A SURVEY ON AUTO-CONFIGURATION MECHANISMS FOR MOBILE AD-HOC NETWORKS (MANETS)

Shahrukh Khalid* and Athar Mahboob**

ABSTRACT

Mobile ad-hoc networks (MANETs) are infrastructure-less networks. Moreover, due to inherent characteristic of mobility of nodes, network merging and partitioning, issues and problems of MANETs are peculiar in nature. Current networking software stacks and services are based on TCP/IP model which is IP address centric. All nodes which want to communicate must have unique IP addresses. Auto-configuration refers to assignment of unique IP addresses to the nodes of MANETs. Due to characteristics of MANETs, assignment of IP addresses to nodes is a non-trivial problem and renders itself as an open issue and potential problem for research. A large number of mechanisms have been proposed for configuring MANET nodes. This paper presents a survey of latest and primitive auto-configuration mechanisms for mobile ad-hoc networks (MANETs).

KEY WORDS: *Mobile ad-hoc networks, IP Address assignment, auto-configuration, infrastructure-less networks, TCP/IP Protocol Stack, IPV4, IPV6*

INTRODUCTION

In the contemporary computer networks which are based on TCP/IP model, it is essential for the devices to have unique IP addresses, so that communication and IP oriented services are enabled. In an infrastructure-oriented network IP addresses bear topological information and hierarchical organization. Presence of central administration entities like DHCP servers make the unique assignment of IP addresses plausible. However, IP address configuration is a non-trivial problem in an autonomously formed MANET, due to peculiar attributes of such networks which are dynamically changing topology, network partitioning and merging and unavailability of central administration. Manual configuration of addresses assignment cannot ensure uniqueness of IP addresses and is not feasible due to the nature of MANET. Therefore, auto-configuration is the only viable option for IP address assignment in the MANET context. The area of auto-configuration mechanisms or protocols for IP address assignment has gained interest in research community and a large number of such mechanisms have been proposed. In this survey we provide a background of auto-configuration problem classification of mechanisms; details of Stateless, Stateful and Hybrid mechanisms respectively; qualitative comparison of the surveyed mechanisms.

BACKGROUND OF PROBLEM

IP address for routing support

There are number of devices like smartphones, PDAs and notebooks which can behave as MANET nodes. Presently available devices have by default vendor ad-hoc networking support and do not allow scalability and support for enabling MANET to its full extent[1]. To enable such support as illustrated in Figure 1, proper routing support is required for enabling one hop and multi-hop communication among the mobile nodes[2]. For routing mechanism to function throughout MANET it is mandatory to assign unique and discernible IP addressees to each node[3].

Figure 1: Requirement of routing support in Mobile Ad hoc networks (MANETs)

* *Hamdard University, Karachi, Pakistan*
** *DHA Suffa University, Karachi,Pakistan*

Without the assignment of unique IP address single hop and multi-hop communication and services like VoIP, instant messaging, internet browsing, etc. cannot be enabled.

NETWORK PARTITIONING AND MERGING

The dynamicity of MANET in terms of partitioning and merging adds diversity to the problems of auto-configuration. Various use cases can be discussed in this context. Suppose addresses have been assigned somehow to MANET nodes shown in Figure 2. Now if node A leaves the particular MANET then the address assigned to the node gets unmanaged if there is non-existence of any overlaying mechanism. Supposedly if there exists a mechanism which could set free the IP addresses for further assignment if a node leaves then what will happen in case the previous node re-appears.

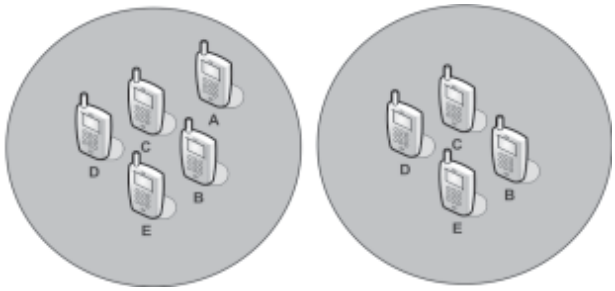

Figure 2: Nodes leaving a MANET

Consider two MANETs illustrated in Figure 3 in which nodes have been assigned distinct IP addresses through some mechanism. Now consider if cloud of nodes in the right network moves to the left and tries to become the part of the network then how the mechanism could ensure the uniqueness of IP addresses in case there exists duplicate addresses in the newly formed network in Figure 4.

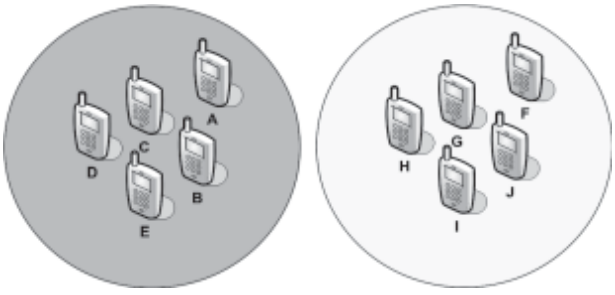

Figure 3**:** Two different MANETs

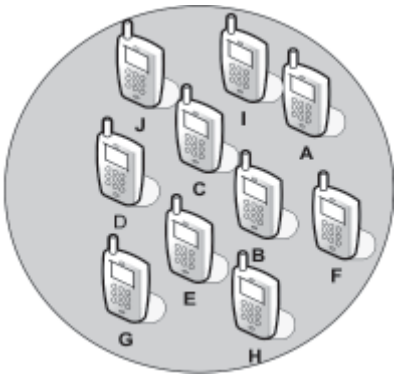

Figure 4**:** Merger of two MANETs

INSUFFICIENT SUPPORT FOR STANDARD SOLUTIONS

Infrastructure based IP address assignment solutions do not suffice the need for auto-configuration mechanism of MANETs. Dynamic Host Configuration Protocol (DHCP) proposed by. Droms[4] et al and its modified form for IPV6 addressing DHCPV6 by Troan, and Droms[5], rely on the use of centralized servers for ensuring unique IP address assignment.

Stateless auto-configuration mechanism for IPV6[6], initially builds a link local address and sends this address using neighbor discovery protocol (NDP) to its one hop peers[7]. As relying on a single DHCP server for IP Address configuration in MANETs will cause a single point of failure in dynamic MANET topology whereas such a server implementation will require multi-hop communication to reach and function which is different from infrastructure based network configuration and not supported for MANET context. Moreover, stateless IPV6 auto-configuration is also based on exchanging messages by one hop peers and multi-hop communication is not supported inherently. Intel[8] and Cisco[9] have reported that there is a possibility of building identification of nodes on the basis MAC addresses but even MAC addresses of devices may also not be unique.

BASIC REQUIREMENTS FOR AUTO-CONFIGURATION

Basic requirements and objectives for auto-configuration protocols are comprehensively summarized by Bernardos[10], Calderon[11] and Moustafa[12] and these include:

(i) Ability to assign unique IP address and to ensure that no two or more nodes obtain the same IP address.

(ii) An IP address gets associated to the node till the time it is in the network. When it departs then the address should be set free for usage by other nodes.

(iii) Quickly adapt to node failures and prevent the nodes from having duplicate IP addresses.

(iv) If one hop node does not have free IP address then there should exist a mechanism so that a distant node could offer free IP address through multi-hop to the node requesting IP address for configuration.

(v) Control traffic should be minimized as much as possible.

(vi) In case of concurrent request for same IP address the protocol should be able to resolve the conflict.

(vii) The protocol should allow provision of network partitioning and merging.

(viii) The protocol should allow synchronization due to the rapid changes in the topology of the MANET.

Moreover, zero configuration networking group[13] gives the following criteria for auto-configuration mechanism to support seamless configuration of ad-hoc wireless networks:

(i) Allocate addresses without involvement of a DHCP server

(ii) Support name to address translation without a DNS Server

(iii) Find services, like printers, without a directory server (DNS Service Discovery)

CLASSIFICATION OF MECHANISMS

Various efforts in the direction of auto-configuration of MANET nodes are described in the ensuing paragraphs. Although there are numerous variations to the auto-configuration mechanisms but each of these mechanisms can be broadly classified as shown in Figure 5 into one of three categories:

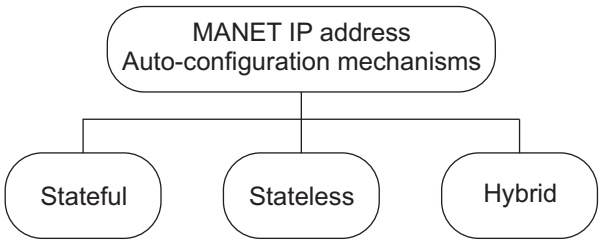

Figure 5: Classification of auto-configuration mechanisms

(i) **Stateful:** The nodes are aware of the network states of other nodes and keep updates through tables.

(ii) **Stateless**: The IP address of a node is generated by the node itself and it is based on some appropriate mechanism to make the probability of duplicate address as small as possible. Although to ensure uniqueness, a process of duplicated address detection (DAD) mechanism is mandatory for ensuring uniqueness.

(iii) **Hybrid Protocols**: Amalgamation of the above two approaches. Computational complexity of this category is higher than the above mechanisms.

STATEFUL MECHANISMS

Easy MANET

Jose Cano et at[14] implemented a visual DNS based system proposed for MANETS for resolving host discovery issues. The solution binds user photo with IP address for easy identification of hosts. More elaborated details of implementation of the solution is offered in Jose Cano, Juan-Carlos Cano, Carlos. Calafate and Pietro Manzoni [15,16] and the recent work by Jose[17] et. al. The architecture of EASY MANET is depicted in Figure 6. Every node initially gets itself configured through a bluetooth server which configures the Layer 3 routing and IP details. The mode of the node then switches to WiFi and the one hop discovery process based on Visual DNS starts. Each node sends a UDP packet to its one hop neighbors which contain a list of known members of MANET. In case of addition of a new member a TCP connection is established between the nodes and information like

IP address and photo are downloaded. The authors claim that the scheme can be extended to support VoIP, video conferencing, etc. in the context of MANET applications.

DISTRIBUTED DYNAMIC HOST CONFIGURATION PROTOCOL (D2HCP)

García et al[18] have proposed a stateful protocol for dynamic IP address assignment. This protocol is based on OLSR routing updates and nodes detect duplicate IP address through OLSR routing messages. All network nodes enjoy the same role and work for maintaining uniqueness of IP addresses through out the network. Each node maintains an IP address block and divides it into two halves. It assigns one block to the incoming node requesting IP address assignment. At the time of assignment of IP address node sends a SERVER_DISCOVERY message in case of available addresses from the server a SERVER_OFFER message is sent by the server node. This type of communication is based on the MAC layer as the node has not yet been assigned IP address. In case of non-availability of addresses at the one hop peer nodes after a certain interval SERVER_POLL message is initiated by the requesting node. After receiving the SERVER_POLL message the IP address bearing node starts IP based communication with the rest of the nodes in MANET and sends IP_RANGE_REQUEST. If empty addresses are available in the network then IP_RANGE_RETURN message is received which contains addresses that can be assigned to the node which has requested the IP address. A D2HCP message flow is shown in Figure 7.

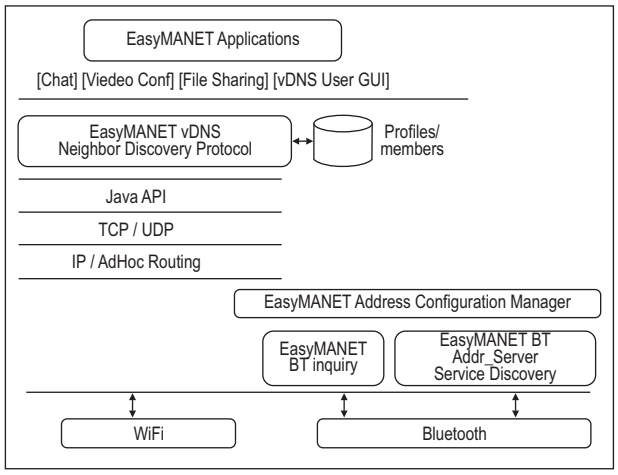

Figure-6: Architecture of EASY MANET

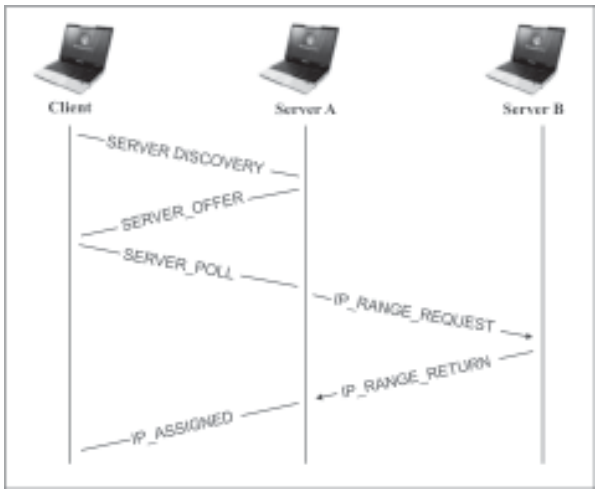

Figure 7: D2HCP Protocol Message flow

SAAMAN

Hussain et al[19] have proposed an IP address auto-configuration mechanism in which routing is based on geo-forwarding mechanism. Authors have named the protocol as SAAMAN: Scalable Address Autoconûguration in Mobile Ad-Hoc Networks. In geo-forwarding each node is enabled with a GPS receiver and it knows its position including latitude, longitude, altitude and height. Each node broadcasts its updated position to its one hop neighbors through ***HELLO*** messages. In order to ensure uniqueness of IP Addresses the protocol implements evenly ***Distributed Detection Servers*** (DDS). The criterion of selection of these servers is based on their hierarchical position in the grid. These servers maintain ***Duplicate IP Detection Tables*** (DDT). When a node requires to join the MANET it chooses a temporary address which the authors refer to as real address. In order to ensure its uniqueness a query is sent by the node to the DDS for checking its plausibility. Addresses configured through the scheme are of the form of having prefix ***AgentID*** and suffix ***HostID***. Where as an ***AgentID*** is common to all particular hosts which are configured through the same addressing agent. When negative messages are received from all available DDS then the node uses the temporary address as its permanent address. Whenever a node has departed from the MANET there exists two scenarios one is graceful and the other one is abrupt. For graceful departure the node apprises the DDS and DDS will delete the respective node from their database. In case of an abrupt departure the protocol requires every node to send periodic Hello messages.

When a DDS does not receive Hello messages from a node after a timer value the respective node is deleted and the address can be used for other upcoming non-configured nodes.

TREE BASED DYNAMIC ADDRESSES

Mamoun et al [20] have proposed a tree based auto-configuration mechanism for MANET in which nodes are classified into three categories based on their roles in the protocol. The main node in the protocol is the ***root node*** which has a diverse set of functions which includes maintenance of records in its database of all group leaders in the network, maintaining free address information held by group leaders, index of leader of leaders for assignment of new root node in case of its own departure from the network, performing the network merging and partitioning tasks. Another kind of node is the ***leader node*** which lies at the next hierarchical level below the root node. This node possesses disjoint set of free IP addresses for assignment to the non-configured nodes. Leader node periodically broadcasts its presence using *hello* messages**.** In case if two leaders are available in a particular region the one with the lower IP address will forego its leadership in the favor of higher IP address number. ***Normal node*** as the name signifies does not have any special function except that it can perform as a router node in case of non availability of leader in a particular area. When a new node wants to join the network it sends an ***addressRequest*** message. In case of no reply after a lapse of ***addressReqTimer*** it initializes itself as a root node, a random number and timestamp is concatenated with the root node ID. In case if this node had initialized itself at an isolated place where there had been no nodes, and now this node enters the area of root node then the node with the lowest ID will be set as the root node.

CLUSTER BASED CONFIGURATION

Longjiang and Xiaoming[21] have proposed cluster based mechanism for auto-configuration based on virtual address agents. An addressing agent entity holds an IP address space for assignment to other non-configured nodes. The protocol also introduces a process of uninterrupted communication strategy when a node having address *a2* moves from cluster A having cluster head *a1* to a new cluster say cluster B having cluster head *b1*.

At cluster B the address changes from *a2* to *b2*. Say the node was initially having communication with *cn* which is a correspondent node. Now in order to continue communication link with *cn* the node *a2* when it enters into cluster B, it apprises the cluster head about its previous IP address and the cluster head after assignment of new IP address apprises the gateway node *a3* about this mapping information that *a2* is now *b2* so that traffic between *cn* and *b2* can be routed through the gateway node *a3* and cluster head *b1* (Figure 8).

SECURE PROPHET ADDRESSING

Zhou et al[22] have proposed a secure scheme named as Secure Prophet Auto-configuration which is a security extension to authors previous work[23]. A prophet address auto-configuration scheme is based on a stateful function ***fn*** which is called as ***seed***. This functions holds two properties: (1) if it is called two

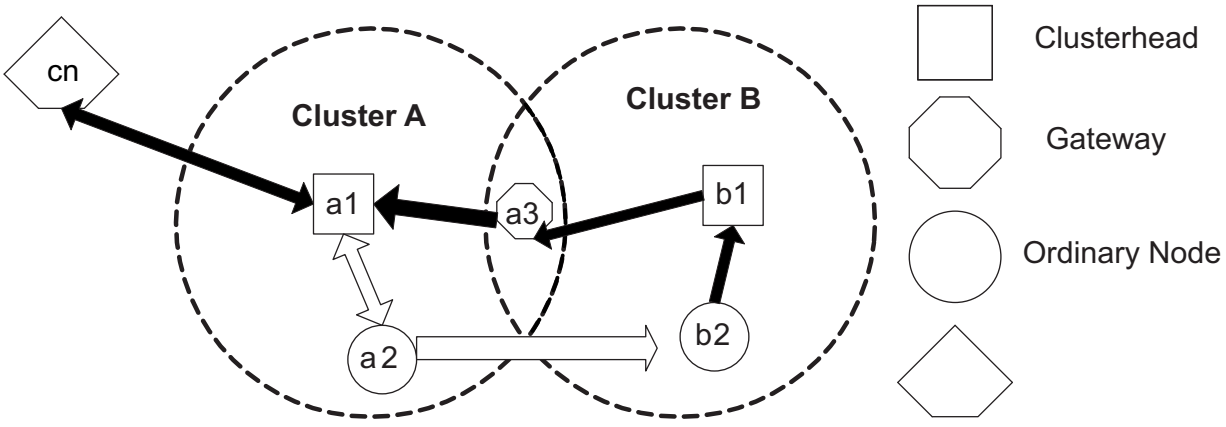

Figure 8: Cluster based auto-configuration

times then the interval generated by two calls is extremely large and (2) the probability of occurrence of a unique number in limited calls to the *fn* is extremely low. There is an implicit assumption in the scheme that all nodes update their internal state after IP address is allocated to them. In case of an adversary node it does not update its state. Thus to secure the scheme authors have proposed a rule or formula which safeguards from adversarial attacks. In order to apply the rule each corresponding node is required to acquire a series of parameters from the allocator node which include seed value of whole MANET, index of increasing exponent, source address of reply node and priority number. Based on these parameters the allocator address can be calculated. Thus if allocator address matches the address generated by the rule the reply is valid otherwise it will be discarded. In case of a valid reply the node generates an IP address based on the acquired parameters and a random value. The state transition logic of the protocol is depicted in Figure 9.

TREE BASED COORDINATED ADDRESSING

Sheu et al[24] have proposed an IP address assignment technique in which few nodes have been nominated to perform the role of a coordinator. A new node without IP address can find the nearest coordinator and requests for an IP address assignment through unicast communication. For increasing the efficiency a tree based topology is maintained for the coordinators. Whenever a node leaves the MANET it releases its IP address and apprises to its coordinator to update the list of free IP addresses.

NONCE AND MAC ADDRESS

Huq et al[25] have proposed auto-configuration mechanism based on MAC and random number nonce. In this mechanism each node maintains an IP table of all the nodes in the network. The authors argue that due to memory capacity of contemporary wireless devices maintaining a large database will not be problematic. When a new node wants to join the network it acquires the IP address list of all the members by sending a broadcast. After that next IP address is assigned using the following procedure. A node generates a random number referred as nonce as its identifier and binds this with its MAC address and IP address. So a composite table of Nonce, MAC address and IP address is built and shared with all the nodes in MANET. In case of network merger and two nodes appearing to have same IP address, conflict resolution can be carried out on the basis of nonce

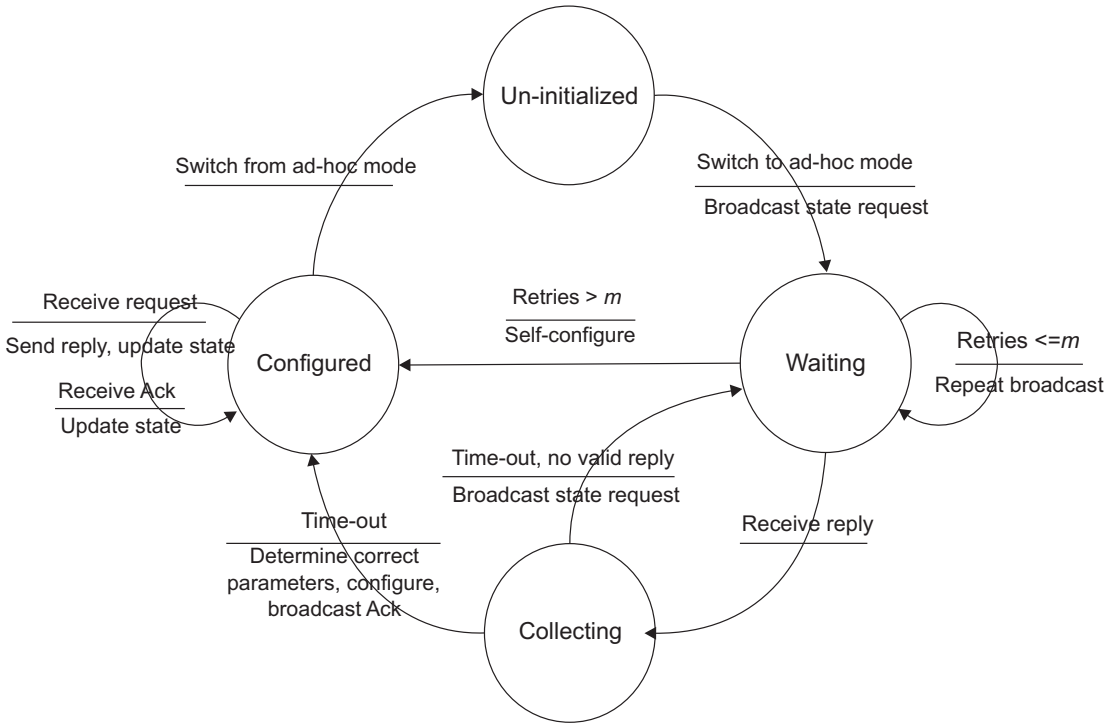

Figure 9: State transition diagram of Secure Prophet address auto-configuration

and MAC address mapping information.

MOHSIN AND PRAKASH PROTOCOL

In Mohsin and Prakash protocol proposed by Mohsin. and Prakash[26] each node divides the IP addresses into binary division of blocks. Each node maintains the table which has state of all other nodes in the network. This table is continuously updated for synchronization. When a joining node requests for IP address the node with free address blocks gives one to the requesting node. In case of abrupt departure from the MANET the server node upon monitoring the routing traffic will see whether the node has departed or not. In case of no routing information rest of nodes will be conveyed the departure information of the node. In case of graceful departure of the node it will convey the intention of leaving the network and all the nodes consequently update their table.

THOPPIAN AND PRAKASH PROTOCOL

Thoppian and Prakash[27] suggested the protocol in which each node maintains a disjoint set of IP addresses. When a node requests for an IP address the requested node if it has a free address block will divide the block into two and assign a one to the requesting node. In case the requested node does not have free blocks it will search the network for availability of free addresses and choose the node with largest available address space. In order to detect network merging each network maintains its Network ID and continuously broadcasts it in the HELLO message. In case a node receives a new Network ID a new network is detected. In case of detection of merger the node can offer free IP addresses to the joining node. The joining node also needs to change its network ID so that it could become the part of the network.

MANETCONF

MANETCONF by Nesargi and Prakash[28] protocol is a stateful type protocol. Each node has a common distributed table of IP addresses. When a joining node requests for IP address it chooses an initiator node through broadcast message. The initiator asks the permission of all the other nodes in the network before assigning the IP address to the requesting node. If no conflict occurs the free IP address is assigned to the requesting node. After the address assignment the action is again broadcast to all the nodes in the network for keeping updated version of the shared distributed tables.

STATELESS MECHANISMS

STRONG DUPLICATE ADDRESS DETECTION

In strong duplicate address detect (SDAD) mechanism by Perkins et al[29], a node selects its own IP address and then sends the Address REQuest AREQ message in the network. This will cause flooding in case of a node bearing the same IP address reply AREP message will be generated by the node. Thereafter the node will select another IP address and will repeat the same mechanism. In case of no reply from node the requesting node will check its timer value and in case of expiration of timer the IP address will be selected for using in MANET.

WEAK DUPLICATE ADDRESS DETECTION

Weak Duplicate Address Detection (WDAD) protocol by Vaidya and N.H[30] requires each node in the network to generate and bind a unique key along with its IP address i.e. a key-IP pair is generated for every node. When packets are required to be send by the node it also sends the key along with the IP address. The receiving node checks the binding of node IP address with key in its table and if they do not coincide it will mark the address as invalid. By enabling that each node could have a key and ensure that packets could only be routed to the category of node having Key-IP pair generated. For this protocol to work necessary modifications must be made in the routing protocol so that it is also able to carry the key along with the IP address.

PASSIVE DUPLICATE ADDRESS DETECTION

Passive duplicate address detection (PDAD) mechanism by Weniger et al[31] exploits the information of proactive routing protocol control information traffic for detecting the duplicate IP Addresses in MANET. Three variations of PDAD exist:

(i) PDAD (SN): PDAD Sequence Number relates to the fact that each node while transmitting proactive routing protocol traffic auto-increments the sequence

number field of the routing protocol and stores the state of sequence number. Such that when a node receives a packet having the same IP address and higher sequence number value field then duplicate IP address can be diagnosed.

(ii) PDAD (SND): PDAD Sequence Number Difference is the observation made by any other node in the sequence number difference of same IP Address routing packets. That is when the difference is realistically larger than then auto-increment sequence number then a node can notice the duplicate address.

(iii) PDAD (SNE): There may be a possibility that the sequence number values of two nodes with same IP address are same. In this peculiar case the link state information of neighbor nodes is compared. In case of difference a duplicate IP Address is detected.

DISTRIBUTED ADDRESSES

Sonia et al[32] proposed a distributed address auto-configuration scheme in which two categories of nodes can take part for configuration of non-configured nodes. The authors have categorized them as ***Configuration Agents*** and rest will be ***simple nodes***. Configuration Agent is a node which possesses a list of available IP addresses which can be assigned to other nodes. These agents possess disjoint set of addresses. When any agent wants to configure a new agent it gives part of its address space to the new upcoming agent for further distribution of addresses in MANET. Every agent sporadically broadcasts an ***advertisement message*** to announce its existence. This message possesses following information: IP address of itself, size of its addressing space and the network identification number. The job of the simple node is to behave as a bridge between the ***requester*** and the configuration agent. In case if a node receives a number of advertisement messages either directly or through the simple node it chooses its configuration agent who has the largest address space. At the time of initialization a requester node sends an ***address request*** message using a combination of temporary address space and its MAC address for avoiding problems of duplicate temporary address. The node instantiates a timer, after broadcasting the address request message. In case of no response the requester node configures itself as a *configuration agent*. The protocol allows network merger based on the network identifiers. The lowest in number network identifier nodes forego their identifiers.

PRIVACY ADDRESSING

Privacy Addressing by Longjiang et al[33] is based on RFC 3041[34] which is a privacy addressing extension to IPV6 stateless auto-configuration. In accordance with this RFC a node acquires a new IP address after the lapse of a timer value through the use of a pseudo-random number generator. The authors refers this extension for MANET as ***privacy extension approach*** (PEA). The benefit of such a scheme is that it protects a particular node from getting its IP address spoofed from a malicious intruder in the network. Key idea of the protocol is illustrated in the state diagram in which a periodical mechanism of randomization in terms of address generation is added. For the set of protocols which use a centralized allocation table and those which use distributed common allocation table the randomization and periodical process is easy to apply. Whereas the set of protocols which use multiple disjoint sets of allocation tables the protocol proposes a new mechanism referred as ***shuffled splitting method*** (SSM). In normal cases after splitting the address space into two parts the second part is forwarded to be ***requester*** node. But in SSM for ensuring random address picking by a requester node the parent node forwards the second part if itself belongs to first part else it will forward the second part. The authors also use the secure pool distribution in which message exchange is by virtue of public and private key cryptography mechanism. A State transition diagram of privacy addressing is shown in Figure 10.

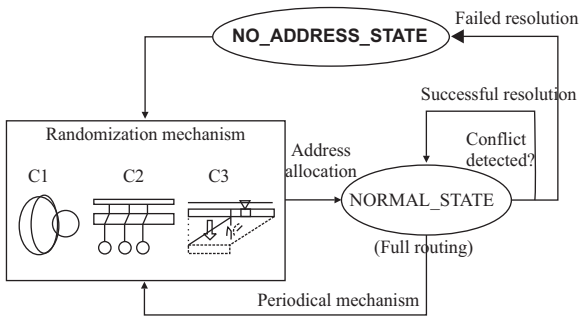

Figure 10: State transition diagram of privacy addressing

ID BASED DYNAMIC SCHEME

Ghosh and Datta[35,36] have proposed scheme named as ***ID based IP configuration scheme*** (IDDIP) In this scheme each node can act as a proxy node and is able to generate a unique IP address for non-configured node. Along with a unique IP address, each node is identified by a unique ID. Thus each node in this protocol is identified by an IP address and ID tuple i.e. <***node ID, IP address***>. Every node has a pre-distributed one-way hash function say (H). Address allocation starts when a new node wants to join the MANET. The non-configured node generates a public/private key pair and periodically broadcasts a ***DISCOVER*** message with its signature to its neighbor nodes. Upon expiry of the timer value the node configures itself as a root node and generates a network ID and node ID. In case of availability of neighbor nodes these node after receiving the discover message send a signed offer ***OFFER IP*** message to the requesting node. In case of a number of replies the non-configured node chooses the least value of the IP address and consequently replies back with a ***SIGNED SELECT*** message to the proxy node who has offer the particular IP address. The nodes can identify each other through the use of hash function pre-distributed. Network partitioning and merging is based on the generated network id.

EXTENDED PRIME NUMBER BASED IP ADDRESS ALLOCATION SCHEME

Kumar and Singla[37] proposed an extended prime number based IP address allocation scheme. In this scheme considerably large number of nodes are assigned as proxies. Proxy nodes can further assign addresses to other nodes. A prime number holder IP address bearer node is said to be proxy as depicted in the Figure 11 and Table I. The range of addresses generated by the proxy node is a sequence progressing twice of its own number.

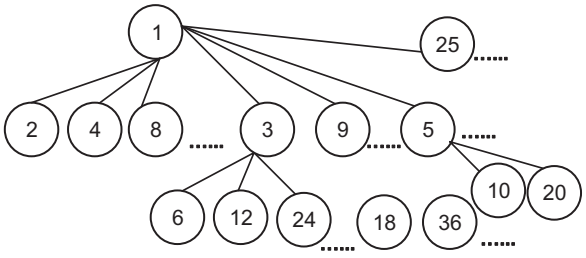

Figure 11: Graph of nodes

Table I: 50 Nodes address allocation

Host Number	Address Generated	No of Nodes
1(Root)	2,3,4,5,7,8,9,11,13,16,17,19, 23,25,27,9,31,32,37,41,43,47.49	23
3	6,12,24,48	4
5	10, 15,20,30,40, ,45	6
7	14,21,28,35,42	5
9	18,36	2
11	22,33,44	3
13	26,39	2
17	34	1
19	38	1
23	46	1
25	50	1

PRIME NUMBER ORIENTED ADDRESSING

A prime number address allocation (PNAA) is proposed by Hsu et al[38]. In this scheme each node behaves as a proxy and can assign addresses to other nodes. The first node is 1 the sequence for prime numbers is 2,3,5,7 and so on till the consumption of the address space. If root 1 assigns 2 to any other node the node 2 will assign addresses following 2*1 with 2 as the largest prime factor and product of the prime series as follows:

2 à 2*2, 2*3, 2*5,2*7…….. and so on

Similarly for 6 =3*2 with 3 as the largest prime factor

6 à 6*3, 6*5, 6*7, …… and so on

Assignment of prime numbers is illustrated in Figure 12.

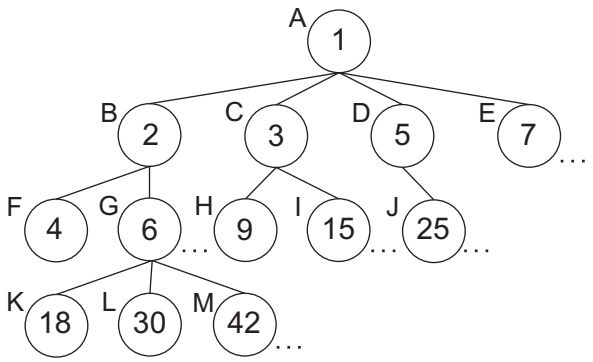

Figure 12: Address assignment graph

HASH FUNCTION BASED NAME

Kim et al[39] proposed a hash oriented Name Based Auto-configuration (NBA). In this scheme a node builds its IP address on the basis of user selected name. IP address is found through a commonly shared Hash function. In case of a name conflict authors have proposed three variations as illustrated in Figure 13:

(i) NBA: In this aspect the node simply changes the name and obtains a new address from hash function, then again check for the conflict and if no conflict occurs a unique name and address is assigned to the node.

(ii) NBA LP: LP stands for linear probing. In this variant, in case of the conflict address is incremented by one and conflict resolution is carried out through out the network nodes.

(iii) NBA-DH: DH stands for double hashing. In this variation the node builds its address through dual hashing in which one function is SHA1 algorithm[40]. In case of occurrence of conflict the algorithm resorts to NBA-LP mechanism.

HYBRID MECHANISMS

Domain based (DACF)

In ***Domain based auto-configuration*** (DACF) by Longjiang et al[41] authors have suggested a domain oriented configuration for addressing the issue of IP address assignment of MANET nodes. As illustrated in the Figure 14 the protocol uses the state transition diagram for various node configuration setups. A node is said to be in NO_ADDRESS_STATE mode when it does not possess an IP address. After obtaining of an IP address and ***domain generation*** it switches its mode to ***NORMAL_STATE***. A normal state configuration may signify any one of two roles for a node. Either it behaves as a server for assignment of IP addresses to other nodes or it may behave as a normal node. In case of address conflicts the protocol uses passive Duplicate address detect ***PDAD*** *(Passive duplication address detect mechanism)* mechanism based on ***PACMAN*** (Passive Auto-configuration for Mobile Adhoc Networks) [42] and the node observes the ongoing routing packets information. In case of successful resolution of conflict the normal state of the node is restored otherwise its state is changed to the NO ADDRESS STATE. The protocol also uses the mechanism of virtual address space of PACMAN. DACF divides each address into two part the prefix is called as ***interID*** which refers to a particular domain whereas remaining part is ***intraID*** which refers to all the parts in a particular domain.

The initialization of domain based auto-configuration is based on a domain initiator which generates series of interIDs by a pseudorandom number generator and picks the first one for its domain. The other

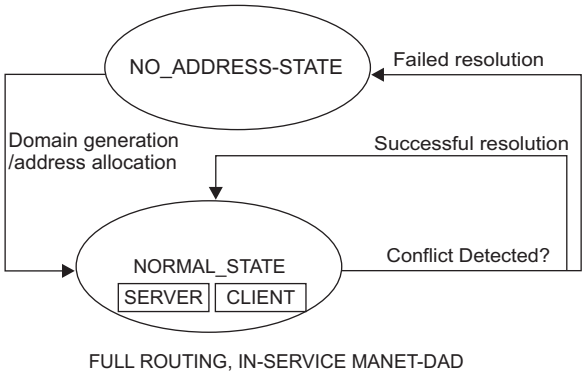

Figure 14: State diagram for DACF

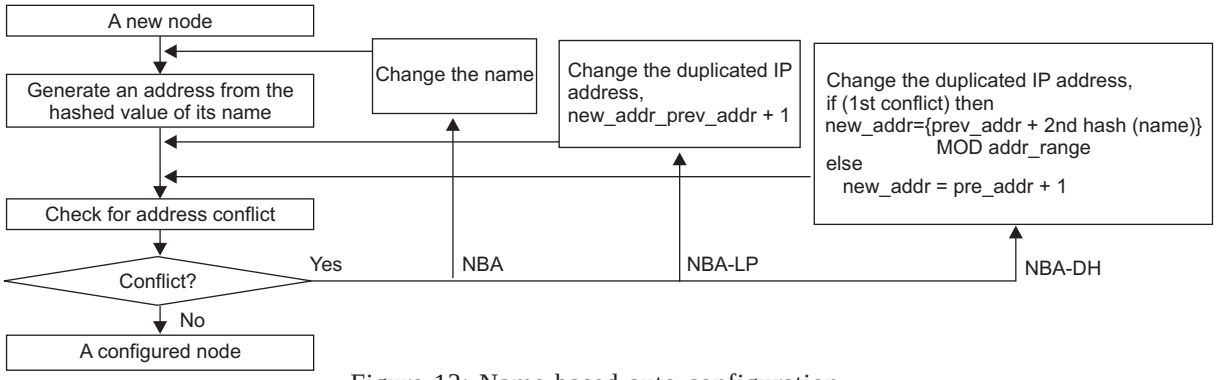

Figure 13: Name based auto-configuration

in series interIDs are used for subsequent conflict resolution.

PASSIVE AUTO-CONFIGURATION FOR MOBILE ADHOC NETWORKS (PACMAN)

This is a hybrid protocol[42] in which a stateless mechanism deals with a node selecting its own address based on a probabilistic function with low probability of occurrence of duplicate address. But no function has zero probability of ensuring duplication in addresses therefore this protocol further exploits the cross layer information from the OLSR[43] routing protocol to detect duplicate addresses. This mechanism is passive duplicate address detection (PDAD) mechanism as mentioned above. The architecture of PACMAN is illustrated in Figure 15.

HYBRID CENTRALIZED QUERY

Sun et al[44] proposed a hybrid mechanism of auto-configuration in which a node generates its own IP address and then it runs a strong DAD mechanism to address problem of address conflict. After this it communicates with a central node known as Address Authority to register its address. An Address Authority maintains a network identity based on its MAC address and continuously broadcasts the same in HELLO messages. In case of existence of only a single node it assumes the role of an Address Authority.

QUALITATIVE COMPARISON OF MECHANISMS

MANET auto-configuration protocols can be compared on the basis of number of characteristics mentioned in the Table 2.

Table 2: Factors for mechanism comparison

Factor	Description
Security	Whether the mechanism has security features
Uniqueness not	Scheme guarantees unique addresses or
Overhead	Amount of control information flow
Latency	Amount of time required for address acquisition
Routing	Whether protocol depends on a routing protocol
Uniformity	All nodes having same role or not
Address type	IPV4 or IPV6
Scalability	Size support large or small

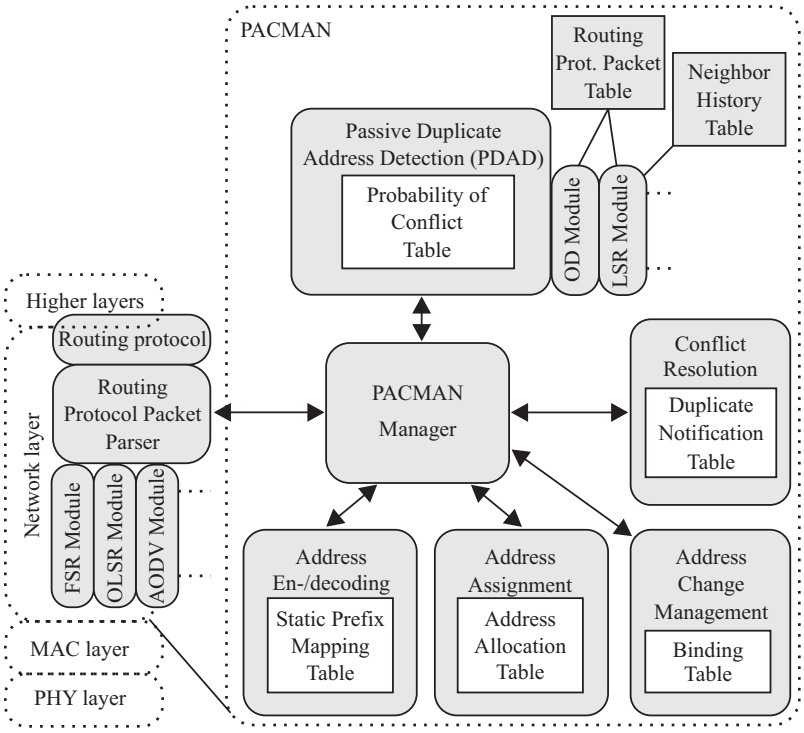

Figure 15: Architecture of PACMAN

Table 3: Stateful Mechanisms

Mechanism / Factor	Easy MANET	D2HCP	SAAMAN	Tree Based Dynamic	Cluster based	Secure prophet	Tree Based coord	Nonce & MAC	Mohsin & prak.	Thopp & Prak	MANET Conf
Security	No	No	No	No	No	Yes	No	No	Yes	Yes	No
Uniqueness	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	No
Overhead	Medium	Low	Low	Low	Medium	Medium	Medium	Medium	Medium	Medium	High
Latency	Low	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	High
Routing	No	Yes	No	No	No	No	No	No	No	No	No
Uniformity	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes	Yes
Address type	IPV4	IPV4	IPV4	IPV4	IPV4	IPV4	IPV4	IPV4	IPV4, IPV6	IPV4	IPV4
Scalability	Small	Large	Large	Large	Large	Large	Large	Large	Small	Small	Small

Table 4: Stateless Mechanisms

Mechanism / Factor	SDAD	Weak DAD	PDAD	Distributed Addresses	Privacy addressing	IDDIP	EPNA	PNAA	Hash function
Security	No	No	No	No	No	Yes	No	No	Yes
Uniqueness	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Overhead	High	Medium	Low	Low	Medium	Medium	Low	Low	High
Latency	High	Medium	Low	Medium	Medium	Medium	Medium	Medium	Medium
Routing	No	No	Yes	No	No	No	No	No	No
Uniformity	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Address type	IPV4	IPV4	IPV4	IPV4	IPV4	IPV6	IPV4	IPV4	IPV4
Scalability	Small	Large	Large	Large	Large	Large	Large	Large	Medium

ISSN 1023-862X

Table 5: Hybrid Mechanisms

Mechanism Factor	DACF	PACMAN	HCQA
Security	No	No	No
Uniqueness	Yes	No	Yes
Overhead	Low	Low	High
Latency	Medium	High	High
Routing	Yes	Yes	Yes
Uniformity	No	Yes	No
Address type	IPV4	IPV4	IPV4
Scalability	Large	Large	Small

On the basis of factors presented in Table 2 a qualitative comparison of stateful, stateless and hybrid protocols are given in Table 3, 4 and 5 respectively.

FUTURE RESEARCH DIRECTIONS

Security

A great emphasis is now being placed on security of auto-configuration protocols. Many recent protocols have been developed with security extensions extensions [35,36,45,46]. Newly developed protocols will have suitable cryptographic support in such a way that processing overhead can be minimized.

VIRTUALIZATION OF PLATFORMS

Chakchai et al[47] have proposed a derivation of an ID/Locator split concept model[48]. This model has a great potential of applicability in terms of auto-configuration mechanism in MANETs. In their work authors have described various problems of IP oriented models which is over-riding role of IP address i.e IP address is an identifier for a host as well as a locator in the routing space. If this over riding role can be separated by assigning unique identifiers then problem of auto-configuration can be addressed. However adaptation of the proposed model is MANET domain requires considerable amount of research and experimentation.

CONCLUSION

In this paper we have provided the background of Auto-configuration problems in MANETs. Seemingly trivial auto-configuration problem poses a considerable bottleneck in wider adoption of MANETs. We have classified the available mechanisms into three broad categories including stateless, stateful and hybrid. A number of Auto-configuration protocols in the classified categories have been surveyed. It is evident that these mechanisms are essential means for enabling the IP oriented services between the nodes. Each of these mechanism has its merits and demerits and an appropriate protocol can be selected for implementation in MANET context. We have presented a qualitative analysis of our surveyed results in separate categories. Future research direction in the field of auto-configuration will have a profound emphasis on security considerations. ID/Locator split concept mechanism like Virtualization of objects model have an immense potential to apply in the field of auto-configuration mechanisms for MANETs. Thus newly developed techniques in the area of Computer Network research will open new areas in Auto-configuration mechanisms and this will facilitate in improvements in solving the communication barriers in MANETs.

REFERENCES

1. *IEEE 802.11 Wireless Local Area Networks, 2013, http://www.ieee802.org/11/*

2. *Brownlee B. Liang Y 2011,"Mobile Ad Hoc Networks An Evaluation of Smart phone Technologies", Defence R&D Canada , DRDC CORA CR -169.*

3. *Ad-Hoc Network auto-configuration Work Group (autoconf),2013, http: //tools.ietf.org/wg/autoconf/*

4. *Droms R. 1997, "Dynamic host conûguration protocol," RFC 2131.*

5. *Troan, O. and Droms, 2003,"R. IPv6 Prefix Options for DHCPv6", RFC 3633,http:// www.ietf.org/rfc/rfc3633.txt*

6. *Thomson S. and T. Narten, 1998, "IPv6 Stateless Address Autoconfiguration", RFC 2462.*

7. *Narten, T., Nordmark, E.Simpson and W Soliman, H, 2007, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, http:// www.ietf.org/rfc/rfc4861.txt*

8. *Intel, 2002,"Duplicate MAC address on intel*

stl2 server board", http://www.intel.com/support/motherboards/server/stl2/sb/cs-007538.htm

9. *Cisco, 1997,"Duplicate MAC addresses on cisco 3600 series", http://www.cisco.com/en/US/ts/fn/misc/7.html*

10. *Bernardos C, Calderon M. and .Moustafa H., 2008, "Ad-Hoc IP Autoconfiguration Solution Space Analysis", Internet Draft, http://tools.ietf.org/pdf/draft-bernardos-autoconf-solution-space-02.pdf*

11. *Bernardos C, Calderon M. and .Moustafa H., 2008, "Survey of IP Address Autoconfiguration Mechanisms for MANETs", Internet Draft,http://tools.ietf.org/html/draft-bernardos-manet-autoconf-survey-04*

12. *Bernardos C, Calderon M. and .Moustafa H., 2008, "Evaluation Considerations for IP Autoconfiguration Mechanisms in MANETs", Internet Draft,*

13. *Zero configuration networking group, 1999, http://www.zeroconf.org*

14. *Jose Cano, Juan-Carlos Cano, Carlos T. Calafate and Pietro Manzoni, 2007, "Solving the user-to-host binding problem in ad hoc networks through the dissemination of photographic identifiers", in Fourth ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, Crete Island, Greece.*

15. *Jose Cano, Juan-Carlos Cano, Carlos T. Calafate and Pietro Manzoni, 2010, "Experiences in Developing Ubiquitous Applications" in Designing Solutions-Based Ubiquitous and Pervasive Computing: New Issues and Trends.IGI Global,ch.5,pp.97-112.*

16. *Jose Cano, Juan-Carlos Cano, Carlos T. Calafate and Pietro Manzoni, 2010, "EasyMANET: an extensible and configurable platform for service provisioning in MANET environments" in Communication Magazine, IEEE.*

17. *Jose Cano Reyes, 2012, "Integrated Architecture for Configuration and Service Management in MANET Environments", PhD Thesis,Valencia.*

18. *García Villalba, L.J., García Matesanz, J., Sandoval Orozco, A.L. and Márquez Díaz, J.D.,2011, " Distributed Dynamic Host Configuration Protocol (D2HCP).", Sensors.*

19. *Hussain SR, Saha S and Rahman A, 2010, "SAAMAN: Scalable Address Autoconûguration in Mobile Ad Hoc Networks", Springer, J Netw Syst Manage.*

20. *Mamoun F. Al-Mistarihi, Mohammad Al-Shurman and Ahmad Qudimat, 2011 ,"Tree based dynamic address auto-configuration in mobile ad hoc networks", Elsevier, Computer Networks, Vol 55, pp 1894-1908.*

21. *Longjiang Li,Yunze Cai and Xiaoming Xu, 2009 ,"Cluster-Based Autoconûguration for Mobile Ad hoc Networks", Springer, Wireless Pers Commun, vol 49, pp 561-573.*

22. *Hongbo Zhou , Matt W. Mutka and Lionel M. Ni, 2010, "Secure prophet address allocation for MANETs", Security Comm. Networks., Wiley, vol.3, pp 31-43.*

23. *Hongbo Zhou , Matt W. Mutka and Lionel M. Ni, 2003, "Prophet address allocation for large scale MANETs", Elsevier, Ad Hoc Networks, pp 423-434.*

24. *Jang-Ping Sheu, Shin-Chih Tu, Li-Hsiang Chan , 2008 , "A distributed IP address assignment scheme in ad hoc networks", International Journal of Ad Hoc and Ubiquitous Computing - Vol. 3, No.1 pp. 10 – 20.*

25. *Huq S, Kavitha D, Sreenivas KE Murthy and Satyanarayana B. 2011, "Dynamic IP Address Auto-configuration in MANETs", Computer Networks and Information Technologies Communications in Computer and Information Science Volume 142, pp 452-457*

26. *Mohsin, M. and Prakash, R., 2002, "IP Address Assignment in a Mobile Ad Hoc Network". Proceedings of Military Communications Conference (MILCOM), Anaheim, CA, USA, September, Volume 2, pp. 856-861.*

27. *Thoppian M.R. and Prakash, R. , 2006, "A Distributed Protocol for Dynamic Address Assignment in Mobile Ad Hoc Networks", IEEE Trans. Mob. Comput., vol 5, pp 4-19.*

28. *Nesargi, S. and Prakash, R., 2002, "MANETconf: Configuration of Hosts in a*

Mobile Ad Hoc Network.", Proceedings of IEEE INFOCOM, New York, NY, USA, pp. 1059-1068.

29. *Perkins, C.E., Malinen, J.T., Wakikawa, R., Belding-Royer, E.M. and Sun, Y., 2001, "IP Address Autoconfiguration for Ad Hoc Networks",Internet Draft, http://tools.ietf.org/html/draft-perkins-manet-autoconf-01.*

30. *Vaidya and N.H., 2002, "Weak Duplicate Address Detection in Mobile Ad Hoc Networks", Proceedings of ACM MobiHoc Lausanne, Switzerland, June 2002; pp. 206-216.*

31. *Weniger, K., 2003, "Passive Duplicate Address Detection in Mobile Ad Hoc Networks", Proceedings of the IEEE WCNC, New Orleans, LA, USA.*

32. *Gamar Sonia, Amine Elabidi and Kamoun Farouk, 2010, "Distributed address auto configuration protocol for Manet networks", Telecommunication Systems, Springer, pp 39-48,Volume: 44,Issue: 1,*

33. *Longjiang Li, Yuming Mao and Supeng Leng, 2011, "Privacy addressing and autoconûguration for mobile ad hoc networks", Computer Communications, Elsevier, vol. 34, pp 423-428,*

34. *T. Narten and R. Draves, 2001, "Privacy extensions for stateless address autoconûguration in IPv6", RFC 3041.*

35. *Uttam Ghosh and Raja Datta, 2011 ,"A secure dynamic IP conûguration scheme for mobile ad hoc networks", Ad Hoc Networks, Elsevier, vol 9, pp 1327-1342.*

36. *Uttam Ghosh and Raja Datta, 2012, "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,Springer, pp 295-308.*

37. *Harish Kumar and R. K. Singla, 2009, "Architecture for address auto-configuration in MANET based on extended prime number address allocation (EPNA)", WSEAS. Trans. on Comp. Vol 8, pp 549-558,*

38. *Hsu, Y.Y., Tseng and C.C., 2005, "Prime DHCP: A Prime Numbering Address Allocation Mechanism for MANETs", IEEE Commun. Lett.*

39. *S A Lee Y A Lee B B Kim N A Kang, 2006, "Name-based autoconfiguration for mobile ad hoc networks", ETRI Volume: 28, Issue: 2, Pages: 243-246*

40. *Charlie Kaufman, Radia Perlman, and Mike Speciner, 2002, "Network security, Private communication in a public world", Prentice Hall, pp. 118-146*

41. *Longjiang Li, Yunze Cai and Xiaoming Xu, 2009, "Domain-based autoconûguration framework for large-scale MANETs", Wirel. Commun. Mob. Comput, Wiley,Vol 9, pp 938-947.*

42. *Weniger, K., 2005, "PACMAN: Passive Autoconfiguration for Mobile Ad Hoc Networks", IEEE J. Sel. Area. Comm., 23, 507–519.*

43. *Clausen T. and Jacquet, P., 2003, "Optimized Link State Routing Protocol (OLSR)", IETF Internet RFC 3626,http://www.ietf.org/rfc/rfc3626.txt.*

44. *Sun, Y., Belding-Royer and E.M, 2003, "Dynamic Address Configuration in Mobile Ad Hoc Networks", Technical Report UCSB 2003-11, Department of Computer Science, University at Santa Barbara: Santa Barbara, CA, USA.*

45. *Zohra Slimane, Abdelhafid Abdelmalek,Mohamed Feham and Abdelmalik Taleb-Ahmed, 2011, "Secure and robust IPV6 autoconfiguration protocol for mobile adhoc networks under strong adversarial model", International, Journal of Computer Networks & Communications (IJCNC) Vol.3, No.4.*

46. *Abdelhaûd Abdelmalek, Zohra Slimane, Mohamed Feham and Abdelmalik Taleb-Ahmed TCSAP, 2011, "A New Secure and Robust Modiûed MANETconf Protocol", WiMo/CoNeCo Springer, CCIS 162, pp. 73–82.*

47. *Chakchai So-In, Raj Jain , Subharthi Paul and Jianli Pan, 2011, "Virtualization architecture using the ID/Locator split concept for Future Wireless Networks (FWNs)", Computer Networks, Elsevier, Vol 55, pp 415-430.*

48. *Stoica I, Adkins D, Zhuang S, Shenker S, Surana S. 2004, "Internet Indirection Infrastructure", IEEE/ACM Transaction on Networking 12 (2) pp 205–218.*