ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

A New Proposed Technique to Prevent NAV attack in MACA Protocol

Vivek Pathak
Lovely professional University

Ambrish Gangal
Lovely professional University

Abstract: **The performance of Ad-hoc network is calculated by the number of packets successfully delivered to the destination. In multi-hop wireless networks, every node acts as middle node to forward packets to other nodes. To increase the overall network performance, number of packets delivered to the destination successfully must be increased. In the congested network the coordination between the active nodes must be maintained to increase network performance .In this paper, we discuss medium access protocol, MACA .The Hidden terminal problem and exposed terminal problem had been solved by using MACA. In this paper we review MACA and highlight the NAV attack which is possible in this protocol .We also propose the new technique for the prevention of NAV attack. When triggers the NAV attack in MACA protocol overall network performance degrades.**

Keywords: **Hidden, Terminal, MACA, Exposed, Ad-hoc, NAV, Attack**

I. 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.

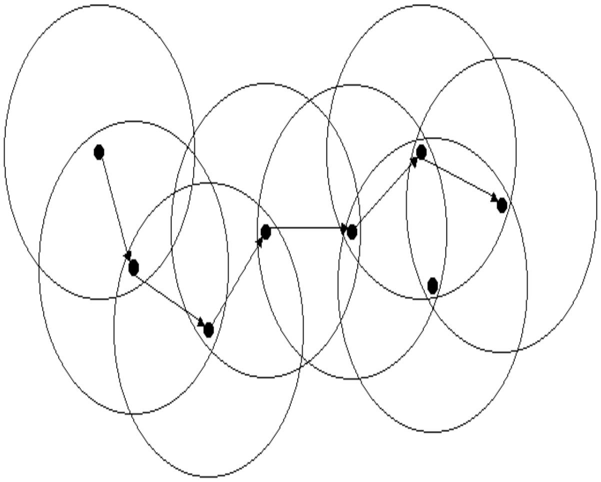

Fig1: Multi-hop Ad-hoc Network

As, Shown in the figure1 when source and destination nodes are not in the range of each other intermediate nodes are responsible for data forwarding. The nodes coordination must be maintained between the nodes to increase the network performance .When the mobile nodes are perfectly coordinated, before the data transmission it can sense the medium, if the transmission medium is free then only it can transmit the data. With the use of this approach packet collision will be reduced, many of the algorithms are proposed for medium access these protocols are like ALOHA, Slotted ALOHA, MACA etc .Among all the protocols MACA is the most efficient protocol .MACA can also solve the hidden and exposed terminal problems.

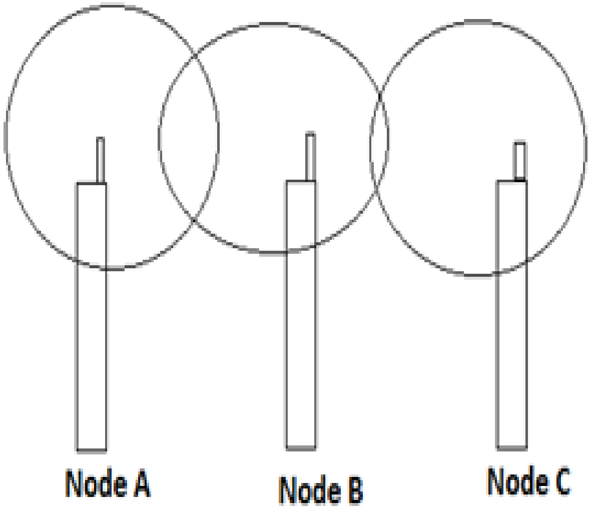

Fig2: Hidden Terminal Problem

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.

II. 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].

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].

III. NAV ATTACK

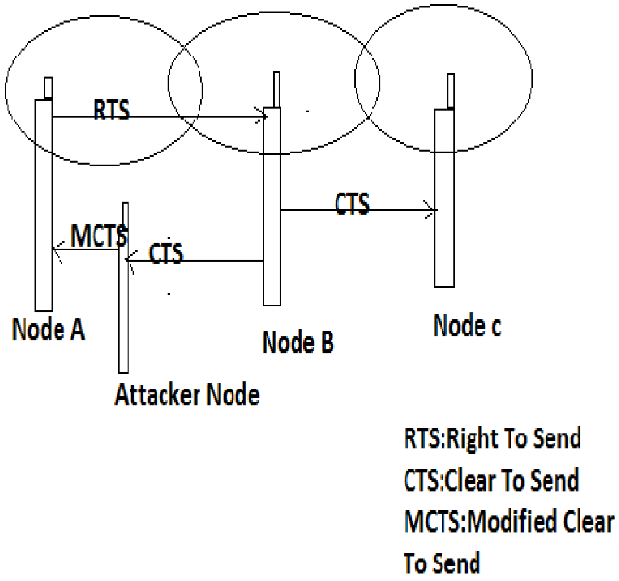

Fig3: NAV Attack

As shown in the figure 3, When Node 1 sends the RTS packet to Node B .Node B broadcast the CTS packet .In-between the Node B and Node A there is attacker node which sniff the CTS packet and modified the CTS .After modifying the CTS it reply the CTS packet. Attacker node can modified the NAV value in the CTS packet.NAV attack is the active type of attack and can greatly effects the network performance .Let us suppose the NAV value is 5 sec which is set by the Node B .The attack modified that value to 10 sec .After 5 sec Node B will free to receive the RTS packet, but the Node A will blocked for another 5 sec .The data packets and RTS collision will take place in this situations. This approach allows an attacker to transmit with extremely low power or using directional antennae, thereby reducing the probability of being located. The maximum time that the channel can be reserved for in a single frame is limited by the size of the duration field, a maximum of 32767 microseconds [2]. Assuming that the attacker sets maximum value, he has to transmit only 30 times per second, and therefore, easy for the attacker [2].

IV. PROPOSED TECHNIQUE

In our new proposed technique we work to prevent NAV attack in MACA protocol. The MACA protocol is the MAC protocol and it provides the solution to hidden and exposed terminal problems. When any node get the channel access, other nodes get blocked for the certain time period .The time period for which the nodes get blocked is NAV value .Attacker node modified this NAV value .To prevent NAV attack in the MAC protocol we propose to use the timer. After the fixed time the receiver node will send some packets to the sender node to check it NAV value. This technique will be implemented in the simulator NS-2 .The proposed technique will require modifications in the MACA protocol to prevent NAV attack.

V. FUTURE WORK AND CONCLUSION

In this paper ,we conclude that the hidden terminal and exposed problem will be solved by using RTS and CTS packets .The hidden terminal problem will greatly effects the network performance .In our work we also discuss about the NAV attack which is possible in the MACA protocol. In our future work, we will work to implement the proposed technique and also do the competitive study between tradition MACA protocol and our proposed technique protocol.

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, "Attacks in wireless network"