International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 2, May 2014, PP 138-142

A Survey on IP Conflicts in MANETS

Rameswara Reddy.K.V[1], Dr. R. Praveen Sam [2], K.Istaq Ahmad [3]
Computer Science and Engineering Department,
G.Pulla Reddy Engineering College,
Kurnool, Andhra Pradesh, India.

Abstract: *Mobile Adhoc Networks are independent and self organized networks and it does not have any infrastructure and frequently changing their topology. The nodes acts as router and communicate with each other. Much effort has been put into the improvement of routing protocols for route discovery and preservation for the nodes in a MANET to communicate. The researchers in the routing area assume that all the nodes in the network are already configured to have unique IP address in the network. Dynamic Address Allocation (DAAD) and Management is a very critical problem in MANETs. There is no centralized supervision and superior authority to guide the address allocation among the nodes, The IP address auto configuration is to be done by the individual nodes themselves. Research has been going on to avoid the address conflicts in MANETs using less complex methods that reduces communication overhead and best latency. In this paper we present a study of detection of Duplicate Address Conflicts that arise in an ad hoc network.*

Index Terms: *MANET , Dynamic Address Allocation , Routing*

1. Introduction

A mobile ad hoc network (manet) [1] is formed by the wireless transmitting devices that communicate with each other through wireless channel and without the aid of any fixed or standard infrastructure. the nodes in an adhoc network themselves acts as routers and cooperate among themselves to achieve communication between any two nodes of the network. the total network consists of simple nodes and the network does not need any centralized administration to guide them how to communicate. The ad hoc networks are used in some important and typical applications such as Military Field Activities, catastrophe Situations, Local and Educational Requirements, Wireless Sensor Networks etc.

Routing is a most important part of ad hoc communication. The communication between the nodes is done through a single path established and the establishment of the path is called Routing. Most of the researchers concentrated on routing protocols and of course is a major issue to be solved earlier. But the researchers in the routing area take into assumption that the nodes in the network can be uniquely identified using their IP Addresses. This means that the nodes in the network are assigned with a unique IP address each.

Hence most functionalities of the network are completely dependent on the IP addresses of the nodes. It is very much important to see if there are any two nodes in the network with the same IP address. Any nodes in the network with duplicate addresses may cause mal functioning of the network.

In a network, there arise two cases where a duplicate address is possible. Initially it is assumed that the network is initialized with n number of nodes and each node is assigned with a unique IP. Then duplicate addresses arise because of *Node.*

Initialization: when in a network, a new node is initialized; it is to be detected if its self generated IP address matches with any other node in the network and in case, is to be assigned with new available IP, done by the nodes in the network itself.

Node mobility: when a node in a network or a partition of the network moves from its home network to a new network, it is to be monitored if its present IP address matches with that of any other node in the network. If the address already exists, the new node is to be assigned with the different and available IP.

Duplicate Address Detection (DAD) is the methodology introduced for monitoring the repetition of IP addresses by the individual nodes itself. This paper presents the importance of detection of IP address conflicts and different schemes introduced till date for detection.

The rest of the paper is organized as follows: Section II gives the related issues of the duplication of IPs, Section III briefs classification of DAD schemes. Section IV tells about existing methodologies and Section V presents a theoretical comparison of the existing methodologies and Section VI concludes the paper giving the scope for the researchers to concentrate in future.

2. Related Issues

Unavailability of the centralized administration, a MANET requires a unique identifier for each host for reliable communication. Due to mobility, when a new node comes to join the network, it is necessary to see if there is already a node in the network with its IP.

In order to send or receive packets between two nodes, they should possess unique addresses in the network. IP address auto-configuration schemes have to be improved to remove the overhead of manual configuration. Node mobility can cause network partitions. In such partitioned networks, the nodes possess unique addresses independent of the other partitioned networks.

Duplicate addresses may occur in a network because of mobility of the nodes. The nodes under different networks or sub networks may have same IP addresses. This will not affect the functionality of the networks. When a node from one network moves to another network, address conflicts may occur. Here two cases arise.

Case 1: when only one node moves from one network to another network. Here the mobile node breaks up its links with the older network and will be in contact with the new network only.

Case 2: when a group of nodes move from one network to another network. Here the nodes in the group are interconnected but they break up links with the older network.

Case 3: when an entire network move to merge into another network. This case is often referred to as network merging. Care should be taken while designing a protocol for IP allocation and Duplicate IP detection for each case. The node resources and network resources are to be concentrated while developing a mechanism. For case 1, methods like simple broadcasting of IP and waiting for reply can be applied. But the same method results more overhead for case 2 and even more for case 3. For case 2, it could be suggested for the methods such as linear IP allocation. For case 3, the broadcasting may not yield better results. Mechanisms such as allocating new network id for the merged network may give better results.

It is also to be concentrated to develop methodologies those less use external equipment (such as GPS).

3. Classification of DAD Schemes

The duplicate addresses in the network can be detected using two different mechanisms

1. Leader Action: a leader is elected in the network based on different criteria. The leader is responsible for the detection of duplicates of the addresses in the network. The leader maintains a table of available and free IPs of the network.
2. Individual Node Action: Here no leader exists. The individual nodes themselves monitor the network for the duplicates of the addresses. If any conflict is detected they themselves solve the conflict through exchange of messages.

In the first mechanism, the leader election process plays a vital role. When the leader fails, a new leader is to be elected. All these processes contribute to more overhead in the network.

In second mechanism, every node is a leader. The nodes monitor the network by exchanging different packets.

The Duplicate Address Detection can be classified based on the nature of the detection as

3.1 Proactive Duplicate Address Detection

In Proactive Duplicate Address Detection, frequent probing in the network is done for the detection of the duplicate addresses. For this purpose, some dedicated packets are employed to monitor the network.

The advantage of this methodology is that the duplicate addresses in the network can be completely removed. This methodology also got some disadvantage as the number of packet transmissions in the network are large and may lead to more overhead and bandwidth limitations. This methodology may use either the Leader Action mechanism or the Individual Node Action mechanism.

3.2 Reactive Duplicate Address Detection

Here the duplicate addresses are detected only when some network action is performed. No separate packets are dedicated for the detection of the duplicate addresses. Routing is the basic functionality of MANETs. Using routing packets itself, any duplicates of the addresses are detected.

The main advantage of this methodology is that additional overhead is avoided for the detection of the duplicate addresses. For using this methodology, care should be taken as different cases may arise which cause false detection. The disadvantage of this methodology is that the duplicate addresses are detected only at the time of routing. This methodologies use only Individual Node Action mechanism.

The DAD schemes are again classified based on the accuracy of the detection, as

3.3 Strong Duplicate Address Detection Schemes (SDAD)

SDAD schemes use either Leader Action or Individual Node Action. These schemes use the methodology of Proactive Duplicate Address Detection. They probe the network for the duplicates of the addresses. These schemes maintain greater accuracy in detecting the duplicates of IP addresses. But large Overhead is observed in these schemes. The definition of strong DAD attempts to cap-ture the intuitive notion of a "correct" or desirable behavior of a DAD scheme. We later show that strong DAD is not always achievable.

Before proceeding further, we would like to state two simplifying assumptions, which can be relaxed with simple changes to the proposed protocol:

1. Presently, we ignore the issue of address reuse in our discussion. However, proposed schemes can be mod-ified easily to incorporate limited-time "leases" of IP addresses.
2. For simplicity of discussion, we assume that each node in the wireless ad hoc network has a single interface, and we refer to the address assigned to this interface as the "node address". When a node is equipped with multiple interfaces, the protocols presented here can be easily adapted.

Informally, strong DAD allows detection of a duplicate address "soon after" more than one node chooses a given address. With strong DAD, if multiple nodes have chosen a particular address at a given time, then **at least** one of these nodes will detect the duplicate within a fixed inter-val of time.[1] An alternative would be to require **all** nodes to detect the duplication.

3.4 Weak Duplicate Address Detection Schemes (WDAD)

These schemes detect the duplicates less accurately. These schemes provide lesser overhead compared to SDAD schemes. These schemes utilize either Leader Action or Individual Node Action mechanisms. Both Proactive Duplicate Address Detection and Reactive Duplicate Address Detection methodologies can be employed in these schemes.

Delays in ad hoc networks are not always bounded. Even if the message delays were bounded, determining the bound is non-trivial (particularly when size of the network may be large and possibly unknown). Impossibility of strong DAD in presence of unbounded delays implies that timeout-based duplicate address detection schemes such as will not always detect duplicate addresses.

Motivated by the above observations, we propose **Weak** Duplicate Address Detection as an alternative to strong DAD. Weak DAD, unlike strong DAD, can be achieved de-spite unbounded message delays. The proposed weak DAD mechanism can be used either independently, or in conjunc-tion with other schemes.

Weak DAD relaxes the requirements on duplicate address detection by not requiring detection of all duplicate ad-dresses. Informally, weak DAD requires that packets "meant for" one node must not be routed to another node, even if the two nodes have chosen the same address

The DAD schemes are also classified based on the scope of detection as

3.5 Active Duplicate Address Detection Schemes (ADAD)

The ADAD schemes detect the winner and looser along with the detection of the duplicate addresses.

3.6 ii. Passive Duplicate Address Detection Schemes(PDAD)

The PDAD schemes detect only the duplicates in the network. The PDAD schemes are not concerned with the winner and loser. Most link state routing protocols use sequence numbers to distinguish fresh from old routing information. The idea of PDAD-SN is to exploit this property. It can be observed that nodes in a properly configured network obey the following rules:

A node uses increasing sequence numbers

A node uses each sequence number only once

Two nodes do not have the same neighborhood at the same time, if they are more than two hops apart from each other.

Following these properties, two theorems can be stated that apply if no duplicate addresses exist. If one of these does not apply, an address conflict is present in the network.

1. Two messages with the same sequence number and source address are copies of the same message.

A node does not receive a link state packet with its own address as source address and a sequence number, which is higher than its own counter value. The only exception from this is a sequence number wrap-around.

4. Existing Methodologies

Strong Duplicate Address Detection Schemes were proposed in [2]. In this mechanism, the nodes generate their own IP and probe in the network for the repetition of the IP. If a reply is received, new IP is generated and the process is repeated.

Perkins et al [3] have proposed a simple Duplicate Address Detection Schemes where the nodes choose a random address and send a request to the address. When no reply is received the address is fixed as the permanent address. This method got some limitations as the probability of the number of repetitions of the process of generating the new address and probing, is not clear. When two networks merge, the process proposed could yield a high overhead and may malfunction because of bandwidth limitations.

Vaidya‘s proposal [4] was aimed at the packet delivery to the correct node even if two nodes are with same address. Strong Duplicate Address Detection is not possible in this scheme. The proposal requires the modification of existing routing protocols to implement this scheme.

In [5], the proposed scheme used a leader to identify the group, and the nodes joining the network are assigned with the sequential addresses, with the newest member taking over the charge as leader. Each node periodically sends an update beacon message to the nodes with the next and previous addresses so that the node looses can be detected. Any node that becomes inactive for a particular period should acquire new IP.

Prophet address allocation Scheme [6] uses a mechanism similar to that of [5]. The first node that initialized in the network acts as the prophet and it allocates IP address to the new nodes that join the network. The presence of Duplicate Addresses is detected by the prophet. But this mechanism requires a super node (called as Prophet) to monitor the network. This method limits that the super node got the additional responsibilities and may die out quickly because of battery depletion. Leader election process is to be followed for the newer prophet.

In [7], five different schemes were introduced which detect the duplicates of the addresses in the network using only the routing messages. The schemes use two types of information such as Location of the nodes and the Neighbor List of the nodes. The main advantage of these schemes is that they use no other probing messages for the detection of duplicates of the addresses in the network. In this paper, the authors didn‘t mention any mechanism through which winner and looser are detected and how new IP is assigned for the looser. Another limitation of the schemes is that the duplicate addresses are not detected proactively. This may lead to the presence of the duplicate addresses in the network. And more over, the schemes require additional facilities such as GPS.

In [8], schemes for duplicate address detection in on-demand routing protocols are presented. These schemes use no other control messages for the detection of the duplicate addresses. Hence a very low overhead is achieved. The routing messages such as RREQ and RREP are used for the detection of duplicates of the addresses in the network.

However, the accuracy of detection is doubtful. These schemes may lead to false detections and which may result in the mal functioning of the nodes in the network.

5. Theoretical Analysis

A theoretical analysis of the Classifications of DAD Schemes is presented in Table 1.

The performance metrics of any DAD schemes are Accuracy, Detection Ratio, Overhead, and the load on any single node.

The Accuracy shows how accurately the duplicate addresses are detected avoiding the false detections. The Detection Ratio can be defined, as the ratio of total number of duplicate addresses detected in the network to the number of duplicate addresses actually exists.

Overhead is defined as the number of control packets needed in the network to the number of data packets that transmit in the network. Overhead represents both the node resources and network resources. If the overhead is more, the numbers of packets that transmit in the network are more and this leads to the quicker depletion of the battery of the nodes and limit the bandwidth.

The load on any single node is also should not be encouraged. This may lead to the failure of the node and for the election process, overhead may be incorporated. The failure of a node is disadvantageous and may even cause network partitioning.

5.1 Analysis of Classifications of DAD Schemes

In Leader action Classification the load on any single node is High. In Individual Node action the load on any single node is Low. In Proactive DAD the accuracy, detection ratio and overhead is High. In Reactive DAD the accuracy, detection ratio and overhead is Low. In SDAD accuracy and overhead is high. In WDAD accuracy is High.

REFERENCES

[1] Mobile Ad-hoc Networks (MANET), “www.ietf.org/html.charters/manet charter.html”

[2] C.E. Perkins, E. M. Belding-Royer, S. R. Das, ―IP Address Auto-Configuration for Ad Hoc Networks, Mobile Ad Hoc Networking Working Group- Internet Draft, January 2001.

[3] Perkins et al, ―IP Address Autoconfiguration for Ad Hoc Networks – Internet Draft(Nov. 2001)

[4] Nitin Vaidya ―Weak Duplicate Address Detection in Mobile Ad Hoc Networks, ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), June 2002.

[5] Nakjung Choi, C.K.Toh, Yongho Seok, Dongkyun Kim, Yanghee Choi, ― Random and Linear Address allocation for Mobile Ad hoc Networks, IEEE Communications Society, WCNC 2005.

[6] Hongbo Zhou, Lionel M. Ni, Matt W. Mutka, ― Prophet address allocation for large scale MANETs, www.elsevier.com/locate/adhoc, 423-434, 2003.

[7] Dongkyun Kim, Hong-Jong Jeong, C.K. Toh, Sutaek Oh, ― Passive Duplicate Address Detection Schemes for On-demand Routing Protocols in mobile Ad hoc Networks, IEEE Transactions onVehicular Technology, (To Appear 2009).

[8] K. Weniger, ―PACMAN: Passive Auto Configuration for Mobile Ad hoc Networks, IEEE Journal of Selected areas in communication , vol 23, No. 3, March 2005.

[9] K. Weniger and M. Zitterbart, “IPv6 autoconfiguration in large scale mobile ad-hoc networks,” in Proc. of European Wireless 2002, vol. 1, Florence, Italy, Feb. 2002, pp. 142–148.

[10] N. H. Vaidya, “Weak duplicate address detection in mobile ad hoc networks,” in Proc. of ACM MobiHoc 2002, Lausanne, Switzerland, June 2002, pp. 206–216.

[11] M. Gerla, X. Hong, and G. Pei, “Fisheye state routing protocol (FSR) for ad hoc networks,” IETF Draft, 2002.

[12] T. Clausen, P. Jaqcuet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, “Optimized link state routing protocol,” IETF Draft, 2002.