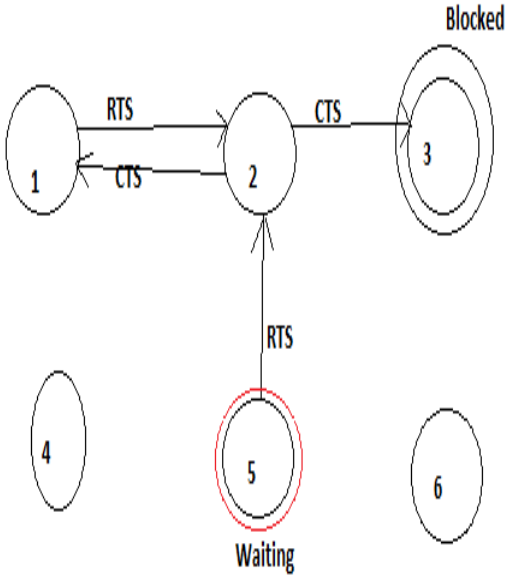

Figure 3: Problem of Delay in MACA

4. NEW PROPOSED TECHNIQUE

The proposed technique will be based on the ant colony optimization and Bat algorithm. When the hidden terminal problem will exist in the network, the source node will send RST packet to the destination nodes and destination node will broadcast the CTS packet to its corresponding nodes. When any other corresponding node wants to communicate with the destination it kept on sensing the destination node. In the large network, the correspondent node will make a path to destination node using ant colony algorithm to sense the destination whether it is free or not. When the destination node is free correspondent node will start communication with the destination node using BAT algorithm. The BAT algorithm is used to reduce packet collision in the network. The proposed technique is implemented in NS2 and in figure 4 simulations is shown. In figure 5 and 6 simulation results are shown in the form of graphs.

5. CONCLUSION

In this paper, we conclude that the hidden terminal problem will reduce the network throughput and it is solved by using MACA protocol .In MACA protocol many problems may exits one such problem is delay.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

To solve this problem new technique has been proposed which is based on ant colony optimization and BAT algorithm. The simulation results shown proposed technique is much efficient than the previous techniques.

REFERENCES

[1] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[2] K.Sugantha, S.Shanmugavel. A Statistical Approach to detect NAV Attack at MAC layer.

[3] Zhong Zhou, Zheng Pengt, Jun-Hong Cui, and Zaihan Jiang. Handling Triple Hidden Terminal Problems for Multi-Channel MAC in Long-Delay Underwater Sensor Networks.

[4] Sunil Kumar, Vineet S. Raghavan, Jing Deng. Medium Access Control protocols for ad hoc wireless networks: a survey.

[5] Chane L. Fullmer and J.J. Garcia-Luna-Aceves. Solutions to Hidden T erminal Problems in Wireless Networks.

[6] Lin Chen, Khaled Aslan Almoubayed, Jean Leneutre. Detection and Prevention of Greedy Behavior in Ad Hoc Networks.

[7] Sumit Khurana, Anurag Kahol, Anura P. Jayasumana. Effect of Hidden Terminals on the Performance of IEEE 802.11 MAC Protocol.

[8] Rajeev K. Shakya, Satyam Agarwal, Y. N. Singh, Nishchal K. Verma, and Amitabha Roy. DSAT-MAC: Dynamic Slot Allocation based TDMA MAC protocol for Cognitive Radio Networks.

[9] Sachin Dev Kanawat Department of Computer Engineering, Institute of Technology & Management,Rajasthan, India, e-mail:sachinkanawat@gmail.com "Attacks in wireless network"