# A Review of Addressing Protocols in Mobile Ad-hoc Networks

N. Ramakrishnaiah
Dept. of Computer Science & Engineering,
University College of Engineering, JNTUK,
Kakinada – 533003, A.P., India.

P. Chenna Reddy
Dept. of Computer Science & Engineering,
JNTUA College of Engineering,
Pulivendula – 516390, A.P., India.

## ABSTRACT

A Mobile Ad hoc Network (MANET) is a self organizing, multi-hop wireless network without infrastructure. Most of the research in the area of MANETs focuses on routing protocols. Although routing protocols assume unique node addresses, the question of how to assign them remains open. Addressing is a tough task in MANETs because of its node mobility and lack of infrastructure. An address autoconfiguration protocol for ad-hoc networks not only assigns unique addresses to its mobile nodes but also maintains its address pool efficiently. An addressing protocol assigns a unique address to its mobile nodes with less overhead and delay and also handles the network partitioning and merging effectively. Several address autoconfiguration protocols have been proposed for MANETs. This paper presents the brief description of the addressing protocols in MANETs and their comparison in terms of performance metrics address uniqueness, latency, overhead and scalability.

## Keywords

Wireless networks, Mobile ad-hoc networks, Address autoconfiguration protocols.

## 1. INTRODUCTION

Dynamic address assignment in traditional networks is done by using either a stateful protocol such as Dynamic Host Configuration Protocol (DHCP) [1] or a stateless protocol such as IPv6 stateless address autoconfiguration [2]. When the network demands unique IP addresses, we usually use stateful approach otherwise use stateless approach, in which address uniqueness is maintained along the route. The DHCP requires a centralized server to allocate addresses to new nodes. It can't be directly applied to MANETs, because ad hoc networks have a highly dynamic topology and not possible to maintain a centralized server. The traditional stateless protocols can't be directly applied to MANETs, because all the nodes in the ad hoc network may not be reachable in a single hop.

Every node in a MANET needs some sort of identity before participating in any type of communication. Each host in an ad hoc network needs to be exclusively addressed so that the packets travelled hop by hop and are delivered to the destination. Every node has a MAC address at the link layer level. However, use of MAC address as a distinctive identifier has the following restrictions [3].

- This hardware based addressing approach requires specific implementations for each type of hardware.

- The MAC address might not be unique. We can alter the MAC address by reprogramming the EEPROM.

- There are examples of many NIC cards from the same vendor with the same MAC address.

Address assignment in MANETs is a difficult task. An address autoconfiguration protocol for dynamic allocation of unique addresses to mobile nodes is needed in MANETs. From the last decade, many addressing schemes have been proposed for MANETs.

This paper describes various addressing protocols in wireless ad hoc networks and their comparison in terms of various performance metrics.

The rest of this paper is organized as follows: section 2 presents the description of the protocols, section 3 defines the performance metrics of addressing schemes and also comparison table with regard to those metrics and section 4 presents conclusions of the paper.

## 2. DESCRIPTION OF ADDRESSING PROTOCOLS

The most recent classification scheme based on address assignment approach to categorize addressing protocols is discussed in [4]. It categorizes the addressing schemes as neighbor based schemes, decentralized schemes and centralized schemes.

### 2.1 Neighbor based Schemes

In neighbor based schemes, a new node gets an address from its neighbor nodes and uniqueness is ensured with local communication. In these schemes, each node which is responsible for address assignment maintains a disjoint address space or a specially designed function is used to assign the addresses to newly joined nodes.

Zhou et al. [5] suggested a Prophet Address assignment protocol for MANETs that uses a specially designed function to produce a chain of random numbers as addresses of nodes. A random number is generated by the first node as its identity and make use of another number as the seed of the function to generate addresses to new nodes. When a new node wishes to enter into the network, the first node or its neighbor node generates another number by using its seed value, say $a_2$ and a state value and give them to new node. New node uses $a_2$ as its identity and state value as the seed of function to generate addresses. In this scheme, the communication overhead and delay are low, but address conflicts may occur in large address space.

Mohsin et al. [6] suggested an addressing scheme called as Buddy protocol, which uses numerous disjoint allocation tables for address allocation. In this scheme, each node has an e x c l u s i v e set of addresses those can be allocated to newly joined nodes. An initiator node can have single or many sets of addresses, the latter case occurs when neighbor

nodes depart the MANET with prior information and release their unused address blocks. A coordination process is used to collect the leak addresses, when a node leaves the network suddenly without prior information. An initiator node with one address block divides its block of unused IP addresses into two disjoint sub-blocks, one for itself and the other to assign to new node, or if the initiator node has multiple blocks of unused addresses then it allocates one block to the new node. The new node assigns itself by taking the earliest value from the received set of addresses and maintains the remaining addresses for upcoming nodes. This protocol uses the network ID mechanism to detect and solve network partitioning and merging cases.

In Li et al. [7], a domain based frame-work for address configuration of MANET (DACF) is proposed. It improves auto-configuration performance by assembling nodes into domains. Domain in this scheme is a weak structure that is nodes may roam to different locations after they are configured in one domain. Initially node will be in NO_ADDRESS_STATE. After getting IP it goes to NORMAL_STATE, after that it performs MANET_DAD for address conflicts, if conflict is detected then it goes to NO_ADDRESS_STATE otherwise it remains in NORMAL_STATE. There are two types of nodes in it, Client and Server. DACF uses the same virtual address space as used PACMAN. Virtual address length is the length of IP minus the prefix. DACF divides an address into inter ID and intra ID. Inter ID is the prefix of domains and intra ID discriminate dissimilar nodes in the same domain. Inter ID is generated by probabilistic algorithm. Conflicts can be solved by sending address conflict notification messages. This attains lower conflict probability and may have slight communication overhead while broadcasting.

Gammar et al. [8] suggested an addressing scheme (DAA), in which address allocation is the duty of the configured nodes. Nodes are separated into two categories, configuration agent and simple node. Configuration agent is used to allocate an address to a requester and to guarantee its uniqueness. Every agent has to maintain a free address space. Simple node is an intermediate node, and used when there is no direct contact between the new node and the agent. Network initialization is the first process which sends address request message. Two cases may occur; either the single node alone or many nodes begin the network. If it is new, then the node configuration occurs. Network identifier change and Network merger are the procedures with the guest nodes. Address recovery is to recollect the addresses departed nodes from the network. First agent checks whether neighbor recorded the received advertisements, if so, it will change its state as simple node, and otherwise it will send a global addressing space request message for part of the space. This protocol provides solution for network partitioning and merging.

Fernandes et al [9] suggested a light-weight protocol (FAP) that configures nodes based on a distributed address space stored in filters. Network initialization is the first process to be done and after that each node begins broadcasting periodic hello messages with its filter signature. A node ingress procedure consists of three nodes, host node, joining node and other nodes. Host node sends hello messages to joining node and joining node sends address filter, in turn host node sends address filter then joining node sends AREQ (A) to host node, in turn host node sends it to other nodes by flooding. Network merging and node departure are also part of the procedures of FAP.

Indrasinge et al [10] proposed a conflict-free address allocation scheme (CFAA) to allocate an address to a requester and also provides solution for MANETs merging. New host address assignment can be done with the block of IPv4 private addresses. In an address first 24- bits are used for addressing and rest of 8-bits is used for MANET ID. The probability of occurrence of two MANETs with same ID is 1/256. MANETs merging is of two types, either identical MANETs merging or different MANETs. If it is the case of identical, then the first host which detects the merging will broadcast a message with a new MANET ID to all hosts belong to the MANET. If it is the merging of other type, then the larger MANET will adopt the smaller MANET. Address reclamation can be of two types, either graceful i.e., with informing the parent or abrupt that is without informing the parent or its neighbors.

Yong et al [11] suggested a dynamic address allocation protocol based on genetic algorithm (DAA-GA). It also detects merging of two or more networks and resolve duplicated addresses. Genetic algorithm is a computation model which replicates the Darwin's development process of genetic choice and natural exclusion. It uses IPv4 32-bits, in which first 8-bits for NetID and next 32-bits for host address. The NetID is created by the first node in the network and is a random value. In this scheme, MANET initialization is the first process to be done and then election of the leader and live node and then new node joining can occurs. Network portioning and merging can takes place at any time, this protocol works well in these cases especially in the case of MANETs merger.

Li et al [12] proposed a Cluster based addressing scheme for MANETs (CAA). A cluster member gets an address from a cluster head with in one-hop distance; as a result address allocation task is dispersed around cluster heads. In this way, the address allocation in different clusters can be done in parallel. Architecture of this protocol consists of five nodes. Cluster head is the node which assigns address in the same cluster. Cluster member has no responsibility of address assignment. Root node is a node which is a cluster head and can allocate an address for a cluster head. Cluster gateway is the communication area for two or more clusters. A node which is not declared as cluster member or cluster head or cluster gateway or root node is called a new node. IPv6 address is separated into four parts, MANET_ID, TREE_ID, CLUSTER_ID, and NODE_ID. Address configuration can be done by the series of request and response messages between nodes. Generation of root node, cluster head, cluster member and cluster gateway can be done by calculating the one-hop distances between nodes. Address reclamation and maintenance can be done by sending repeated update messages and acknowledgements. Network partitions and merging can be detected by MANET IDs.

In Li et al [13], spanning tree based autoconfiguration is proposed for MANETs (SAA). Spanning-tree is a logical group of connected nodes. It is built dynamically in a completely distributed fashion. Before acquiring an address, a node uses the link local or the MAC address to communicate with its neighbors. Each node keeps a list of its neighbor's link-state addresses. Requestor node sends a query message having source field and the link-local address. The nearest neighbor allocates an address to requester and all nodes will update their parent and trace back to the requester node by its parent. Address allocation can be done by dividing into different subnets. Each requestor has a PID (parent identifier) to distinguish from others and it has a subnet survey timer.

Subnet partitioning and merging can be detected by NID's (sub-network identifier).

Li et al. [14] proposed a localized addressing scheme for ad hoc networks (LaConf). All the nodes on the network border are called as addressing agents (AA) and are accountable for address assignment to new nodes. Address assignment information is maintained in AA. The geographic routing scheme, Greedy-Face-Greedy (GFG) is used for finding and defining border nodes. A central AA coordinate all address agents and also reconfigures the network whenever it detects network partitioning or merging. A new node gets its address from a nearest AA by local communication or from central AA by GFG based multi hop communication. A geographic hash table is used for duplicate detection and each address is hashed to a exclusive location in the network. It assigns addresses with low delay, but uniqueness not guaranteed and overhead also high to coordinate all border nodes or AAs.

Wang et al. [15] proposed a tree-based addressing scheme for a MANET (TBAA). The network is built as a tree based on an association relationship between adjacent nodes. At the beginning of the protocol an S value is assumed, that is the maximum number of child nodes a parent node can configure. The value of S depends on the size of the network. We can't calculate the accurate size of network at the beginning and if the density of child nodes at parent nodes is more than S value then there is no room to add new nodes. Hence this scheme is not scalable for large size networks.

Wang et al. [16] proposed a hierarchical architecture and merges the centralized and distributed approaches for address configuration in MANETs (DHAA) using IPv6 address format. A clustering algorithm is used to build the network and have four types of nodes. The cluster head assigns addresses to its member nodes in distributed fashion, cluster member acts as forwarding node, central node is an elected cluster head and assigns addresses to cluster heads in a centralized fashion and new node which is not marked as a cluster member or cluster head or central node. In this scheme, say x, y and z are integers and their values are calculated by the size of the MANET and are used for central node id, cluster head id and cluster member id respectively and (128-x-y-z) bits are used for MANET id. The new node receives H_Adv messages from cluster heads within a fixed interval and then obtains an IPv6 address from cluster head with minimum number of assigned cluster member ids. The member nodes in a cluster periodically sends M_Update message to its header and header sends M_Update_Ack to its members. If the cluster header does not received M_Update message within a fixed interval from its member then it reclaims the corresponding member address for future allocation. Like that, if the cluster member does not received M_Update_Ack message within a fixed interval from its header then it starts new header election algorithm. The cluster headers uses the same process to notify its existence to the central node and starts election process to select the new central node if it misses the acknowledgement message. It also provides the solution for network merging. In this protocol, x, y and z values are determined based on the size of the network in the initial stage. We cannot estimate the exact size of the network at the beginning, so that it fails if the number of nodes in a cluster is more than z-bits range.

## 2.2 Decentralized Schemes
In decentralized schemes, address allocation process is distributed across all nodes in the network. An agreement is made among all nodes to allocate an address to a new node in

the network and the protocols using Duplicate Address Detection (DAD) procedure falls under this category.

In strong DAD [17], weak DAD [18] and passive DAD [19] every newly joined node assigns itself with an address and its distinctiveness is verified with DAD process. If it detects replication then it selects one more address and reiterates the same process until it gets a unique address.

Mansi et al. [3] suggested a dynamic addressing method for a MANET (DAC), in which each node have a set of unused addresses. It takes the consent of all nodes when allocating an address to a new node. If a node goes away from the network, its address is recollecting back to the pool. The unexpected departure of a node cause the address loss, it employs the cyclic flooding method to recollect the lost addresses. However, this cyclic flooding method makes use of a lot of network resources.

Nesargi et al. [20] proposed a decentralized scheme called as MANETconf, in which a distributed common allocation table is used for address assignment. To obtain an address, the new node selects one of its neighbor nodes as proxy node. The proxy node selects an address from its address table and sends a message to all nodes in the network. In response to this message, all nodes check the selected address in their local address tables and if it is free, mark it as allocation pending and sends an allocate reply to the proxy node. If the proxy node receives all allocate reply messages then allocate selected address to new node and sends confirmation message to all nodes in the network. If the proxy node receives at least one non-allocate reply message then it discards the selected address and repeat the same process by selecting another address. This process is repeated for a finite number of times to assign an address to a new node. In this scheme, network merging is detected when a node receives the packet with different network ID. When merging occurs, communicating nodes exchange their allocation tables and flood them to all nodes in their networks. The network merging causes address conflicts and these conflicts are resolved by making the node with smaller amount short-lived TCP connections should obtain a new IP address.

Ozturk et al [21] proposed a scalable distributed address allocation scheme for ad-hoc Networks (SDAA). It presents a dynamic address assignment scheme along with hierarchical cluster network architecture. A network consists of clusters and each cluster has a head and other nodes. Each network has a root node and acts as a gateway between the ad-hoc network and external network, such as internet or intranet. An IP address is assigned through DHCP or IPAA for a root node. Every node has a permanent global unique address, which is used for external communication and for communication within a MANET, dynamically assigned addresses are used. Global unique addresses are represented by capital letters and six byte global unique addresses are developed with IEEE 48 bit MAC address space. Root node is the first node in the network and will also become cluster head and with a dynamic address as 01: FE. 01 represents the network ID and FE represents the node ID. All cluster heads has XX: FE format address, where XX is the network ID assigned by the root node. XX: FF and XX: 00 are reserved for network wide broadcast. Network address and node address together form eight bits such that 256 network cells and a maximum of 254 nodes in each network cell. Thus each node is addressed by 16 bit.

Luis et al [22] proposed Distributed Dynamic Host Configuration Protocol (D2HCP) for MANETS. It uses

optimized link state routing (OLSR) table driven routing protocol for synchronization and address uniqueness is guaranteed under a variety of network conditions, including network splits and message losses. Data structures of this protocol handle both auto-configuration and OLSR routing mechanisms. For auto-configuration free IP blocks available field should be mandatory. Node joining procedure involves discovery, offer and count, ready and local variables. Synchronization is the job of recollecting the IP addresses of nodes that depart the network without notice and makes them available to other nodes by attaching to the right of the free block. By separating the unused addresses in two blocks, one of them will be delivered to a new node that joins the network, the node which receives a address block act as server and other nodes act as client nodes or relaying nodes.

Chen et al [23] proposed a Ring-based Address Auto-configuration (RAA) for MANETS. In this scheme, each node autonomously allocates subset of IP addresses to new nodes and does not require the duplicate address detection procedure during the address allocation process. RAA protocol verifies the amount of TCP connections and amount of nodes to allow duplicate nodes to re-join the network partitions, so that lost nodes are re-entered. In RAA, there are five node states. Initial, a new node waiting for a vacant address block. Stable is the state when node gets an identity. Merge, when merging of networks takes place. Holder is the state if the node leaves the network and other nodes selects its address. Finish is the state if the node leaves the network. Address resources are uniformly dispersed for each node in the network. RAA suits for small and normal scale MANETs.

Hsu et al. [24] suggested an addressing scheme, called prime DHCP (PDHCP). This scheme does not require DAD to allocate addresses to newly joining nodes. Using a PNAA (prime numbering address allocation) each node acts as a DHCP proxy to calculate a unique address for new nodes. PNAA uses canonical factorization theorem that is every positive integer can be written as a product of prime numbers to generate addresses. Proxy node allocates prime numbers in rising order. Non root nodes can assign prime numbers in address equal to its own address multiplied by the unused prime number, starting from the largest prime factor of its own address. The address recovery issue is not discussed. The DHCP proxy requests its predecessor node to execute the address assignment process, if the address pool of a DHCP proxy runs out. In this case the address allocation cost is amplified and the latency is extended.

Hussain et al. [25] proposed a scalable a scalable address configuration scheme for MANETs (SAAMAN). A new node configures itself with an address and its uniqueness is verified with all Duplicate Address detection Servers (DDS). A node which offers duplicate address detection service is called a DDS. It uses geographic forwarding mechanism to select the routes and DDS nodes. The duplicate address detection servers are distributed across the network. A duplicate address detection server maintains a table called Duplicate Detection Table (DDT), which contains the addresses of its neighbor nodes. A new node sends its address to its neighbor DDS, which in turn sends this address to all DDS severs to verify its uniqueness. If there are multiple DDS servers for the selected address then the new node discards the selected address and repeats the process with another address. It is suitable for large scale networks but lot of overhead is incurred in synchronizing the duplicate detection servers.

## 2.3 Centralized Schemes

In centralized schemes, a central entity, called as leader or server in the network is accountable for address assignment. This central entity maintains all the information related to address configuration. These schemes have high overhead in maintaining central entity and also if it fails, the total system collapses.

Günes et al [26] proposed a Centralized Autoconfiguration protocol (CAC) which uses a centralized allocation table for address allocation of new nodes. In this scheme, a single node is dynamically elected as a leader and it will maintain the list of all nodes and their addresses in the network. In this scheme each node will be in one of three states: address agent, unbound and bound. A node is said to be in unbound state, if it does not have a valid IP address. A node changes to a bound state, if it receives a valid IP address from the address agent. The network maintains only one address agent (leader) and an unbounded node enters into this state when it does not find a node from which it wants to get an address. It waits for a fixed period of time and then declares itself as an address agent and self assigns an address and is responsible for allocating addresses to new nodes. The address agent senses its presence by sending periodic agent live messages and collects leak addresses from the reply messages of live nodes. If the bounded nodes do not hear a periodic agent live message then the leader election mechanism is used to elect a new agent. Network merging took place when the network have more than one address agent. The address agent who has the lowest MAC address will be the new address agent and it combines all address tables and resolves the address conflicts.

In S. Toner et al. [27] suggested self-organizing node address management in ad-hoc network (SOAM), in which a sole node called as leader is accountable for assigning addresses to new nodes. A newly joined node sends a request for an address. A neighbor node called as agent in new node transmission range forwards the message to leader and gets an unused address and allocate it to new node. The leader node uses periodic flooding mechanism to maintain its address tables and to collect address leaks, so that the cost is high.

Al-Mistarihi et al. [28] suggested a tree based dynamic addressing protocol (T-DAA). The topology of the network is built as a tree and classifies the nodes as a leader node, a normal node and a root node. If a new node does not find a leader node in its transmission range then uses normal node as a pass on node to send the messages to leader node. The leader nodes have the disjoint unused addresses and assign them to newly join nodes. The network has only one root node, and it maintain the information about all leaders and their address pools. The root node is also answerable for address recovery and network merger. In this protocol, if the address space tires out at any leader node or the root node fails, then the control overhead and address delay is increased.

## 3. PERFORMANCE COMPARISON
## 3.1 Performance Metrics

Following are the metrics used for the evaluation of autoconfiguration protocols.

- *Uniqueness:* An addressing protocol must assign a unique to each node in the network because conflict addresses can cause severe routing problems.

- *Latency:* The period of time from beginning of address assignment process till its completion.

- *Overhead*: The amount of control packets exchanged in the process obtaining an address.

- *Scalability*: The addressing scheme must be scalable. i.e. the performance of the protocol will not be degraded if the size of the network increases.

## 3.2 Performance Comparison

This section presents the performance comparison of the above discussed protocols in terms of performance metrics.

The neighbor based schemes have better performance in terms of address uniqueness, latency and overhead, but poor in scalability. Another serious problem with neighbor based schemes is, if the network has uneven density then overhead and latency are drastically increases.

The decentralized schemes have better performance in terms of overhead and scalability, but poor in latency. The protocols weak DAD and passive DAD do not ensure address uniqueness and also depend on routing protocols.

The centralized schemes ensure address uniqueness and less latency, but high overhead in maintaining central server.

These schemes suffer with single point (server) of failure and their performance will be degraded as the size of the network increases.

The performance comparison of address auto-configuration protocols in terms of performance metrics is shown in Table 1.

## 4. CONCLUSION

Allocating addresses in Mobile Ad Hoc Networks is a challenge task due to random mobility of nodes and lack of infrastructure. In this paper, the need of address autoconfiguration and the brief description of various addressing protocols and their pros and cons were presented. It defines various performance metrics and also a comparison table of different address auto-configuration protocols is presented with regard to these metrics. This paper concludes that there is no single protocol satisfying all the performance metrics and further research is needed in this area.

**Table 1. Comparison of address auto configuration protocols**

| Category | Protocol | Uniqueness | Latency | Overhead | Scalability |
|---|---|---|---|---|---|
| **Neighbor based schemes** | Prophet | No | Low | Medium | Yes |
| | Buddy | Yes | Medium | Medium | No |
| | DACF | Yes | Medium | Medium | Yes |
| | DAA | Yes | Low | Medium | No |
| | FAP | Yes | Low | Medium | No |
| | CFAA | Yes | Low | Medium | No |
| | DAA-GA | Yes | Low | Medium | No |
| | CAA | Yes | Low | Medium | No |
| | SAA | Yes | Medium | Low | No |
| | LaConf | No | Low | Medium | No |
| | TBAA | Yes | Low | Low | No |
| | DHAA | Yes | Low | Medium | No |
| **Decentralized schemes** | SDAD | Yes | High | High | No |
| | WDAD | No | Low | Medium | No |
| | PDAD | No | Low | Medium | No |
| | DAC | Yes | Medium | High | No |
| | Manetconf | yes | High | High | No |
| | SDAA | Yes | Medium | Medium | Yes |
| | D2HCP | Yes | Low | Low | No |
| | RAA | Yes | High | Low | Yes |
| | PDHCP | No | Low | Medium | No |
| | SAAMAN | Yes | High | Medium | Yes |
| **Centralized schemes** | CAC | Yes | Medium | High | No |
| | SOAM | Yes | Low | High | No |
| | TDAA | Yes | Medium | Medium | No |

## 5. REFERENCES

[1] Droms, R. 1997. "Dynamic host configuration protocol". Network working group, IETF, RFC 2131.

[2] Thomson, S., Narten, T. and Jinmei, T. 2007. "IPv6 address autoconfiguration". IETF, RFC 4862.

[3] Thoppian, M.R. and Prakas, R. 2006. "A distributed protocol for dynamic address assignment in mobile ad hoc networks". IEEE Transactions on Mobile Computing, 5(1), 4-16.

[4] Kim, S., Lee, J. and Yeom, I. 2008. "Modeling and performance analysis of address allocation schemes for mobile ad hoc networks". IEEE Transactions on Vehicular Technology, 57(1), 490-501.

[5] Zhou, H., Ni, L. M. and Mutka, M. W. 2003. "Prophet address allocation for large scale MANETs". Ad Hoc Networks, 1, 423–434.

[6] Mohsin, M. and Prakash, R. 2002. "IP Address Assignment in a Mobile Ad Hoc Network". In Proceedings of IEEE MILCOM 2002, 2, 856-861.

[7] Li, L., Cai, Y. and Xu, X. 2009. "Domain-based autoconfiguration framework for large-scale MANETs". Wireless Communications and Mobile Computing, 9 (7), 2938–947.

[8] Gammar, S. M., Amine, E. and Kamoun, F. 2010. "Distributed address autoconfiguration protocol for Manet networks". Telecommunication Systems, 44 (1), 39–48.

[9] Fernandes, N. C., Moreira, M. D. D. and Duarte, O. C. M. B. 2013. "An Efficient and Robust Addressing Protocol for Node Auto-Configuration in Ad-hoc Networks". IEEE/ACM Transactions on Networking, 21(3), 845-856.

[10] Indrasinge, S., Pereira, R. and Haggerty, J. 2009. "Disjoint Conflict Free Address Auto-Configuration for Mobile Ad-hoc Networks". In Proceedings of IEEE NBIS 2009, 343-349.

[11] Yong, L., Ping, Z. and Jiaxiong, L. 2009. "Dynamic Address Allocation Protocols for Mobile Ad-Hoc Networks Based on Genetic Algorithm". In Proceedings of IEEE WiCom 2009, 1-4.

[12] Li, L., Cai, Y. and Xu, X. 2009. "Cluster-based and Distributed IPv6 Address Configuration scheme for MANET". Wireless Pers Comm., 49, 561-573.

[13] Li, L., Cai, Y. and Xu, X. 2007. "Spanning-tree based auto-configuration for mobile ad-hoc networks". Wireless Pers Commun, 43, 1465-1477.

[14] Li, X., Deng, Y., Nayak, A., Stojmenovic, I. and Narasimhan, V. 2011. "LaConf: A localized address autoconfiguration scheme for wireless ad hoc network". Tsinghua Science and Technology, 16(5), 529-538.

[15] Wang, X. and Qian, H. 2014. "A Tree-based address configuration for a MANET". Int. Journal of Pervasive and Mobile Computing, 12, 123-137.

[16] Wang, X. and Qian, H. 2015. "Dynamic and hierarchical IPv6 address configuration for a mobile ad hoc network". Int. J. Commun. Syst., 28, 127-146.

[17] Perkins, C., Malinen, J. T., Wakikawa, R., Belding-Royer, E. M. and Sun, Y. 2001. "IP address auto-configuration for ad hoc networks". IETF Draft.

[18] Vaidya, N. H. 2002. "Weak duplicate address detection in mobile ad hoc networks". In Proceedings of ACM MobiHoc 2002, 206–216.

[19] Weniger, K. 2003. "Passive duplicate address detection in mobile ad hoc networks". In Proceedings of IEEE WCNC 2003, 3, 1504-1509.

[20] Nesargi, S. and Prakash, R. 2002. "MANETconf: Configuration of hosts in a mobile ad hoc network". In Proceedings of IEEE INFOCOM 2002, 2, 1059–1068.

[21] Ozturk, Y. and Nagarnaik, V. 2011. "A Scalable Distributed Dynamic Address Allocation Protocol for Ad-hoc Networks". Wireless Network, 17, 357-370.

[22] Luis, J. G. V., Julian, G. M., Ana L. S. O. and Jose, D. M. D. 2011. "Distributed Dynamic Host Configuration Protocol (D2HCP)". Sensors 2011, 11, 4438-4461.

[23] Chen, Y., Lin, T. and Lin, S. 2007. "RAA: A ring-based address auto-configuration protocol in mobile ad-hoc networks". Wireless Pers Coommun, 43, 549-571.

[24] Hsu, Y. and Tseng, C. 2005. "Prime DHCP: a prime numbering address allocation mechanism for MANETs". IEEE Communications Letters, 9 (8), 712–714.

[25] Hussain, S. R,, Saha, S. and Rahman, A. 2011. "SAAMAN: Scalable address autoconfiguration in Mobile Ad Hoc Networks". J. Netw. Syst. Manage., 19(3), 394-426.

[26] Günes, M. and Reibel, J. 2002. "An IP address configuration algorithm for zeroconf mobile multihop ad hoc networks". In Proceedings of Intl. Workshop on Broadband Wireless Ad Hoc Networks and Services 2002, 1–11.

[27] Toner, S. and O'Mahony, D. 2003. "Self-Organising node address management in Ad hoc networks". Lecture Notes in Computer Science, 2775, 476-483.

[28] Al-Mistarihi, M. F., Al-Shurman, M. and Qudaimat, A. 2011. "Tree based dynamic address autoconfiguration in mobile ad hoc networks". Computer Networks, 55(8), 1894-1908.