Print ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Address Auto-Configuration in Self Organizing Mobile Ad Hoc Networks: Requirements and Performance Metrics - A Survey

Sumathy S*, Ram Sri Kumar P
School of Information Technology and Engineering, VIT University, Vellore, India- 632 006
***Corresponding author: E-Mail: ssumathy@vit.ac.in, Mobile number: 9865481293**

ABSTRACT

Address configuration and allocation to various devices participating in communication is a key challenge in wireless mobile ad hoc networks due to the absence of specialized servers to dynamically assign addresses. Infrastructure less nature and dynamic topology of such networks lead to major concerns such as routing, security, QoS, address auto-configuration, reliability and scalability. Address auto-configuration protocols perform the tedious task of assigning unique addresses to every node participating in the network taking into consideration the issues prevailing when nodes carry duplicate addresses. They also provide support during network partitions and merges. Assigning address to a new node participating in the network may require broadcasting probes to reflect the status of the acquired addresses with the rest of the nodes in the network. However, it is observed that broadcasting leads to communication and computational overhead, require more storage space, experience latency and delay which in turn may affect the network's overall functionality and thereby the performance. Existing approaches are analyzed to illustrate the overheads prevailing in address auto-configuration and its protocols with respect to design, addressing mechanism, and performance metrics, with a perspective to provide an overview of various design choices to be considered in relevance to the requirement factors applicable to real time scenarios.

KEY WORDS: Auto-configuration, Stateful address allocation, Stateless address allocation, Network partition, Network merges.

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a multi-hop infrastructure less network, where nodes rely on their neighbor nodes to forward data to the destination node. In general, transmission reliability, convergence time and scalability factor affects the performance of the network. IP based address is assigned to a new node joining an infrastructure based network by Dynamic Host Configuration Protocol (DHCP) and the address is released when the node leaves the network. Such centralized address assignment cannot be extended to MANET due to its dynamic topology where nodes join or leave the network randomly. This also leads to few other functional characteristics such as merging support, partitioning and prefix delegation which is required to be addressed emphasizing the need of an auto address configuration protocol. They assign unique addresses to the mobile nodes joining the network and resolve duplicate address assignment conflict dynamically. However, such protocols incur certain overhead in terms of signaling, which needs to be taken into consideration as it has an impact on the performance of the network significantly. Similarly, other factors such as robustness which accounts for unreliable physical layer and scalability factor is also required to be considered.

Ability to perform effective communications through the wireless medium without centralized coordination requires tremendous amount of organized functionality among the participating nodes. Although, ad hoc networks are easily deployed, configuring the nodes to function intelligently is a daunting task. In real time networking scenarios, unforeseen circumstances which when not considered while configuration usually tend to bring down the network. No matter how efficiently the configurations have been done, in a long enough time scale, nodes are prone to malfunction. However, for any sort of worthy data communication to happen, nodes must be given unique identities. Address uniqueness involves re-use or reclamation of addresses and other resources.

2. METHODS & MATERIALS

MANET Characteristics and Requirements: Dynamic topology, error prone medium and mobility support tend to effect variable changes in the functionality and structure of MANET. Challenge is to ensure that this does not compromise the ongoing communication. For the network to perform in a stable state, certain conditions and requirements must be met. In accordance with specific MANET scenario and node characteristics, address autoconfiguration mechanisms with different functionalities must be designed to meet the needs and address the network constraints. Autonomous networks of ad hoc nature that are not connected to any external network through a gateway or centralized server are said to be standalone MANET, since all communication happen within the network. Whereas, those ad hoc networks that are connected to the external network like the Internet through a gateway are connected MANETs. Accordingly, addressing techniques must account for the data transmission without protocol compatibility issues across the networks which might have deployed different addressing protocols. This is an important factor to be considered while designing the protocol. Few such characteristics are; Mobility, Address Uniqueness, Partitioning and Merging Support, Robustness, Scalability, Duplicate Address Detection, Routing Protocol Dependency, Network Flexibility, Prefix Assignment, Decentralized Nature.

Routing protocols are usually designed independent of the underlying addressing mechanism. An address auto-configuration protocol designed specifically to enhance or assist in the performance of a particular routing protocol may not adhere to the requirements of other independent routing protocols. There is no specific addressing protocol which is capable of meeting the demands of any dynamic network scenario. Protocols are designed to satisfy certain demands pertaining to specific network scenario with variable attributes. Before deploying the network, the addressing protocol must be selected after considering the network requirements and its behavior. Unlike various IP address based networks such as IPv4 or IPv6, there are no servers running Dynamic Host Configuration Protocol (Droms, 1997; Volz, 2006) to take care of addressing all the nodes in self-organizing networks. Hence, an address auto-configuration protocol needs to take care of assigning unique address to all the nodes in the network, account for the dynamic nature of their presence in the network, resolve the issue of nodes carrying duplicate addresses, and provide support for network partition and merge. Wang and Qian, (2015), have proposed a dynamic and hierarchical IPv6 addressing mechanism considering both distributed as well as centralized address configuration schemes. The cluster head performs the unicast communication and also addresses the network partitioning and merging issue without collision.

In traditional broadcast based communication, each node has to employ neighbor discovery methods to identify the nodes in the range further to which the packets are forwarded to all the nodes in the vicinity. This leads to more redundancy as there is a possibility for the nodes to receive the same packet separately from different nodes in its range. When an address is assigned to a new node joining a partitioned network, there are considerable chances for the new address to become a duplicate address subsequently when the network merges. This may lead to duplicate address assignment. In general, auto-configuration based addressing protocols can be categorized as routing protocol dependent protocols, routing protocol independent protocols and protocols that utilize information from routing protocol. Pre-sensitive DAD, In-sensitive DAD and DAD free mechanisms are proposed in existing literature.

Existing Address Auto configuration Protocols: Mobile ad hoc networks do not rely on any fixed infrastructure and hence does not require any explicit address configuration in dynamic address assignment (Sun, and Belding-Royer, 2004). Address auto-configuration protocols are majorly classified as stateful, stateless and hybrid protocols. In case of stateful protocols, each node in the network maintains an address allocation table corresponding to the logical addresses of all other nodes. Hence, stateful protocols are also termed as conflict free protocols. However, maintaining the consistency of the allocation table is a challenge in dynamic networks where networks split and merge frequently. Nodes following stateless auto-configuration protocols do not record any information of address allocations of other nodes except for its own.

Stateless protocols follow trial and error method to detect unique address which is available for allocation. Hence they are also called as conflict detection protocols. The nodes perform duplicate address detection (DAD) on a randomly chosen address to avoid duplicate addresses assignment (Garcia Villalba, 2011; Xiaonan and Shan, 2013; Moore, 2006). Authentic exchange of the credentials while resolving duplicate addresses using auto address configuration protocols is also an important criterion. While supporting partitioning and merging of the networks, it becomes essential to propose solutions to avoid IP address conflicts. Mohsin, and Prakash, (2002), have defined a binary split idea such as a buddy system which efficiently manages the network partitioning and merging on assigning unique partition ID. Address to a new node joining the network is assigned either using an agreement protocol which ensures unique address assignment or with a mutually exclusive set of addresses.

Tayal and Patnaik (2004) have discussed on a distributed unique address assignment scheme where minimal overhead in terms of reduced broadcast messages are focused. An analytical model to evaluate the efficiency of certain address allocation schemes is proposed by Kim (2008), to derive the efficiency in terms of overhead due to communication and the packet loss parameter. The mathematical model proposed holds good to analyze the efficiency of MANETconf and various neighbor based routing protocols. A fundamental requirement of any addressing protocol is to avoid duplicate addressing. Few protocols function in such a way that they do not require additional check for the presence of duplicate nodes. Such protocols are DAD free and they avoid all overheads involved in the process of detecting duplicates (Perkins, 2001). For application specific networks, choosing an auto-configuration protocol that synchronizes well with the implemented routing protocols may increase the performance considerably and reduce the redundant operations which may otherwise be employed (Mase, 2006). Few scenarios may call for address configuration that is independent of any routing protocol. The ability to support IPv6 prefixes to the nodes participating in the network can be considered to extend the compatibility (Wang and Qian, 2015).

Stateful auto-configuration protocols: Stateful address allocation protocols can be classified as local and global. Since the proposal of MANETconf by Nesargi and Prakash, (2002), and Prophet Address allocation in Zhou, (2003), various stateful addressing protocols such as RSVconf (Bredy, 2006), EMAP (Ros, 2006), LHA (Yousef, 2007), D2HCP (Garcia Villalba, 2011) and OSA (Al-Mahdi, 2013) have been proposed and largely implemented. MANETconf (Nesargi and Prakash, 2002) follows a mutual exclusion algorithm using agent based distributed agreement process which maintains two tables where the address pending table maintains the nodes that have been

initiated with an address but have not confirmed any address and address allocated table that maintains all the addresses that have been allocated. A node selects an address for the requesting node which is not present in both of its tables. It then floods the network with a request message to confirm the address allocation. All nodes acknowledge positively on receiving this request message if the address is not found in their table, otherwise acknowledge negatively. Since all nodes must respond with a reply to the initiator node regardless of address duplication, it incurs high overhead in terms of more bandwidth consumption. The whole process of initiation and flooding must be repeated even if a single negative acknowledgement is received by the initiator. This broadcasting request consumes more bandwidth across nodes in the network. Moreover, a node has to wait until it receives a unicast reply from all the nodes in MANET. A conflict free address distribution scheme termed Prophet Address Allocation is proposed by Zhou (2003), where a specific function maintained by a node generates new addresses in relevance to its state. The initial address of the first node in the MANET is randomly chosen along with a random seed for the function which becomes the prophet for the MANET. On arrival of new nodes, the prophet node generates a new IP address and updates its state. Thus, the prophet node in the network is empowered to generate a random seed for a new node becoming a part of the network and hence avoids duplicate address assignment. Due to the use of one hop broadcasting for establishing communication between the new node and the configured node, message overheads are very low. This scheme ensures unique and short address allocation time, moderate conflict detection, maintenance of the state information with reduced latency in a scalable network.

RSVconf protocol (Bredy, 2006), supports MANET which involves nodes with high mobility where frequent and quick merging and partition of the network occurs. A new node broadcasts proxy requests searching for a suitable proxy node that could assign an address. Proxy nodes maintain an IP database from which free IP addresses are selected for new nodes. Also, a reservation message is broadcasted to all the nodes in the network. On receiving the reservation message, each node checks for the presence of that particular IP in its database. If a conflicting match is found, the node sends a response back to the proxy node, otherwise it registers that particular IP as allocated in its database. This protocol does not allow merging multiple networks simultaneously. This may lead to formation of numerous single node networks. Moreover, RSVconf allows only two networks to merge at a time, hence, merging all the available single node network becomes tedious and leads to very high merger overheads. Unlike Prophet Address Allocation scheme, in distributed dynamic host configuration protocol (D2HCP, Garcia Villalba, 2011), any node in the network can assign half of its address range to the new joining node. Free addresses available with the nodes are determined by OLSR routing protocol. Auto configuration is performed locally with the neighbor nodes on exchanging control packets. D2HCP provides scalability with minimum overhead in large networks. Duplicate address conflict arises as addresses are generated and assigned randomly in MANET. Weniger (2003), has proposed a passive duplicate address detection mechanism (PDAD), upon monitoring the traffic while routing data in a passive mode. Fisheye and OLSR routing protocols are applied for routing traffic in a moderately dense network. Both the routing protocols prove efficient in addressing the duplicate address conflict.

Stateless auto-configuration Protocols: Stateless protocols may function requiring the use of MAC addresses or without it. Simple DAD (Perkins, and Malinen, 2001), AROD (Kim, 2007), and AIPAC (Fazio, 2006) do not require the use of MAC addresses. IPv6 SAA (Narten, 2007), and ND++ Grajzer (2014), presents an extended neighbor discovery protocols which rely on the usage of MAC address. Nodes usually follow a naive approach of randomly choosing an address followed by duplicate address detection to check for the existence of duplicates. Perkins and Malinen, (2001), have proposed a simple Duplicate Address Detection (DAD) methodology to flood the network with an address request when a new node joins a network. Similar to Zero Conf protocol, the new node selects a random address on the network. Duplicate address detection is essential as this does not guarantee unique address when network partition and merging occurs further. This simple DAD scheme facilitates a new node to randomly select an address and broadcast the address and wait for certain duration. A reply from other nodes within the interval suggests that the address has been allocated already which forces the new node to select another random address.

To overcome the drawback of longer address allocation process and more communication overhead, Kim, (2007), have proposed a distributed address configuration protocol based on address reservation mechanism AROD, where each node in the network reserves an IP address in advance so that they can effectively assign new nodes with the reserved addresses followed by DAD to ascertain its uniqueness. Applying optimistic DAD effectively reduces the communication overheads and latency while allocating the reserved address to a new node joining the network. Since the number of broadcast is minimal, address assignment is done quickly. Fazio, (2006) have proposed a new stateless protocol termed AIPAC, which assigns unique Net ID for each MANET apart from unique Node ID for the nodes and reduces lot of references among nodes and addresses the issue of partitioning and gradual merging effectively. Narten, (2007) discuss on a stateless auto configuration mechanism (IPv6 SAA) to configure the hosts and routers without relying on any server. This scheme allows a node to generate its own address combining both the interface identifier and the prefix of the subnet ID. Duplicate address detection is performed further to detect duplicate addresses if any is assigned. Grajzer, (2014) have proposed an extended IPv6 protocol (ND++) for

discovering the neighbors to improve the duplicate address detection mechanism efficiently. They have deployed a multipath relay procedure on utilizing the flooding mechanism to achieve better address auto-configuration in MANET.

Heirarchical auto-configuration protocols: Hierarchical addressing provides means to optimize the redundancy involved in broadcast communication by establishing a spanning tree while addressing nodes prior to applying any routing protocols for the network. Also, unlike other address auto-configuration protocols, this addressing method carefully avoids the problem of flooding the network with address update packets for obtaining an address on checking for presence of duplicate addresses. Al-Mistarihi, (2011) have proposed a tree based dynamic address auto configured protocol (T-DAAP) where the nodes are divided as root, leader and normal nodes. Leader nodes are responsible for assigning addresses to new nodes joining the network. Root node maintains the information required by other leader nodes to know the status which resolves the duplicate addresses while the network partition and merge later. The proposed scheme incurs minimum bandwidth as it follows unicast transmission. An extended IPv6 with stateless neighbor discovery for performing address auto configuration is proposed and discussed by Weniger and Zitterbart, (2002). Landmark nodes similar to leader nodes announce their presence to the entire network and coordinate in assigning unique addresses. Hierarchical approach is used to discover the neighbor nodes efficiently.

Security in address auto configuration: Wang (2005), have proposed a secure self-authentication based Address Auto-configuration mechanism for Mobile Ad Hoc Networks to bind the IP address with a public key enabling a node to self-authenticate in order to prevent the nodes being attacked. The binding is performed over the IP addresses which may be extended and applied to a random address generated to dynamically assign address to a new node joining the network. This approach prevents denial of service and negative reply attacks, but it is susceptible to resource consumption attack as many credentials are involved in the authentication process during the key generation.

Hybrid auto-configuration protocols: DHCP is used to allocate IPv4 addresses to nodes dynamically when they become a part of the network. Ancillotti, (2009), have proposed extensions to DHCP termed AH DHCP to assign dynamic addresses to the new nodes joining the multi-hop ad hoc network extended as a WLAN. The proposed auto configured address assignment protocol integrates wired and ad hoc wireless technology reducing the overheads such as configuration delay considerably.

Network Scenario: Addressing mechanisms can be categorized based on various criteria since not every protocol would strictly fall under a specific category. Protocols are crafted specifically to adhere to a set of standards and are set to satisfy the required conditions to be characterized accordingly. Among these available categories of protocols, a particular choice is made by identifying the nature of the application for which the network is deployed. Pure MANETs are not connected with any other external networks, hence they are also known as standalone MANETs. In standalone networks, the traffic generated by the nodes are contained within the MANET and are not carried to the external environment. Since, these networks are isolated, they do not have to follow any addressing mechanism or nomenclature pertaining to global networks. Hybrid or connected MANETs have some sort of connectivity to one or more networks that are external to the current network (Templin, 2010). They agree upon certain standards to communicate between them without affecting any of their internal networks. They will have specific protocols for intra-network communication and a commonly agreed protocol for inter-network communication. Such networks usually employ gateways to support inter-networking.

Issues in Address Auto-Configuration:

Signal Overheads: Communication as information exchange through control or management packets happen quite often in order to maintain the coordinated functionality of the network which leads to overhead in the traffic.

Processing Complexity: Apart from the task of relaying, nodes have to perform various subroutines to ensure smooth traffic flow. Hence, nodes are configured with intelligent behavior which requires heavy processing to adhere to the protocol's requirements.

Security: Wireless medium is openly accessible and information transferred is crudely encrypted to prevent from intended packet captures. Any malicious node can participate imitating as a genuine node since most nodes can self-authenticate and hinder the smooth data transfer.

Convergence Time: The time duration the network takes to address all nodes successfully since its initiation is the convergence time. When networks scale, time for convergence increases as well. Various factors affect the convergence time, mostly delayed due to the control overheads.

Address Space: Address space does not matter to the network if it is standalone since all nodes will be adhering to the same conventions. If the network is hybrid in nature and employs multiple protocols, address space becomes a major issue. Inter-operability and compatibility with other network devices becomes difficult to manage in such networks.

Integration with External Networks: When there is a need to extend the boundaries of communication, devices involved must be able to understand each other's protocol to interact.

3. RESULTS

Comparative Analysis of Address Auto-Configuration Protocols: The analysis provided in table.1, is performed based on certain characteristic such as the dependency on a particular routing protocol, support for merging, prefix assignment. Table II provides few protocols and functions as standalone networks. Routing Protocol Dependency is experienced by certain protocols whereas protocols proposed by Perkins (2001); Weniger (2002); Jeong (2003); Moushin (2002); Tayal (2004); Zhou (2003) are independent of the routing protocol used with respect to the stand alone networks. Likewise, Wakikawa (2002); Hoffman (2006); Fazio (2006); Ahn (2009); Lee (2009); Boot (2009); Jelger (2005); Templin (2010); Bernardos (2006) have proposed protocols which are independent of the underlying routing protocols for connected networks. Similarly, with respect to protocols that support connected external networks, few protocols are independent of the routing protocols (Wakikawa, 2002; Hofmann, 2006; Ahn Lee, 2009), while few are dependent on the underlying routing protocols (Adjih, 2005; Ruffino 2006) as given in Table.3. Merging support is provided by certain protocols while others do not. However, overheads prevail in terms of more broadcasts and flooding.

It is observed that most of the protocols presented support merging of the network, while few support partial merging and the rest do not support merging. Similarly, the provision to assign prefix to the addresses is not feasible in many, while few support them. The overheads in terms of duplicate detection and flooding are still experienced by most of the existing protocols.

Table.1. Analysis of various parameters in address auto-configuration

Authors	MANET Type	Routing Protocol Dependency	Address Uniqueness	Distributed/ Centralized	Merging Support	Prefix Assignment	Overheads by Flooding
Perkins, and Malinen, (2001),	Standalone	Independent	Duplicate Address Detection (DAD)	Distributed	No	No	Yes
Weniger, and Zitterbart, (2002)	Standalone (extendable)	Independent	Non-unique Address Detection (NAD)	Distributed (contains leader nodes)	Yes	No	Yes
Mohsin, and Prakash, (2002)	Standalone	Independent	Doesn't require detection	Distributed	Yes	No	Yes
Tayal and Patnaik (2004)	Standalone	Independent	Doesn't require detection	Distributed	Yes	Possible	Yes
Weniger, (2003)	Standalone	OLSR Dependent	Detects Passively	Distributed	Yes	No	No

Table.2. Comparison of protocols that functions exclusively as standalone network

Authors	Routing Protocol Dependency	Address Uniqueness	Distributed / Centralized	Merging Support	Prefix Assignment	Overheads/ Message Flooding
Perkins (2001)	Independent	Duplicate Address Detection (DAD)	Distributed	No	No	AREQ floods
Weniger (2002)	Independent supports hierarchical structure	Non-unique Address Detection(NAD)	Distributed (contains leader nodes)	Yes	No	Yes
Jeong (2003)	Independent	Strong & Weak DAD	Distributed	Yes	No	AREQ floods for DAD
Moushin (2002)	Independent	Doesn't require detection	Distributed	Yes	No	Yes
Tayal (2004)	Independent	Doesn't require detection	Distributed	Yes	Possible	Yes

Weniger PDAD-OLSR (2003)	OLSR Dependent	Detects Passively	Distributed	Yes	No	No
Mase (2006)	OLSR Dependent	Assumes existence of NAD	Distributed	Yes	No	No
Zou (2003)	Independent	Doesn't require detection	Distributed	Yes	Yes	Very Few
Nesargi (2002)	proactive routing protocol	Non-unique Address Detection	Distributed	Yes	No	Yes (two repetitive messages)

Table.3. Comparison of protocols that support connected networks (external)

Authors	Routing Protocol Dependency	Address Uniqueness	Distributed/ Centralized	Merging Support	Prefix Assignment	Overheads/Message Flooding
Ruffino (2006)	OLSR	Doesn't use Non-unique Address Detection	Distributed. Requires gateways for IPv6 support	Partially	No	Gateway Broadcasts
Clausen (2005)	Independent, but uses OSLR	Non-unique Address Detection(NAD)	Distributed (contains leader nodes)	No	Yes	ADDR_BEACON and AREQ
Ros (2006)	Unicast	Non-unique Address Detection(NAD)	Distributed	No	Yes	DAD_REQ, GC_REQ
Wakikawa (2002)	Independent	Doesn't require detection	Distributed	No	No	Only if gateway advertisements are frequent
Hofmann (2006)	Independent	NAD	Distributed	No	Yes	High. MRAN & GW_ADV
Fazio (2006)	Independent	Doesn't require detection	Partially Distributed	No	No	Very Few
Ahn (2009)	Independent	Doesn't require detection	Partially Distributed	No	No	GW_ADV
Lee (2009)	Independent, uses routing tables.	Doesn't require detection, uses MAC address & network prefix	No Centralized Server but Distributed Gateways are involved	No	Yes	SERA messages
Boot (2009)	Independent	Traditional IPv6 approach	No Centralized Server but Distributed Gateways are involved.	No	No	BRIOs
Adjih (2005)	OLSR	Non-unique Address Detection(NAD) & Passive DAD	Distributed	Yes	No	Low
Cha (2003)	AODV, Proactive	Doesn't require detection	Gateways	Yes	No	RREQ, GW_ADV
Jelger (2005)	Independent	Doesn't use Non-unique Address Detection	Distributed	Yes	Yes	Gateways

Templin (2010)	Independent	SLAAC & DHCP mechanism	Border Routers (EBRs)	Yes	Yes	Low
Bernardos (2010)	Independent	SLAAC & DHCP mechanism	No Centralized Server	Yes	Yes	Low

4. CONCLUSION

New variations of protocols are introduced to make addressing more efficient providing hybrid network extensibility. When protocols are deployed in real networks, the conditions are extremely unpredictable and rigorous. Foreseeing or predicting the network behavior is highly impossible. The address auto-configuration protocols presented enable nodes to dynamically configure logical addresses without flooding the network with a flexible addressing nomenclature which adapts to the constantly changing structure of the MANET. Address delegation is done to detect duplicate addresses while ensuring that all nodes are uniquely identified. Various parameters such as overhead in communication and computation (minimal), latency(reduced), dependency on routing protocols(less), mutual authentication of address, impact due to partitioning and merging of the network in terms of performance(minimal), appropriate synchronization to ensure the configuration of the network is the key focus of the survey presented. This analysis provides a perspective of future research direction focusing on hybrid address auto-configuration and hierarchical addressing protocols which helps in effectively avoiding the broadcast storm problem.

REFERENCES

Adjih C, Jacquet P, Laouiti A, Muhlethaler P, Address auto configuration in Optimized Link State Routing Protocol, draft-laouiti- manet-olsr-address-autoconf-01, 2005.

Ahn, Sanghyun, and Yujin Lim, MANET address configuration using address pool, draft-ahn-autoconf-addresspoo, l-00, 2009.

Al-Mahdi H, Nassar H and El-Aziz S, Performance Analysis of an Autoconfiguration Addressing Protocol for Ad Hoc Networks, Journal of Computer and Communications, 1, 2013, 30-43.

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

Ancillotti E, Bruno R, Conti M & Pinizzotto A, Dynamic address auto configuration in hybrid ad hoc networks, Pervasive and Mobile Computing, 5 (4), 2009, 300-317.

Bernardos C, Calderon M & Moustafa H, Survey of IP address auto-configuration mechanisms for MANETs, IETF, draft-bernardosmanetautoconf-survey-05, Txt, 2010.

Boot, Teco and Arjen Holtzer, Border Router Discovery Protocol (BRDP) based Address Autoconfiguration, 2009.

Bredy R, Osafune T and Lenardi M, RSVconf, Node Autoconfiguration for MANETs, 6th IEEE International Conference on ITS Telecommunications Proceedings, 2006, 650-653.

Cha, Hyun-Wook, Jung-Soo Park, and Hyoung-Jun Kim, Extended support for global connectivity for ipv6 mobile ad hoc networks, Internet Engineering Task Force (IETF) draft, 2003.

Clausen T and Baccelli E, Simple manet address autoconfiguration, IETF Internet Draft, 2005.

Droms R, Dynamic Host Configuration Protocol, Network Working Group – RFC, 2131, 1997.

Fazio M, Villari M and Puliafito A, AIPAC, Automatic IP address configuration in mobile ad hoc networks, Computer communications, 29 (8), 2006, 1189–1200.

Garcia Villalba LJ, García Matesanz J, Sandoval Orozco A.L and Márquez Díaz J.D, Auto-configuration protocols in mobile ad hoc networks, Sensors, 11 (4), 2011, 3652-3666.

Garcia Villalba LJ, Matesanz JG, Sandoval Orozco AL and Marquez Díaz J.D, Distributed dynamic host configuration protocol (D2HCP), Sensors, 11 (4), 2011, 4438–4461.

Grajzer M, Zernicki T and Głąbowski M, ND++–an extended IPv6 Neighbor Discovery protocol for enhanced stateless address autoconfiguration in MANETs, International Journal of Communication Systems, 27, 10, 2014, 2269–2288.

Hofmann P, Multihop radio access network (MRAN) protocol specification, draft-hofmann-autoconf-mran-00, 2006.

Jelger, Christophe, and Thomas Noel, Proactive address autoconfiguration and prefix continuity in IPv6 hybrid ad hoc networks, SECON, 2005.

Jeong J, Kim H, Jeong H, Kim D, Park J, Ad Hoc IP Address Auto configuration draft-jeong-adhoc-ip-addr-autoconf -06.txt, Internet- Draft, 2003.

Kim N, Ahn S and Lee Y, AROD, An address auto-configuration with address reservation and optimistic duplicated address detection for mobile ad hoc networks, Computer Communications, 30 (8), 2007, 1913–1925.

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

Lee J, Ahn S, Yu H, Kim YS & Jin JS, Address autoconfiguration and route determination mechanisms for the MANET architecture overcoming the multi-link subnet model, IEEE International Conference on Information Networking, ICOIN, 2009, 1-5.

Mase, Kenichi and Cedric Adjih, No overhead auto configuration OLSR, draft-mase-manet-autoconf-noaolsr, 01, 2006.

Mohsin M and Prakash R, IP address assignment in a mobile ad hoc network, In IEEE Proceedings on MILCOM, 2, 2002, 856-861.

Moore N, Optimistic duplicate address detection (DAD) for IPv6, Monash University, 2006.

Narten T, Thomson S and Jinmei T, IPv6 stateless address autoconfiguration, 2007.

Nesargi S and Prakash R, MANETconf, Configuration of hosts in a mobile ad hoc network, Proceedings of IEEE Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, 2, 2002, 1059-1068.

Perkins C and Malinen, Akikawa J.R.W, Fielding-Royer E.B, and Sun Y, IP Address Autoconfiguration for Ad Hoc Networks, Internet Draft, IETF Working Group MANET, 2001.

Ros F, Ruiz P, and Perkins C.E, Extensible manet auto-configuration protocol (EMAP), Internet Draft, 2006.

Ruffino, Simone, and Patrick Stupar, Automatic configuration of IPv6 addresses for MANET with multiple gateways (AMG), IETF, draft-ruffino-manetautoconf-multigw-03, 2006.

Sun Y and Belding-Royer EM, A study of dynamic addressing techniques in mobile ad hoc networks, Wireless Communications and Mobile Computing, 4(3), 2004, 315-329.

Tayal AP and Patnaik LM, An address assignment for the automatic address auto configuration of mobile ad hoc networks, Personal and Ubiquitous Computing, 8(1), 2004, 47-54.

Templin, Fred L, Subnetwork Encapsulation and Adaptation Layer, 2010.

Volz B, The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option, RFC, 4704, 2006.

Wakikawa, Ryuji. Global connectivity for IPv6 mobile ad hoc networks, Internet-Draft, draft-wakikawa-manet-globalv, 6-02, 2002.

Wang P, Reeves D.S & Ning P, Secure address auto-configuration for mobile ad hoc networks, In IEEE Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, 2005, 519-521.

Wang X, and Qian H, Dynamic and hierarchical IPv6 address configuration for a mobile ad hoc network, International Journal of Communication Systems, 28(1), 2015, 127-146.

Weniger K, and Zitterbart M, IPv6 auto configuration in large scale mobile ad-hoc networks, In Proceedings of European wireless, 1, 2002, 142-148.

Weniger K, Passive duplicate address detection in mobile ad hoc networks, In IEEE Wireless Communications and Networking, 3, 2003, 1504-1509.

Xiaonan W and Shan Z, An IPv6 address configuration scheme for wireless sensor networks based on location information. Telecommunication Systems, 2013, 1-10.

Yousef A, Al-Mahdi H, Mitschele-Thiel A, LHA, logical hierarchical addressing protocol for mobile ad-hoc networks, Proceedings of the 2nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks, 2007, 96–99.

Zhou H, Ni LM and Mutka MW, Prophet address allocation for large scale MANETs, Ad Hoc Networks, 1(4), 2003, 423-434.