A Survey on IP Configuration of Mobile Ad Hoc Networks with and without DAD Mechanism

Hemamalini.V*, Dr. Zayaraz G**

*Ph.D. Scholar, Department of Computer Science & Engineering, Pondicherry Engineering College, Pondicherry, India
cse.malini@gmail.com
**Associate Professor, Department of Computer Science & Engineering, Pondicherry Engineering College, Pondicherry, India
gzayaraz@pec.edu.in

Abstract- A Mobile Ad hoc Network (MANET) is an instant infrastructure less self-organizing network, in which each node functions as an end host and a wireless relay. This form of wireless network is created by mobile nodes without any existing or fixed infrastructure. The nodes in the MANET need mutually exclusive identities before participating in any form of communication. In particular, each end host in the MANET needs to be uniquely addressed so that the packets can be relayed hop by hop and delivered ultimately to the destination. Existing routing protocols in MANETs have all assumed a priori that mobile nodes are configured with a valid (conflict free) network address. Because of the multi-hop routing, the MAC address at the link layer level cannot serve for this purpose. On the other hand, address configuration in wired networks, such as DHCP, requires the presence of a centralized DHCP server. It does not work well for MANETs due to the mobility of the nodes and the lack of a central authority. There have been several approaches proposed for dynamic addressing scheme. However, mostly all approaches depend on broadcasting for address solicitation and/or duplicate address detection. As a result, several types of security threats in dynamic IP configuration can be observed. Address allocation schemes can be classified into state full schemes or stateless schemes. The state full schemes keep state information in a database that keeps track of which addresses have been assigned to which computers. Stateless schemes let the computers select an address by themselves and perform a procedure, called Duplicate Address Detection (DAD).Thus this paper focuses on the various IP allocation schemes for MANETs with and without DAD.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an instant infrastructure less wireless independent self-organizing network, in which each node functions as an end host and a wireless relay. This form of wireless network is created by mobile nodes without any existing or fixed infrastructure. Since the mobile hosts usually have limited transmission range, bandwidth and battery power, multiple hops are generally required in MANETs to exchange data between nodes. The nodes inside the MANETs needs to be identified mutually before communicating with other devices, in particular, each host in the MANET needs to be addressed uniquely so that the packets can be relayed hop by hop and delivered ultimately to the destination. There is wide classification of existing routing protocols [1] in MANETs that assumes a priori taking into account that mobile nodes are configured with valid IP address. Also due to multi-hop routing the MAC address at the link layer level cannot serve for this IP allocation purpose. When it's to be seen at the other side, address configuration in wired networks, such as the Dynamic Host Configuration Protocol (DHCP) [8], requires the presence of a centralized DHCP server. Due to the mobility of the nodes and the lack of a central authority DHCP doesn't works over here. Given these uniqueness, address allocation in MANETs has attracted a significant amount of research. The purpose of address allocation in MANETs is not only to manage the address space efficiently and effectively but also to cope up with scalability, robustness and security. A un configured node should be able to allocate a unique network address in a timely manner, without costing excessive network traffic overhead. When a node leaves the network, its address should be reclaimed for future usage. All these needs should be well adapted to the distributed and dynamic nature of MANETs. In particular, we have to address the network partitions and mergers. Due to the mobility of the nodes, MANETs can be split into several disjoint partitions with no communications. These network partitions may or may not merge back later. And such partitioning or merging is often invisible to individual mobile hosts. In this paper, we will present a comprehensive survey on the state-of-the-art of address allocation schemes and their comparative study of MANETs. The rest of the chapter is organized as follows. Section 2 presents the background and introduces traditional address allocation schemes for IP-based networks. Section 3 describes System model describing the requirements of the system. Section 4 surveys the existing mechanisms of MANETs IP address allocation. Section 5 presents the comparative study of the schemes and Section summarizes the chapter.

II. BACKGROUND

In this section, we describe the traditional address allocation schemes and explain why they cannot be directly applied in MANETs. The address allocation schemes can be in general classified into stateful schemes or stateless schemes. The stateful schemes keep state information in a database that keeps track of which addresses have been assigned to which computers; while the stateless schemes allows the computers to select an address by themselves and perform a procedure, called Duplicate Address Detection (DAD)[11].

2.1. Traditional Stateful Schemes

2.1.1. Reverse Address Resolution Protocol (RARP): RARP protocol that belongs to TCP/IP group allows a computer to obtain its IP address from a RARP server in the bootstrap procedure [22]. Before obtaining an IP address, a computer has to use its MAC address to communicate with others. It first broadcasts a RARP request that specifies itself as a target. The RARP server on the same network keeps the database of IP addresses. Upon receiving a RARP request message, the RARP server looks up the IP address based on the requester's physical address and replies to the requester. RARP has the following limitations. First, the reply from the server contains only the 4-octet IP address; second, it cannot be used on networks that dynamically assign physical addresses.

2.1.2. Bootstrap Protocol (BOOTP): BOOTP was developed to overcome some of the drawbacks of RARP [23]. It uses UDP to carry messages and hence it can be implemented with an application program. Before obtaining an IP address, a computer can broadcast an IP datagram on the local network by using the limited broadcast IP address 255.255.255.255.The BOOTP server then broadcasts the reply message on the local network, which contains the requester's IP address, the router's IP address, etc. BOOTP is designed for a relatively static environment, and it provides only a static mapping from the physical address to the corresponding network parameters. It is not suitable for a dynamic environment.

2.1.3. Dynamic Host Configuration Protocol (DHCP): DHCP was developed as a predecessor to BOOTP [8].This provides configuration parameters to internet hosts that consists of two components: first one is a protocol for delivering host-specific configuration parameters from a DHCP server to a host and second one is a mechanism for allocation of network addresses to hosts. DHCP is built on a client-server model, in which designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. DHCP supports three mechanisms for IP address allocation. In "automatic allocation", a permanent IP address is assigned to a client. In "dynamic allocation", an IP address is assigned to a client for a limited period of time (or until the client explicitly relinquishes the address). In "manual allocation", a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator. Dynamic allocation is the only one of the three mechanisms that allows automatic reuse of an address that is no longer needed by the client to which it was assigned.

2.2. Traditional Stateless Schemes

2.2.1. IPV6 Stateless Address Auto Configuration: IPv6 stateless address auto configuration is performed only on multicast capable links [24]. A node starts the auto-configuration mechanism by generating a link-local address for its interface. This link-local address is generated by appending the interface's identifier to the well-known link-local prefix. Before assigning the link-local address to its interface, a node must attempt to verify that this link-local address is not used by another node on the same network. This is done by the Duplicate Address Detection (DAD) procedure. Specifically, it sends a Neighbor Solicitation message that contains the tentative address as the target address. Notice that this message uses the well-known un specified address as source IP address, and the solicited-node multicast address as the destination IP address. If another node is also using that address, it will return a Neighbor Advertisement message using the all-nodes multicast address as the destination IP address. If a node finds that its tentative link-local address is not unique in the network, auto-configuration process stops and manual configuration of the interface is required. On the contrary, if a node determines that its tentative link-local address is unique in the network, it assigns the address to itself and starts to communicate with all other nodes using this address.

2.2.2. Zero Configuration Networking (ZEROCONF): Address configuration without a dedicated server has been investigated by the Zero Configuration Networking (Zeroconf) working group of the Internet Engineering Task Force (IETF). The goal of the Zeroconf Working Group is to enable networking in the absence of configuration and administration. The Internet draft [25] describes a method for dynamic configuration of IPv4 link-local addresses used for local communications. When a node wishes to configure a link-local address, it selects an address pseudo-randomly, uniformly distributed in the range 169.254.1.0 to 169.254.254.255. Then it tests whether or not this address is already in use by broadcasting an ARP request for the desired address. If no conflicting ARP reply has been received after a predefined time

limit, then it can successfully claim the desired link-local address. Otherwise, it needs to select a new pseudo-random address and repeat the process.

2.3. Issues of traditional address allocation schemes

The traditional stateful address allocation schemes for IP-based networks require a centralized server to assign addresses to new nodes. Since MANETs have a highly dynamic topology and the centralized server may not always be reachable they cannot be directly applied to MANETs. The traditional stateless schemes cannot directly apply to MANET either because they require all nodes to be reachable via single-hop broadcast messages, which is generally not the case of MANETs. The Zeroconf solution also performs the DAD based on ARP request/reply messages, which may not be possible for MANETs. IPv6 stateless auto-configuration assumes the 48-bitIEEE-assigned globally unique MAC addresses. This hardware-based addressing scheme has the following limitations: (1) The 48-bit MAC address is too long for an IPv4 address. (2) The 48-bitMAC addresses may not be unique [26].It is also possible to change the MAC address by reprogramming the EEPROM or by modifying the MAC address in the OS memory. (3) Some devices in MANETs do not use a 48-bit MAC address. (4) The identity of a node can be easily determined from the network address, which raises privacy concerns.

III. REQUIREMENTS ANALYSIS

3.1. A protocol for assigning IP addresses should meet the following requirements:

(i) A node should obtain an IP address from MANET dynamically.
(ii) No conflict in IP address assignment, i.e., at any given instant of time there should not be two or more nodes with the same IP address.

(iii) When an IP is assigned, it is not guaranteed that the node will always be inside that particular network. When the node departs the network, its IP address should become available for assignment to other nodes.

(iv) If any of the nodes has a free IP address, this address should be assigned to the requesting node.

(v) The protocol should handle network partitioning and merging. When two different partitions merge, there is a possibility that two or more nodes have the same IP address. Such duplicate addresses should be detected and resolved.

(vi) The protocol should make sure that only authorized nodes are configured and granted access to network resources.

3.2. *Objectives*

Objectives of an optimal ad hoc network address configuration protocol:

(I) Dynamic Address Configuration: Nodes should be able to dynamically obtain IP addresses without manual or static configuration

(II) Uniqueness: Nodes should obtain unique addresses for correct routing and communication

(III) Robustness: The addressing protocol should adapt to the dynamics of the network, including partitions and merges

(IV) Scalability: The protocol should avoid significant performance degradation as the size of the network increases.

(V) Security: Without authentication, several types of security threats can be seen at the time of address allocation. Therefore, security is also a prime concern for the address allocation protocol of a MANET.

3.3. Partitioning Of MANET

The split of network into more than two sub-networks is known as partitioning which leads to IP address leakage. So MANEs partitioning can be of two types: graceful departed and graceless departure.

3.3.1. Graceful Departure: If nodes leave their network after informing their neighbors by sending their current status and information by signed RELEASE message to its ancestor then it is said to be graceful departure. Every node maintains recycle LIST for updating the allocation status for its departed children. After receiving the signed RELEASE message from

its children, the parent checks the authentication of the children as well as the signature of RELEASE message. If the authentication is successful, the parent node updates its recycle LIST and sends a signed OK message to the children that depart. If the departing node receives a signed OK message from its parent before the timer expires then the departing node departs gracefully. If the root node wants to leave, it informs its greatest descendent to be the new root.

3.3.2. Graceless Departure: A node goes gracelessly departed due to several reasons. (a) Due to loss of packet (b) When two MANETs merge (c) If a MANET splits into two or more MANETs. Therefore it is necessary to detect the graceless departure of a node so that its IP address leakage can be avoided and the address can be reused. To prevent this first every node scans IP addresses of its children. If the parent node discovers that a child node is missing, it then updates the recycle LIST for the missing child node to reuse the IP address later. By periodically broadcasting signed HELLO messages of AODV routing protocol graceless departure or address leak problem can be detected. In the figure 3.1(a), Cluster I has four nodes with address 192.168.1.11, 192.168.1.12, 192.168.1.13 and192.168.1.14. When Cluster I undergoes partition, as in figure 3.1(b), it partitions into Cluster I (a), having the mobile nodes 192.168.1.11 and 192.168.1.13, and Cluster I (b), having the mobile nodes 192.168.1.12 and 192.168.1.14.According to Graceful departure, the nodes in the original cluster (Cluster I) can update their address list (i.e.) remove the leaving node from the list.

3.4. Merging Of Several Manets

When more than two or more networks combine together as a new network then it is called merging. This situation occurs when independent networks come into range of each other that causes IP address conflict. In the figure 3.1(c), Cluster I (a), Cluster I (b) and Cluster II merge to form a single cluster. Cluster II has two nodes with address 192.168.1.11 and 192.168.1.15.When the merging occurs both Cluster I (a) and Cluster II has the node with address 192.168.1.11 so the problem of duplicate addressing occurs in the new cluster that is formed after merging. Therefore when a message packet arrives for the node with the address 192.168.1.11 of Cluster I (a), it can be erroneously routed to the node with the address 192.168.1.11 of Cluster II .In order to overcome this, a Duplicate Address Detection (DAD) is used. As reviewed in MANETconf[18] two nodes exchange their identifiers that initiate a communication. If identifiers are different, then they realize that their networks have merged. Then they act as configured initiators and start reconfiguration of nodes with conflicting address in their own network. In ZAL [28] nothing needs to be done when networks were part of the same larger network because address spaces at different sub-networks were disjoint. Partition ID is used to find out that they belong to the same larger network. If merging networks never met before, ZAL proposes to convert addresses of nodes in smaller networks to that of larger networks. Only addresses in one of the networks can be preserved. The others have to convert. It is a gradual process in which first nodes at the boundaries of smaller networks and then slowly innermost are converted. It is desirable to minimize overhead by minimizing number of address conversions based on distributed algorithms.

3.5. Duplicate Address Detection (DAD)

DAD is required when either a new node joins a MANET or independent networks merge. When a new node picks up a tentative IP address, DAD process determines whether this address is available or not. All the nodes having a valid IP address participate in DAD to protect their IP address being used accidentally by new node. The uniqueness check is based on sending a Duplicate Address Probe (DAP) and expecting an Address Conflict Notice (ACN) back in a certain timeout period. If, after 'n' number of retries, no ACN is received, the node may assume that address is not in use. This process is illustrated in Figure 3.1. But in networks where message delays cannot be bounded, use of timeouts can lead to unreliability. So duplicate addresses may occur in MANET. In case of merge, many nodes may have duplicate addresses and thus overhead of the network would increase suddenly due to start of DAD process for every node. Address auto configuration method must treat it as a special case. [11] Introduces Strong DAD & Weak DAD. Strong DAD allows at least one node to detect duplicate immediately after it has been chosen by another node. Practically it is not possible. Weak DAD is based on enhancement of link state routing. Each node of network owns a unique identifier. A node sends control packet indicating its link state along with its identifier. Each node keeps state of the links it is connected to, corresponding addresses & identifiers. If a node N receives a control packet from a known address but with different identifier, then it has detected a duplicate. 'N' begins to announce duplicate and keep sending packets to the node it previously knows. MANETConf [18] proposes a reliable DAD process. It has two phases: initiation & validation. A new node (requester) takes help of a configured neighbor (initiator) to obtain address. Initiator broadcasts an address for the requester. All nodes have to answer this request. This ensures that requester would not use the address of a temporarily disconnected node. If a node does not answer after a number of tries, its address can be treated as unassigned.

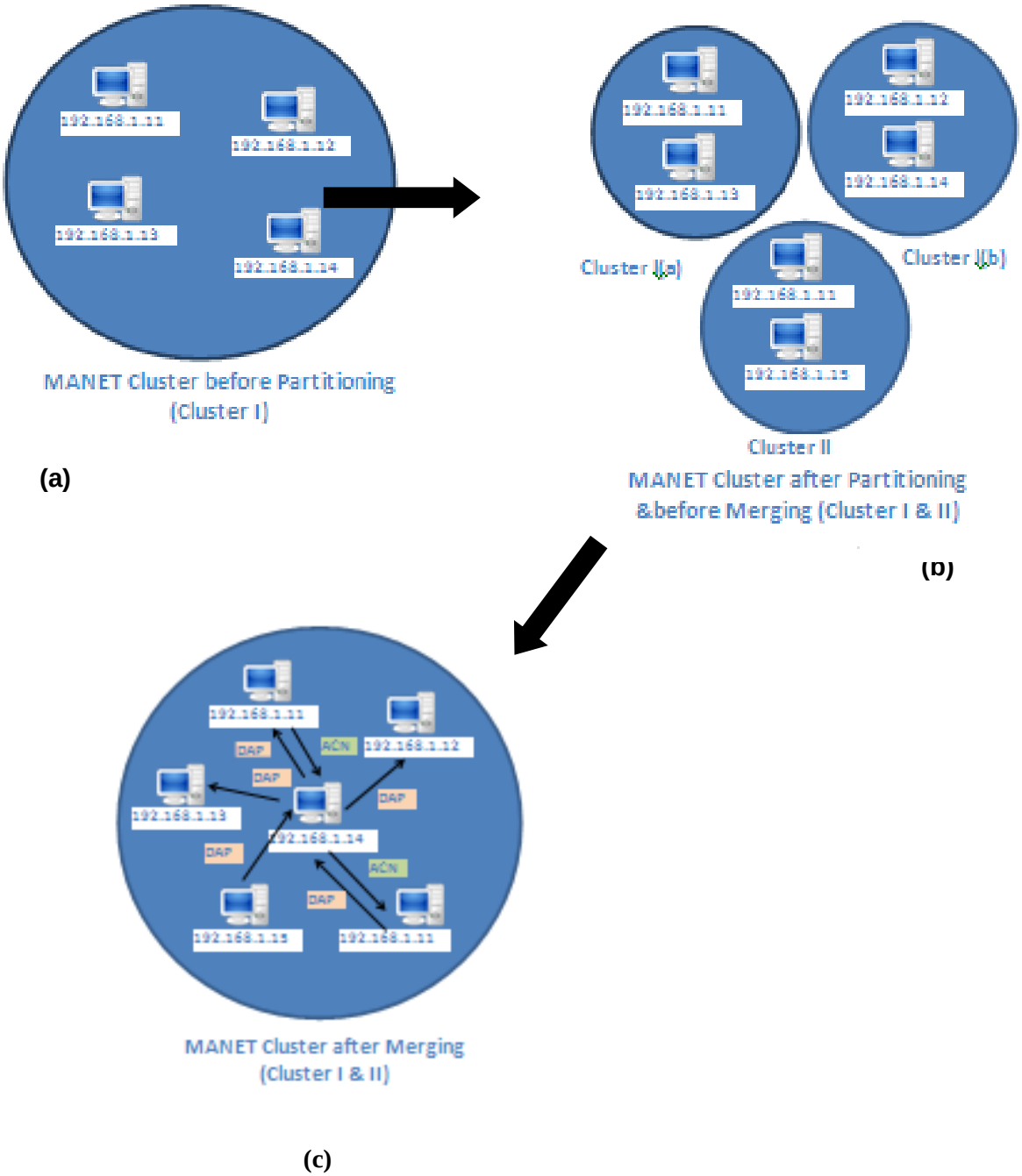

Figure 3.1

The Duplicate address detection can be further understood from the Figure 3.2. The existing MANET consists of the nodes based on their node address, Node A, Node B, Node C, Node D, Node E, Node F and Node G. The new node which joins the MANET approaches the nearest node, Node E and asks for address to be allocated. The Node E allocates the address G for the new node. The Node E then checks with the other nodes in the MANET if the address already exists. During the check, Node G identifies that the address is duplicated and returns the DAD to Node E. Thus the DAD mechanism identifies the occurrence of duplicate addresses in the MANET.

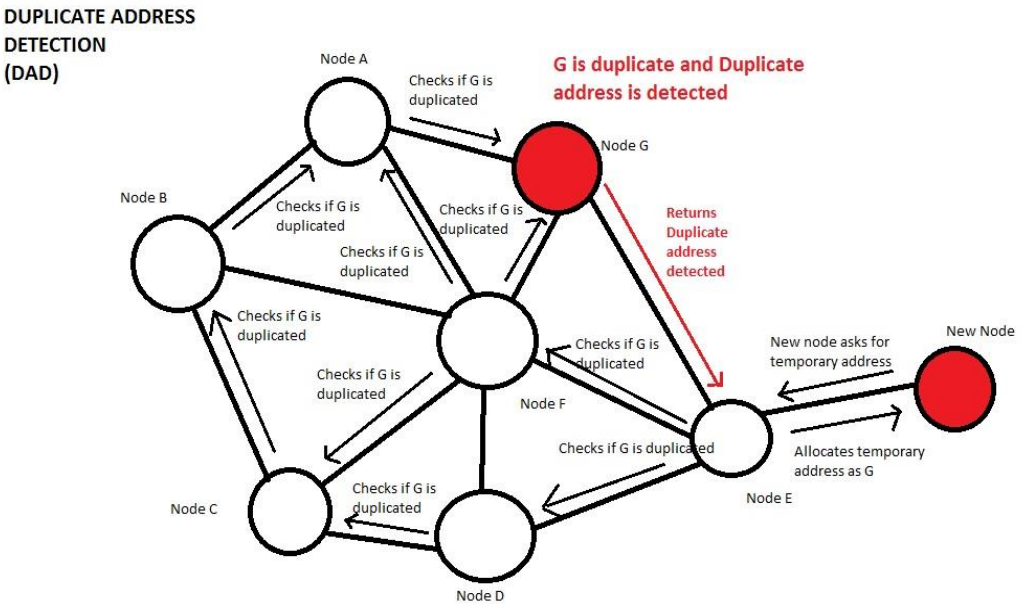

Figure 3.2

IV. ADDRESS CLASSIFICATION

The proposed addressing schemes for ad hoc networks are categorized into three groups: Best Effort Allocation, Leader Based (centralized) Allocation and Decentralized Allocation approaches [10].

In Best effort allocation a node assigns its address without involving any other node in the network, example is Prophet Scheme [14] (generation of random numbers).The advantage in this mechanism is Low addressing latency and low communication overhead. The drawback is that even with a large address space, address conflicts may exist in the network which is resolved by passive DAD [12] or weak DAD [11]. Hence DAD mechanisms also come under Best effort Allocation mechanism. In Leader based approach nodes obtain valid IP addresses from an elected leader or server of the network and hence this eliminates the need of DAD. Some of the schemes are: 1.DHCP [8] (Client-Server Architecture), 2.DACP [15] (Address Authority-temporary address is used to verify the uniqueness),3.VASM[16](Initiator gets IP from Allocator and assigns to Requester),4.Lightweight secure address configuration scheme[17] (uses VASM address configuration scheme).In decentralized allocation the host acquires an IP address either itself or from a neighbor and then performs the DAD to ensure the uniqueness of the address. Some of the schemes are: 1.MANETconf [18] (every node keeps track of the addresses already allocated in the network), 2.AAA [19] (uses randomly selected addresses from the address range of 169.254/16, then applies DAD), 3. Prime DHCP [20] (address can be allocated to the new host without broadcasting it over the whole of MANET-PNAA algorithm), 4. AIPAC[21](Automatic IP address configuration - The Initiator negotiates for the Requester's valid IP address in the allocation phase, corrects the configuration, and then offers it to the requester) 5. Secure host auto-configuration scheme [29] (a node has to answer a question to prove its identity. It uses the buddy system technique to allocate the IP address) 6. Quadratic residue based address allocation [30] (the first node in the network configures itself with an IP address and also generates the number of distinct cycles and length of each long cycle (address block)). 7. Secure auto-configuration scheme [9] (uses self-authentication technique-using one-way hash function) 8. MMIP[31](every node in the network act as proxies and binds the MAC address with the IP address at the time of address allocation)9.ADIP[32](utilizes nodes in the network as proxies and can generate IP addresses from its own IP for a new authenticated host)10. IDDIP algorithm [6] (ID based Dynamic IP) 11. IDSDDIP Algorithm [33] (This scheme is similar to IDDIP but has been proposed for IPv6).

4.1. Best Effort Allocation

4.1.1. Prophet Scheme [14]**:** Here a function f(n) generates a series of random numbers for address allocation. The first node A in the MANET generates a random number and sets its IP address. It also uses a random state value as the seed for its f (n). Another node B can get an IP address from node A along with a state value as the seed for its f (n). Whenever a node joins the MANET, the same process continues for the address allocation.

4.1.2. Weak Dad: This mechanism prevents a packet from being routed to a wrong destination, even if duplicate addresses exist [11].The technique is that a unique key for each node is included in the routing control packets and in the routing table entries. Hence, suppose if two nodes happen to have selected the same IP address, they can still be identified by the use of their unique keys. Hence every node is identified by a unique tuple <address, key>.Usually the authors of [22] suggest using a node's MAC address as its key.

4.1.3. Passive DAD: This is a modification of DAD again where in the nodes use periodic link state routing information to notify other nodes about their neighbors. This is a very hectic measure and hence usually very costly and will result in serious redundancy, contention, and collision, which leads to broadcast storm problem [13].

4.2. Leader Based Allocation

4.2.1. DHCP [8] **(Dynamic Host Configuration Protocol):** DHCP is developed as a successor to BOOTP [23].Here a DHCP server that has been designated allocates network addresses and delivers all the configuration parameters to dynamically configured computers. The most positive aspect of DHCP is its dynamic address assignment, in which the DHCP server does not need to know the identity of the client in prior. Auto-configuration becomes possible if the DHCP has been provided with a set of available IP addresses. At present, DHCP is widely used in Ethernets and Wireless LANs.

4.2.2. DACP [15] **(Dynamic Address Configuration Protocol):** In DACP, the leader is an elected Address Authority (AA) that maintains the state information of the all the nodes in MANET. Then using DAD mechanism a temporary address is used to verify the uniqueness of the allocated address .The main drawback of this protocol is due to DAD that causes overhead and also due to address authority that causes high periodic flooding.

4.2.3. ODACP [10] **(Optimized DACP):** To overcome the overhead caused by DACP, this is introduced without DAD and thus results in pure leader based approach. Here the leader is elected in the same way as in DACP, with every node registering with the leader without flooding address requests. The leader verifies or denies the registration according to the address availability in network. In both DACP and ODACP, the detection of merges and partitions is implemented by leader advertisement.

4.2.4. VASM [16] **(Virtual Address Space Mapping):** The concept of VASM is that it uses virtual address space for addressing new nodes that joins a network. The technique is that it maps one point of virtual address sheet to exactly one new node. The term "virtual" is used to specify that the whole corresponding address space is a 2D flat sheet and each point of this sheet is virtually mapped to a node in MANET. For generation of address the protocol uses coordinate values. In this protocol, nodes are classified into four categories: ***Allocator***: Maintain the address space. They allocate new addresses for joining nodes. ***Initiator***: An intermediate node between *Allocators* and *Requester* node that exchange all messages between them. ***Requester***: new node that needs to get IP addressing order to join the network. ***Normal***: all other nodes are in this category. Each *Allocator* in the network contains a disjoint address space. Therefore, address space overlap between *Allocators* is none.

4.2.5. A Lightweight Secure Address Configuration [17]**:** This is based on Virtual Address Space Mapping (VASM).It uses VASM address configuration scheme for allocation of address which is based on a zero knowledge approach. It also uses secret key and symmetric cryptographic function to avoid Man in Middle attack.

4.3. Decentralized Allocation

4.3.1. MANETCONF [18]**:** Manetconf prevents concurrent assignment of the same address by maintaining an additional allocation table for pending allocations. A new node obtains an IP address by broadcasting a **neighbor query** message throughout the network. The existing node performs an **address query** throughout the network on the new node's behalf. This address allocation requires a positive acknowledgment (ACK) from all known nodes indicating the address is available for use. Each node in the network also agrees on a partition ID to detect partitions and merges. A network partition is detected when the node performing address assignment for a new node fails to obtain ACKs from all other nodes in the network. After the detection, the set of nodes from whom an ACK was not received is deleted from each node's list of in-use addresses. The nodes then agree on a new partition identifier. When partitions merge, nodes in different partitions are required to exchange their set of allocated addresses so that duplicates can be detected. The disadvantage is that high tolerance to message losses, network partitioning and mergers. Its advantage is that it has low latency and communication overheads.

4.3.2. AAA [19] **(AD-HOC ADDRESS AUTO-CONFIGURATION):** In AAA addresses are randomly selected from the address range 169.254/16.Duplicate address detection (DAD) is performed by each node to guarantee the uniqueness of the

selected address. During this process, a node floods an **Address Request** message in the network to query for the usage of its tentative address. If the address is already in use, an **Address Reply** message is unicast back to the requesting node so that a different address can be selected. The absence of an Address Reply indicates the availability of the requested address. The disadvantage of this approach does not consider complex scenarios such as network partitions and merges.

4.3.3. PRIME DHCP [20]**:** It can allocate addresses to the hosts of a MANET without broadcasting over the whole MANET. It makes each host a DHCP proxy of the MANET and run a prime numbering address allocation algorithm individually to compute unique addresses for address allocation. The concept of DHCP proxies and the prime numbering address allocation algorithm (PNAA) together eliminate the needs for broadcasting in the MANET. It can significantly reduce the signal overhead and the latency for hosts to acquire addresses. Some of its disadvantages are **(**i) Nodes working as DHCP servers would not always remain active or connected while the network exists, (ii) Since energy resources of devices are limited, the configuration protocol should not overload some specific nodes for managing addresses, (iii) The bandwidth of wireless communication links is limited, so the configuration of nodes (especially in large networks) should take place with distributed approaches.

4.3.4. AIPAC [21] **(AUTOMATIC IP ADDRESS CONFIGURATION):** This protocol assigns unique IP address to each node and manages possible duplicate addresses due to the mobility of nodes in the network. It avoids the storage of large amounts of data and makes use of procedures that minimize the number of exchanged packets. It also provides a new mechanism, called Gradual Merging of networks that causes the merging process of networks according to their evolution. The disadvantage is that it makes use of network identifiers, but allows different network to coexist. It avoids overloading nodes and communication channels whenever two networks merge.

4.3.5. Secure Host Auto Configuration Scheme [29]**:** The scheme employs the concept of challenge, where a node has to answer a question to prove its identity. It uses the buddy system technique to allocate the IP addresses. In the buddy system allocation scheme, each node maintains a block of free addresses. A configured node which receives an Address Request from a new node, assigns the requesting node an IP address from its block of free addresses. It also divides its block of free addresses into two equal parts and gives one half to the requesting node and the other half it keeps with itself for future use. However, it is always difficult for the individual nodes to manage such type of address blocks in a MANET. Also, it is complex to be implemented.

4.3.6. Quadratic Residue Based Address Allocation [30]**:** Here, the first node in the network configures itself with an IP address and also generates the number of distinct cycles and length of each long cycle (address block).

4.3.7. Secure Auto-Configuration [9]**:** This uses self-authentication technique. By using one-way hash function, it binds a nodes address with public key. Address owner can use corresponding public key to unilaterally authenticate itself. The scheme handles network partitioning/merging by employing the concept of passive DAD mechanism.

4.3.8. MMIP (MAC Mapped IP) [31]**:** This scheme proposes a technique to map the MAC addresses of the nodes along with the IP addresses which are assigned at the time when a node enters the network. Performance analysis shows that this addressing scheme has less addressing latency and control overhead compared to the similar existing schemes.

4.3.9. ADIP [32]: This scheme utilizes nodes in the network as proxies and can generate IP addresses from its own IP for a new authenticated host. The address configuration authentication is done with the help of trusted third party and as such capable of handling the security threats associated with a general dynamic IP configuration.

4.3.10. IDDIP Algorithm [6]**:** In this scheme, an ID based dynamic IP configuration scheme has been presented that can securely allocate IP addresses to the authorized hosts for a mobile ad hoc network without broadcasting over the entire network. Each host in the MANET can generate a unique IP address from its own IP address for a new host. This scheme provides authentication for address configuration without the help of a trusted third party while taking care of the security threats associated with dynamic IP configuration. Additionally this solves the problem of network partitions and mergers along with the arrival and departure of a host efficiently and securely. Most important is no DAD mechanism is used here.

4.3.11. IDSDDIP Algorithm [33]**:** This scheme is similar to IDDIP but has been proposed for IPv6 named as ID based secure distributed dynamic IP configuration. This does not require the need for broadcasting messages over the entire MANET during the address allocation process. In this scheme, each host in the MANET can generate a unique IP address for a new authorized host. It generates node ID as a node identifier which is evaluated using its public key and a secure one way hash function for node authentication purpose. This scheme can handle the problem that may arise due to host failures, message losses, mobility of the host and network portioning or merging.

V. COMPARATIVE STUDY

Metrics comparison of all the existing dynamic addressing approaches

Table 4.1

Metrics	Prophet	DHCP	ODACP	Manetconf	AAA	Prime DHCP	AIPAC
Uniqueness	No	Yes	Yes	Yes	No	Yes	Yes
Latency	O(2t)	O(4td)	O(2td)	O(2td)	O(2td)	O(2t)	O(2t)
Overhead	O(n/2)	$O(n^2)$	O(2l)	$O(n^2)$	$O(n^2)$	O(n/2)	O(n/2)
Complexity	High	Low	Low	High	Low	Low	Low
Periodic Message	No	Yes	Yes	Yes	No	Yes	Yes
Security	No	No	No	No	No	No	No

Table 4.2

Metrics	Buddy	Quadratic Residue	Secure Auto	MMIP	ADIP	IDDIP	IDSDDIP
Uniqueness	Yes	No	No	Yes	Yes	Yes	Yes
Latency	O(2td)	O(2td)	O(2td)	O(2t)	O(2t+m)	O(2t+p)	O(2t+p+c)
Overhead	$O(n^2)$	$O(n^2)$	$O(n^2)$	O(n/2)	O(n/2)	O(n/2)	O(n/2)
Complexity	High	Medium	Medium	Low	Low	Low	Low
Periodic Message	Yes	No	No	No	Yes	Yes	Yes
Security	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 4.1 & 4.2 shows the comparative analysis of all the existing schemes. It has been focused on qualitative evaluation of all approaches. The denominations are as below:

n- No. of mobile nodes in the network
l- No. of links
t- Average 1-hop latency
d- Network diameter
p- Complexity of public key digital signature

The existing Prophet [14] scheme cannot guarantee uniqueness, but the latency of Prophet, PrimeDHCP and AIPAC [21] is 2*t since they send request to their neighbors for IP address. Their communication overhead is average degree (n/2) of each node in network. DHCP [8] gives the guarantee of uniqueness but cannot be deployed in the network. Moreover, DHCP needs to locate the server and thus its latency is 4*t*d and communication overhead is $O(n^2)$.In ODACP[10] all the nodes as

to register with an address authority to reduce the communication overhead from $O(n^2)$ to O(2l) and the latency has to be reduced from 4*t*d to 2*t*d. Moving to the decentralized mechanism MANETconf[18],this requires a positive acknowledgement from all known nodes indicating that the address is available for use. Since DAD is necessary for this the latency of MANETconf is 2*t*d and communication overhead is $O(n^2)$.In AAA [19], the network is flooded by address request message to query the availability of the requested address and hence the latency is 2*t*d and communication overhead is $O(n^2)$.Buddy scheme [7] uses free address pool and partitions the pool of address into two. This address will be given on request by other nodes and hence here each node should maintain address blocks which becomes complicated. Hence the latency depends on the network diameter which becomes 2*t*d and communication overhead is $O(n^2)$.Since quadratic residue[30] method involves with distinct cycles and its corresponding cycle length the latency and communication overhead is same as the buddy scheme. In secure auto configuration [9] DAD message is flooded all over the network and hence the latency is 2*t*d and communication overhead is $O(n^2)$.The last four schemes considers security aspects during allocation process. And so if recognized properly the latest scheme developed by Uttam and Raj [6] needs no DAD mechanism, also it provides security by secure one way hash function (for authentication) and RSA algorithm. Hence the latency for MMIP [31], ADIP [32], IDDIP [6] and IDSDDIP [33] are 2t, 2t+m, 2t+p, 2t+p+c respectively. It has been identified that m, p & c denotes the complexity of the public key signature (RSA algorithm) and the encryption/decryption algorithms. Hence the latency is only fairly good for the last three methods. The communication overhead is the average degree (n/2) for each node of the network.

VI. CONCLUSION

This report has been worked out with all possible dynamic address allocation mechanisms considering the duplicate address detection mechanism and also tried investigating the problems of dynamic addressing in a mobile ad hoc network. Short descriptions of basic addressing schemes have been given to help have an overview of this field in MANET. We also studied the current solutions by categorizing and qualitatively analyzing latency and other performance properties of the approaches.

REFERENCES

[1] C. Perkins, E. Belding-Royer, S. Das, Ad hoc On-demand Distance Vector (AODV) Routing, Draft-ietf-manet-aodv-11.txt, June 2002.
[2] Address Allocation Mechanisms for Mobile Ad Hoc Networks, Xiaowen Chu, Jiangchuan Liu, and Yi Sun, S. Misra, Guide to Wireless Ad Hoc Networks,Computer Communications and Networks, DOI 10.1007/978-1-84800-328-6_14,_ Springer-Verlag London Limited 2009.
[3]Address configuration in MANET, Mobility in TCP/IP, Spring 2006, Hai Nguyen Thi Van, hainguyen@tsc.upc.edu.
[4] Issues & Trends in AutoConfiguration of IP Address in MANET,Harish Kumar, R.K. Singla, Siddharth Malhotra, Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844,Vol. III (2008), Suppl. issue: Proceedings of ICCCC 2008, pp. 353-357.
[5] Ip Address Assignment In A Mobile Ad Hoc Network,Mansoor Mohsin and Ravi Prakash,The University of Texas at Dallas,Richardson, TX, MILCOM 2002
[6] A secure dynamic IP configuration scheme for mobile ad hoc networks,Uttam Ghosh , Raja Datta, journal homepage: www.elsevier.com/locate/adhoc, Vol 9,February 2011.
[7] A Security Framework for Buddy System based MANET Address Allocation Scheme,Abdelhafid Abdelmalek, Zohra Slimane, Mohammed Feham and Abdelmalik Taleb-Ahmed ,IJCSI,July 2011.
[8] R. Droms, Dynamic Host Configuration Protocol, RFC 2131, March 1997.
[9] P. Wang, D.S. Reeves, P. Ning, Secure address auto-configuration for Mobile Ad Hoc Networks, in Proceedings of 2nd Annual International Conference MobiQuitous, 2005.
[10] Y. Sun, E.M. Belding-Royer, A study of dynamic addressing techniques in Mobile Ad Hoc Networks, Wireless Communications and Mobile Computing (April) (2004).
[11] N.H. Vaidya, Weak duplicate address detection in Mobile Ad Hoc Networks, Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc02), June 2002, pp. 206–216.
[12] K. Weniger, Passive duplicate address detection in Mobile Ad Hoc Networks, in WCNC, (Florence, Italy), February 2003.
[13] S. Ni, Y. Tseng, Y. Chen, J. Sheu, The broadcast storm problem in a Mobile Ad Hoc Network, in: Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), 1999, pp. 151–162.
[14] H. Zhou, L.M. Ni, M.W. Mutka, Prophet address allocation for large scale manets, INFOCOM, 2003, pp. 1304–1311.
[15] Y. Sun, E.M. Belding-Royer, Dynamic address configuration in Mobile Ad Hoc Networks, UCSB Tech. Rep., June 2003, pp. 2003–2011.
[16] M. Taghiloo, M. Dehghan, J. Taghiloo, M. Fazio, New approach for address auto-configuration in manet based on virtual address space mapping (vasm), in: International Conference on Information and Communication Technologies: from Theory to Applications (IEEE ICTTA 2008), Damascus, Syria, 7–11 April 2008.
[17] M. Tajamolian, M. Taghiloo, M. Tajamolian, Lightweight secure ip address auto-configuration based on vasm, in: 2009 International Conference on Advanced Information Networking and Applications Workshops, Waina 2009, pp. 176–180.
[18] S. Nesargi, R. Prakash, Manetconf: Configuration of hosts in a Mobile Ad Hoc Network, INFOCOM, 2002, pp. 1059–1068.
[19] C.E. Perkins, J.T. Malinen, R. Wakikawa, E.M. Belding-Royer, Y. Sun ,Ad hoc address autoconfiguration, IETF Internet Draft, vol. draft-ietfmanet-autoconf-01.txt, 2001.
[20] Y. Hsu, C. Tseng, Prime dhcp: a prime numbering address allocation mechanism for manets, in: IEEE Communicatons, August 2005.
[21] M. Fazio, M. Villari, A. Puliafito, Aipac: automatic ip address configuration in Mobile Ad Hoc Networks, Performance Evaluation of Wireless Networks and Communications Computer Communications 29 (8) (2006) 1189–1200.
[22] R. Finlayson, T. Mann, J. Mogul, and M. Theimer. A reverse address resolution protocol.RFC 903, June 1984.

[23] B. Croft, and J. Gilmore. BOOTSTRAP PROTOCOL (BOOTP). RFC 951, September 1985.
[24]S. Thomson, and T. Norten. Ipv6 stateless address autoconfiguration. RFC 2462, December 1998.
[25] B. Aboba, S. Cheshire, and E. Guttman. Dynamic configuration of ipv4 link-local addresses. In IETF Internet draft, July 2004, Work in Progress, http://files.zeroconf.org/draft-ietf-zeroconfipv4-linklocal.txt, July 2004.
[26] DuplicateMACAddresses on Cisco 3600 Series, http://www.cisco.com/warp/public/770/7.html, 1997.
[28] Zhihua Hu & Baochun Li., "ZAL: Zero-Maintenance Address Allocation in mobile Wireless Ad Hoc Networks," Pro-ceedings of 25th ICDCS 2005, pp 103-112, Columbus, Ohio, June 6-9, 2005.
[29] A. Cavalli, J. Orset, Secure hosts auto-configuration in Mobile Ad Hoc Networks, Data Communication and Topology Control in Ad Hoc Networks Ad Hoc Networks 3 (5) (2005) 656–667.
[30] X. Chu, Y. Sun, K. Xu, Z. Sakander, J. Liu, Quadratic residue based address allocation for Mobile Ad Hoc Networks, in:Communications, 2008. ICC '08. IEEE International Conference on, 2008.
[31] U. Ghosh, R. Datta, Mmip: a new dynamic ip configuration scheme with mac address mapping for Mobile Ad Hoc Networks, in:Proceedings Fifteenth National Conference on Communications 2009, (IIT Guwahati, India), January 2009.
[32] U. Ghosh, R. Datta, Adip: an improved authenticated dynamic ip configuration scheme for Mobile Ad Hoc Networks, Int. J. Ultra Wideband Commun. Syst. 1 (2) (2009) 102–117.
[33] **U. Ghosh, R. Datta** : An ID based secure distributed dynamic IP configuration scheme for mobile ad hoc networks , ICDCN'12 Proceedings of the 13th international conference on Distributed Computing and Networking, Pages 295-308 , Springer-Verlag Berlin, Heidelberg ©2012