International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Identification of Hidden Exposed Nodes and Solving Hidden Exposed Problem Using MAC Protocols in AD-HOC Networks

Ch. Srilatha[1], T. Mohana Kumari[2]

[1]Assistant Professor, Dept. of Computer Science, Dr. Lankapalli Bullayya College, Visakhapatnam, India

[2]Assistant Professor, Dept. of Computer Science, Dr. Lankapalli Bullayya College, Visakhapatnam, India

Abstract: ***The term wireless Ad Hoc network is used for the type of network that is established between communicating nodes for the specified period of time. After sometime, the nodes involve in the network move to the other location. This happens due to the wireless ad hoc network is made up of multiple mobile nodes. However, each time user changes location, the device of the user become hidden for the other nodes involved in the network to which the user's node was connected. This sometimes becomes large problem named collision. This study provides the information related to hidden node problem and it also enlists some of the mechanism to avoid the hidden node problem. Moreover, if the hidden node problem occurred in network, even if after applying these mechanism some of the solutions to be applied to solve this problem. This study discussed about some of the protocols called MAC protocols to solve Hidden problems in wireless networks.***

Keywords: Hidden Node Problem, Avoidance of Hidden Node Problem, MAC protocols

1. Introduction

A mobile Ad Hoc network (MANET) is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. MANET is a temporary based wireless network which does not rely on the infrastructure, that is it a decentralized kind of network. This helps people to get connected with any nearby device even if they change their location very often, regardless of their underlying architecture and location.

Mainly there are two parties involved in Mobile ad hoc network such as, communicating nodes and access points. The communication nodes are the end points in the network that are connected to the other nodes in the network. An access point in the network is a hardware device that allows nodes in a network to get connected to other nodes in network. The communication between the nodes in the network can be shared by access point [1].

1.1 Hidden Problem

A hidden node in a network is a device that is visible to the access point but not visible to other nodes attached to the access point. If multiple devices try to send data to the access point at the same time, collision will occur at access point as other nodes are hidden from each node in the network. Hidden node problem can be observed in widespread WLAN setups with many nodes that use directional antennas and have high uploads. Suppose that in a network of three nodes, in figure 1, Node A, Node B,and Access points, if two nodes send data to the access point, may results in collision. This is so because, node A and node B is directly connected to access point but does not visible to each other.

1.2 Hidden Node Model

The relationship between the hidden node area and the distance between two nodes in communication can be derived mathematically. To do this, we first define the following two parameters.

1) Carrier Sensing Range is the range within which a transmitter can detect whether or not another node is transmitting on the medium. We assume is always greater than the maximum transmission range.
2) **Interference Range Threshold** is the distance at which the interference from or more interfering nodes can create packet loss at the receiving node. The parameter is used to describe the multiple layers that comprise the hidden node area. We can determine the expression for by analyzing the distance between the sender and receiver is , the received power of the signal from the sender at the receiver is , and the interference from an interfering node located at a distance of from the receiver

2. Mechanism to Avoid Hidden Node Problem

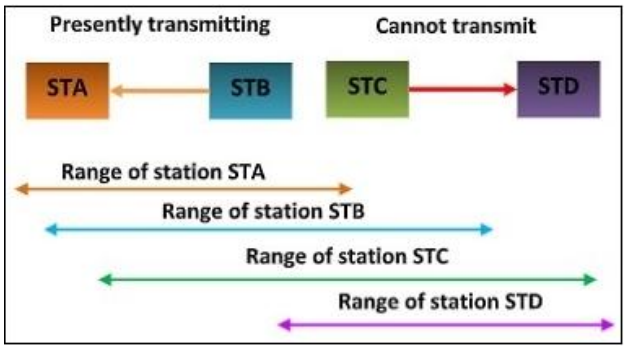
Hidden node problem basically occurs more likely in wireless networks as most of the wireless networks are based on the topology and range of the nodes. If multiple nodes in wireless network tries to send data to the common receiving node then, collision at receiving node. This cause the corruption of data of both sending nodes. So to avoid such problem, there should be a mechanism to be used so that nodes before sending data to any node must check whether the receiving device is free to receive its data or is busy in communicating with other nodes in the network. In this section, we summarize some available mechanism to the problem of hidden node.

2.1 Handshaking Procedure

RTS/CTS method
To avoid collision at receiving end all the neighboring nodes needs to inform that channel will be occupied. This can be achieved by reserving the channel using control messages, which is handshaking protocol. Data collision caused by hidden node problem A message termed as RTS (Request To Send) is send by sender to receiver, which indicates the request of the sender about asking that if receiver is ready to receive or not. A message termed as CTS (Clear To Send) is send by receiver to send only when it is ready to receive. Moreover, wireless network is a broadcast network, when RTS/ CTS messages are broadcast in network, all the neighboring nodes of sender and receiver will be informed that medium is busy. Thus, preventing them from transmitting and it results in avoidance of collision.

3. Exposed Node Problem

Suppose that there are four stations labeled STA, STB, STC, and STD, where STB and STC are transmitters while STA and STD are receivers at some slot of time. The stations are in a configuration such that the two receivers STA and STD are out of radio range of each other, but the two transmitters STB and STC are in radio range of each other. The above diagram shows that a transmission is going on from STB to STA. STC falsely concludes that the above transmission will cause interference and so stops its transmission attempts to STD. However, the interference would not have occurred since the transmission from STC to STD is out of range of STB. This prevention of transmission is called exposed terminal problem.



3.1 Multiple Access Collision Avoidance (MACA)

Multiple Access Collision Avoidance (MACA) is used to avoid collision occur by the hidden node terminal. In MACA the sending device make an announcement before it start sending data to the intended receiver, so that other nodes in network keep salient at the time of data transmission. When sending device sends RTS to receiving device, the receiving device if ready to receive it sends CTS plus the maximum length of data it is ready to receive. A node that hears RTS keep salient for avoiding conflict with CTS and vice versa.

3.2 Busy Tone Mechanism

Busy Tone Mechanism allows the parties involved in transmission of data, i.e. sender and receiver to send a control message named Busy Tone to their neighbor. This improves efficiency by providing allowance to the sender and receiver to reserve the link for the transmission. Moreover, some of the mechanisms like FPDBT (Fixed Power Dual Busy Tone), VPDBT (Variable Power Dual Busy Tone) etc. work on the power that should be used to transmit the control message.

3.3 DUAL Busy Tone Multiple Access

The dual busy tone multiple access (DBTMA) scheme. The operation of the DBTMA protocol is based on the RTS packet and two narrow-bandwidth, out-of-band busy tones. With the use of the RTS packet and the receive busy tone, which is set up by the receiver, our scheme completely solves the hidden- and the exposed-terminal problems. The busy tone, which is set up by the transmitter, provides protection for the RTS packets, increasing the probability of successful RTS reception and, consequently, increasing the throughput. This paper outlines the operation rules of the DBTMA scheme and analyzes its performance

3.4 Solution to avoid hidden node problem

Use of Omni Directional Antennas The nodes involved in the network can use both directional and Omni directional antennas to sense the other nodes in the network. The nodes that uses directional antennas can only sense the nodes includes in the direction follows by the directional antenna, all other nodes involved in the network are hidden nodes. However, this causes the hidden node problem to greater extent. So the better solution to this problem is that each node must use Omni directional antennas to sense all nodes involved in the all direction in the network. This solves hidden node problem as if all the nodes can sense the other nodes in network can wait for their turn if the communication channel is held by some node in the network.

3.5 Moving the Nodes

The alternative method for solving hidden node problem is the movement of the nodes so that each node detect other nodes involved in the network. If it is found that the movement of node occurs the hidden node problem then, it is compulsory for the moved node to move to the same direction back to become non hidden node again. The other way of forcing node to move is to extend the wireless LAN to add proper coverage of the hidden nodes. This may be done by increasing access points, or increasing the sensing power of the nodes involved in the network.

4. Results and Discussion

Each node is sensed by the access point, but may or may not through the other nodes in the network. If multiple hidden nodes send data to the access point at the same time then collision occurs. So, it is necessary to avoid the hidden node problem. In this study, we found the methods to avoid

hidden node problem occurring in the network. Moreover, if by chance the hidden node problem occurred even if the avoidance mechanism applied, then it is required to solve this problem. In this paper, we studied some of the solution can be applied to solve the hidden node problem. The future aspect of this study is the mechanisms involved in detecting the hidden node problem by simulating the behavior of the network.

5. Conclusion and Scope

The wireless ad hoc network is the infrastructure less network that changes their location and gets connected with other nodes in the network on the fly. In this type of network the number of nodes involved in the network is very large. The nodes in the network shared data with help of the node termed as access point. Each time, the node wants to send data to any other node, it will first send that data to access point, then that access point sends data to other receiving node.

References

[1] L. Boroumand, R.H. Khokhar, et.al.,"A Review of Techniques to Resolve the Hidden Node Problem in Wireless Networks", Smart Computing Review, 2(2),2012, 95-110.
[2] Koubaa, A. and Severino, R., et.al. (2009) 'H-NAMe: A Hidden-Node Avoidance Mechanism for Wireless Sensor Networks', Science Direct, 42(3),pp. 10–19.
[3] Kapadia, Viral V, Sudarshan N Patel, et.al. (2010)."Comparative Study of Hidden Node Problem and Solution Using Different Techniques and Protocols." Journal of Computing 2(3): 65–67.
[4] Ko Shibata, Munehiro Takimoto et. Al. , "Expading the Control Scope of Coorperative Multiple Robots", Advances in Intelligent Systems and Computing, 296(2014)17