www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1286-1290

Achieving Energy Efficiency by the Enhancement Of Mac Protocol To Prevent Nav Attack

Pathak Vivek *, Gangal Ambrish
Lovely professional University,Jalandhar, Punjab
vivpathak7@gmail.com

Lovely professional University,Jalandhar, Punjab
ambrish.gangal@hotmail.com

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. There is an algorithm to detect the selfish nodes and also simulated their approach in NS-2 which shows the efficiency of the algorithm of solution [11]. The attacks exploit the local estimation and global aggregation of the metric to allow attackers to attract a large amount of traffic [10].*

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.

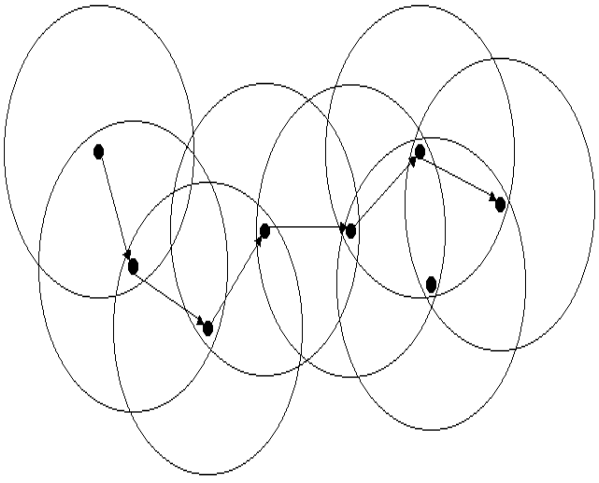

Figure 1: Multi-hop Ad-hoc Network

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.

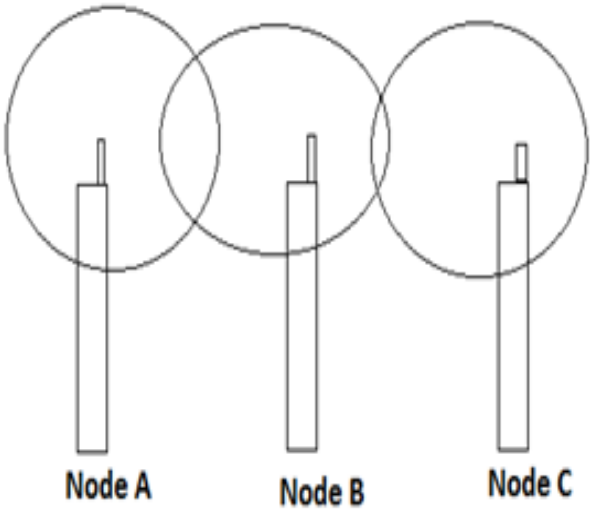

Figure 2: Hidden Terminal Problem

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.

II. 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.

III. OVERVIEW OF TECHNIQUES USED

In our technique we will use the timer to synchronize the NAV value from node A and node B.The sender will only send message when the both value of node A and node B will be same ,if synchronization is not at same time then the sender will immediately block that particular node.

IV. ALGORITHM USED

1. The network is inialized with the finite number of nodes
2. In the network it is assumed that hidden terminal problem exits
3. The hidden terminal problem is solved by MACA protocol

a. MACA is sender initiated protocol
b. Sender send RTS to receiver
IF (Receiver==free)
{
Receiver rely back with CTS packet and set the NAV value
}
Else
{
Sender will be blocked for the certain period of time
}

4. NAV attack is possible in MACA protocol

a. The attacker can change the NAV value and packet collision problem exits
b. To isolate NAV attack Modified MACA is proposed

1. The receiver set the NAV value and broadcast the NAV to corresponding nodes
2. The nodes which receives CTS packet it set its NAV value corresponding to reciver
3. To isolate NAV attack the receiver and sender checks its corresponding NAV values after certain period of time
If (NAV value of sender!=NAV value of receiver
{
NAV value is synchronized between sender and receiver
}
Else
{
Step 3 is repeated until communication finish
}

V. IMPLEMENTATION DETAILS

Implementation of the proposed system has different stages:

Stage 1: We had created a network of different nodes in which a hidden terminal problem exist.
Stage 2: A hidden terminal problem is solved by MACA protocol
Stage 3: Comunication between sender and reciver is established using RTS and CTS technique.
Stage 4 : To isolate NAV attack, Modified MACA is proposed as attacker can change the NAV value and packet collision problem exits.
Stage 5 : Final decision is based on comparison value of NAV value of sender and reciver as discussed in algorithm.

VI. PROCEDURE AND RESULT

An environment of three nodes is created in which all nodes wants to communicate with each other, but when node A send the data with NAV value 10 and it will send to B ,but B node is unable to identify NAV value and in between the communication the attacker will modify the NAV value. Suppose it set the value 5 sec ,when it will send to the node B then synchronization will not work at same time because NAV value of node A is 10 and modify value is 5 Sec.so the packet will loss and immediately node C will be unblocked and collision occur. Starting time for all the node is 10 sec but due to the modify of the message collision occur.

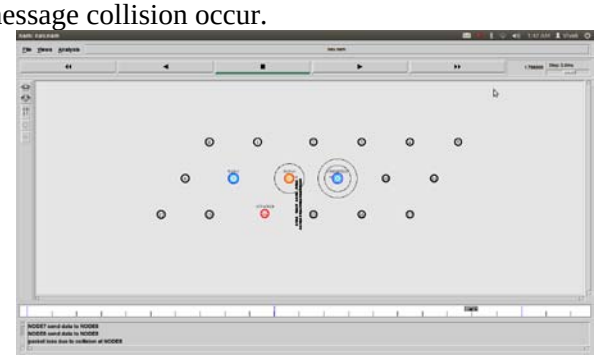

Figure 3: Environment of different node

W are using TIMER IN technique in which node A will transmit the message with NAV 10 than node B will first synchronize and check the NAV value, whether the value is same or not . if not than it will not respond. When node B send hello packet to node A (that is the node is ready to recive) the transmission begins.

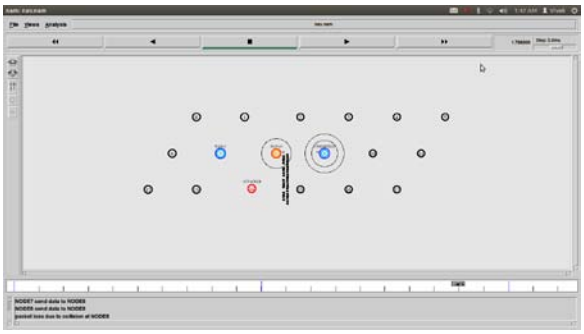

Figure 4: Communication between Node A and Node B

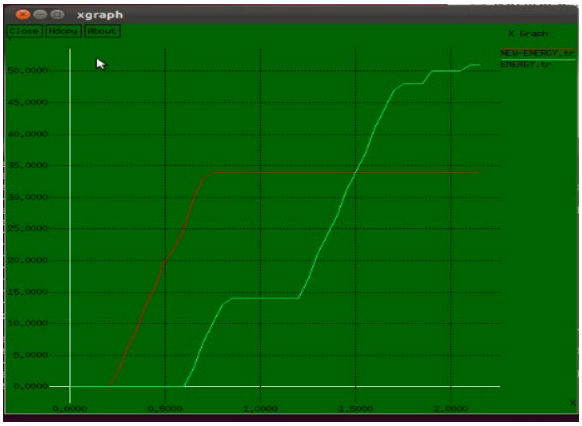

Figure 5: Energy comparison graph

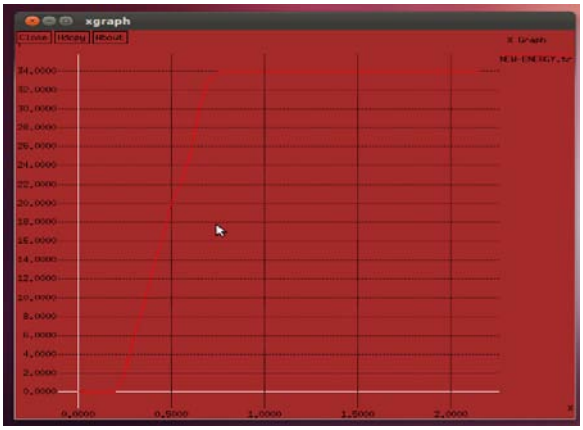

Figure 6: New energy efficiency graph

Figure 5 and 6 depicts the comparison made between two different situation made on the basis of packets delivered from source towards the destination. We examined that highest energy efficiency is achieved when we apply the new technique.Energy efficiency is more in that particular case with no packet loss and when there is no use of the timer the energy will dissipates and more number of packet losses and life of the node will reduces with the number of packet loss in the network. More the number of packet losses larger the energy reduces in the network.

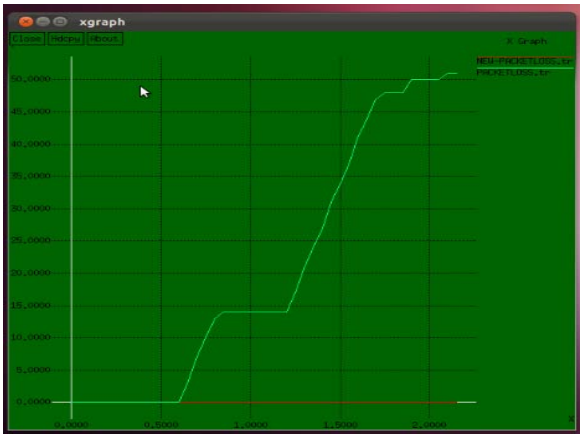

Figure 7: Comparison graph of packet loss in the network

Figure 7 shows the comparison between new throughput and maximum packet loss when we not apply the new technique in the simulation process. With previous technique we have noticed that average throughput is less and with current scenario throughput graph shows constant results.

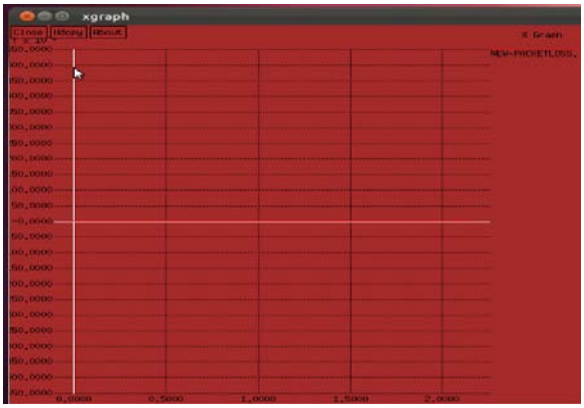

Figure 8: zero packet loss graph

Figure 8 shows zero packet loss while processing the packets that was delivered towards source from the destination. Hence with the throughput comparison graph it shows higher in the scenario where new proposed technique is provided as that of the scenario where timer is not used.

. VII. FUTURE WORK AND CONCLUSION

In this paper ,we this has been found 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, e-mail:sachinkanawat@gmail.com "Attacks in wireless network".

[10] Jing Dong , Curtmola, R. ; Nita-Rotaru, C. , " Secure High-Throughput Multicast Routing in Wireless Mesh Networks', Mobile Computing, IEEE Transactions on, Volume 10, Issue 5, page:653-668, May 2011.

[11] Sankareswary P., Suganthi R., Sumathi G., "Impact of selfish nodes in multicast Ad hoc on demand Distance Vector Protocol", in the proceedings of International Conference on Wireless Communication and Sensor Computing, ICWCSC 2010, pp-1-6, 2010.