ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Unique Address Assignment and Dynamic Configuration of Node Traffic of MANETs

K Sekar

Professor, Department of CSE, S.V. College of Engineering, Tirupati, Chittoor, Andhra Pradesh, India

ABSTRACT: IP Address assignment is a key challenge in Ad hoc networks because it doesn't have predefined infrastructure. Since most dynamic networks have frequent partitions with fading nodes and joining/leaving nodes, a distributed and self-managed mechanism is required by Autonomous Addressing Protocols to avoid address collisions. To reduce the control load and proactively tackle the packet losses and network partitions, a lightweight protocol that can configure mobile ad hoc nodes based on distributed address database that is stored in filters is proposed. This proposal considers merging of partitions, joining nodes and network initialization. This protocol deals with the resolving of collision of addresses, and the reduction of the control traffic, all the while balancing the load in an optimal manner.

KEYWORDS: Adhoc Networks, Computer Network Management, Addressing Mechanisms, IP Address Configuration

I. INTRODUCTION

Whenever two or more devices want to exchange any kind of information they need an interface called network to communicate. This network can be established through LAN covering a building, or a MAN which covers a city or spread across the world which can be a WAN. All the networks formed for the purpose of communication either have an access point or a centre point of contact which manages the network or do not have any central point of contact. The former networks are called as infrastructure networks and later are the infrastructure less networks or ad hoc networks. The infrastructure network has fixed topology and central point of contact which is responsible for all the communication taking place between the devices or entities in the network. Exact opposite is the case with the ad hoc networks. The networks which are formed for purpose only are called as ad hoc networks. These networks are established for a particular purpose, this purpose can be exchange of information. Once the purpose is completed the connection is broken or terminated. They lack infrastructure and do not have any central point of co-ordination. Also the nodes in the network keep on changing the topologies with time. Any node or device taking part in communication is identified by a unique address.

Addressing is a main and very important, challenge in ad-hoc networks as the nodes dynamically change their topology and lack central point of contact. Ad hoc networks cannot use any protocols like DHCP or Network Address Translation. A central server assigning the addresses to the devices is not possible in ad hoc networks which is used in DHCP.A unique addressing scheme based on sequence filters is proposed in this paper which not only dynamically assigns addresses to the nodes in the network but also with less amount of control overhead and more packet delivery ratio. Moreover to detect the partition and merging events a hashing is used instead of random numbers.

Address collisions should be avoided. No two nodes at a given instant of time in the same partition should have same address. Secu rity should also be considered. The protocol should check if the node joining a network is authorized node or an adversary node. If a node utilizing a particular IP address joins another partition its address should become available to other nodes in the networks. The protocol should consider the dynamically changing topology and partition

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

and merging events in the network. Addresses should be assigned with less amount of control overhead and minimum delay [1].
MANETS are usually used for many distributed applications like sensing, providing internet access to unreached communities, disaster handling, because of the lack of central administration in these networks. The distributed network control may be disrupted by several factors, including Network Partitions caused by node mobility, fading channels, and nodes joining and leaving the network. The frequent network partitioning due to the node mobility is an usually neglected issue in Adhoc networks. It becomes even more difficult to assign addresses in these networks, as the environment is ever-changing. This paper proposes and analyses an efficient approach – Filter Based Addressing Protocol (FAP). It contains of a distributed database stored in filters that contain already allocated addresses in a compact manner.
We consider two filters – Bloom Filter and Sequence Filter in designing a filter-based protocol that assures both the univocal address configuration of nodes that join the network and the detection of address-collisions after the merging of partitions. We propose the use of these filters as an identifier for partition, to easily detect the partitions in the networks. All the neighbours in the network, distribute the hash these filters among themselves, and maintain them. Because of this, nodes can detect address collisions with a very small control overhead. Because of this feature, our proposal is a robust addressing scheme as itguarantees that all nodes share the same allocated list.

II. RELATED WORK

A hardware based addressing scheme was proposed which uses the MAC address of a device to assign the unique IP address to the node. This works perfect for the IPV6 addresses. But ninety percent of the nodes still use IPV4 addresses and in these addresses the no of bits are smaller than the MAC address. The solution used is hashing the MAC address to fit in the address suffix. But this also includes random choice of address and does not guarantee a collision free address allocation [2].

A new addressing scheme called as duplicate addressing scheme was proposed. In this protocol, every joining node randomly chooses an address and floods the network with an Address Request message (AREQ) if the randomly chosen address is already allocated to another node; this node advertises the duplication to the joining node sending an Address Reply message (AREP). When the joining node receives an AREP, it randomly chooses another address and repeats the flooding process. Otherwise, it allocates the chosen address. But the drawback of this method is that it does not take into account network partitions which are abruptly done at any time in the ad hoc networks [3].

A few extensions to duplicate addressing scheme are also proposed. These extensions use hello messages and partition identifiers. A group of nodes changes its partition identifier whenever it identifies a partition or when partitions merge. A protocol based on DAD is also used to solve address collisions in the presence of network merging events. This protocol considers that two partitions are merging when a node receives a Hello message with a partition identifier different from its own identifier [4].

A weak DAD was proposed which uses a unique key and routing protocol in addressing. Every node is identified by its address and a key. The collisions with the other nodes are identified by information from the routing protocol. If some nodes choose the same address and key, however, the collision is not detected. Also in this case the routing protocol structure is changed. Weak Duplicate Address Detection (DAD) protocol requires each node in the network to have a unique key. Weak DAD requires that packets meant for one node must not be routed to another node, even if the two nodes have chosen the same address. This is achieved by using the key information for duplicate address detection .In this approach; the routing protocol related control packets need to be modified to carry the key information. In the weak DAD scheme, the packet can still be misrouted in the interval between the occurrence of duplicate IP addresses in the network and their actual detection [5].

MANET conf was proposed after weak DAD. Two types of address lists are present, first allocated and allocation pending. A joining node asks for an address to a neighbour, which becomes a leader in the address allocation procedure. The leader chooses an available address, stores it on the Allocated Pending list, and floods the network. If all nodes accept the allocation request and positively answer to the leader, then the leader informs the allocated address

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

to the joining node, moves the allocated address to the Allocated list, and floods the network again to confirm the address allocation [5].

Another addressing scheme based on high entropy is used. The first node in the network is called as Prophet chooses an address. Then it assigns address to any node which contacts it randomly. Thus an address assignment tree is constructed. Prophet does not flood the network as a result the network overhead is limited. But this protocol requires large address range than any of the previous protocols to guarantee that no address is repeated. So to avoid duplication mechanism like DAD is required which increases the protocol complexity and overhead too [6].

A Dynamic addressing protocol was proposed. In this each node has its own address set. This node subdivides its available address set with joining node and assigns the joining node with the available address from the address set. This method works perfect for the small ad hoc networks. But in large ad hoc networks the problem occurs when the all the addresses in the address set are being assigned. ThenDAP requires the use of DAD in case of merging events which in turn increase the control overhead [7].

III. PROPOSED PROTOCOL

The proposed protocol, Filter – Based Addressing Protocol (FAP), reduces the control load and improves the detection of partition merging without the need for high storage capacity and auto-configures the network addresses dynamically. These results are achieved using small filters and an accurate mechanism to update the states of nodes. Instead of random numbers, it uses Filter-Signature (i.e., hash of the filter) as a partition identifier. As a result, the filter signature changes, with a change in the set of assigned addresses. This filter is placed at every node, to simplify the problems of frequent node joining and to reduce the control overhead.

FAP maintains a distributed database of the currently allocated addresses in a compact manner in filters. The two different filters that are used are Bloom Filter and Sequence Filter. Filter signature, which is a hash of these filters, is an important feature used to easily detect merging of the partitions, which may result in address conflicts.

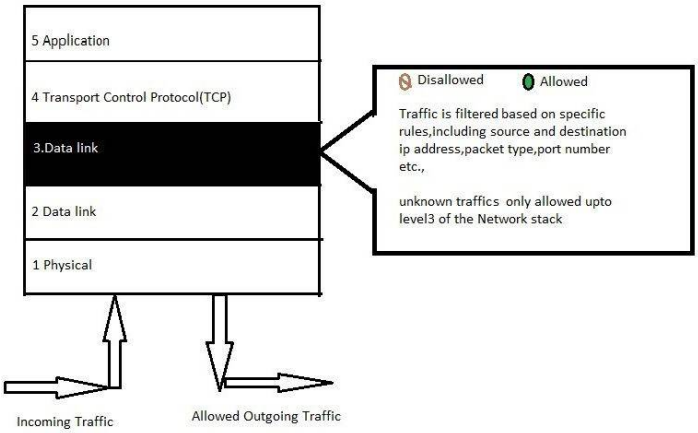

Fig. 1: Filtering of Traffic at different layers

Bloom Filters: The bloom filter is used as a partition identifier and sequence filter is used as a storage filter used to store the unique IP addresses. Bloom filter is a data structure which contains n bits. This n bit vector is composed of set of A= {a1, a2…an}.At first all the bits are set to zero. Each element is then hashed by each of the hash functions. Any kind of hashing system can be used like MD5 or a lookup table method. The output represents a position to be set as 1 on the n-bit vector. This hash of the filter is used as a partition identifier which is unique for all the nodes present in a single partition. Here usage of hash filters instead of random numbers reduces the probability of address collisions. This helps to reduce the address collisions with less amount of control overhead in partition merging events. This hash of the filter which is the partition identifier is periodically advertised in the network and thus partitions are detected.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

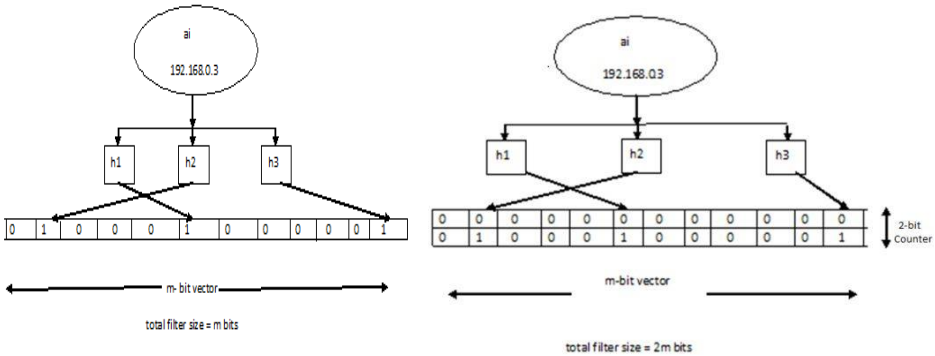

Fig.2: (a) Bloom filter having k=3 hash functions and m=12 bits of filter size (b) 2-bit Bloom filter

Sequence Filter: The sequence filter compacts the addresses and stores them in a sequence. The first address in the filter is called as initial address. It concatenates this address with an r-bit vector where r is the address range defined by the network suffix. Here a term named „delta‟ is used. Thi ves the distance between the initial address suffix a
(0) suffix and current element suffix which is denoted by a (i) suffix. If the bit is 1 then the chosen address is already present in the address filter and if the bit is 0 then the address is not present in the address filter and it can be allocated to other node requesting for the address.

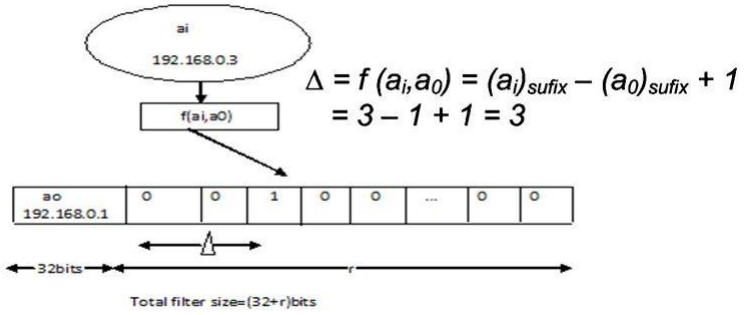

Fig. 3: Sequence filter, with an address range of r=254 addresses

In the proposed addressing method network prefix of 254 addresses is defined. The nodes in the network randomly choose addresses in the network at first. Whenever the new node joins the network selects an IP address randomly. Then it calculates the delta a. If delta position is found out to be 1 then the address is being used by some other node for communication. If the position indicates 0 then the address is available and the new node can choose the address and further use for communication. This method decreases the control overhead, increases the packet delivery ratio, decreases no of message drops.

By the use of filters the nodes are dynamically assigned IP addresses. The protocol also takes into consideration the partition and merging events which are prominent or very usual in ad hoc networks. The control over head is reduced. Number of message drops is also reduced. Delay is reduced as the whole IP address has not to be checked. By the use of sequence filter checking of the delta position is to be done. If it is 1, the IP address is already assigned and if it is 0, then the IP address is not used and can be assigned to any of the node [9].

There are four levels in FAP.

A. NETWORK INITIALIZATION:

There are two types of initializations. One among them is Gradual initialization. Here the node which wants to join will reaches one after another with long interval between them. Another one is abrupt initialization where all nodes reach at the same time. FAP suits well for both of them by using HELLO messages and AREQ messages. Initial node chooses the partition identifier and the remaining nodes are managed by the first node. Node uses HELLO messages to show its current status.AREQ is used to show that available address is already allocated.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

B.JOINING NODES:

The node which wants to join wait for some time The node itself acts as a starting node if it does not get any HELLO message. It acts as a joining node if it receives the HELLO message.

C. ASSIGNING ADDRESS:

An initiator node, which is the first to join the network, chooses an address randomly, using the address range present in the bits of the network prefix, creates an empty address filter, and starts the phase of network initialization. In this phase, the network is flooded N_f times with AREQ messages to make sure that the AREQ message is received by all the initiator nodes. The node leaves the initialization phase after waiting a period T_w and inserts all the addresses with AREQs in the address filter. After this, the node sends Hello messages with the address filter signature that is a hash of the filter. This filter signature identifies the network and is used in detecting partitions. If the initiator node receives AREQ with the chosen address and a different identifier number, an address collision occurs. Then, the node has to wait for a T_c period and choose a different available address and send a different AREQ. After a time T_c, the probability of selection of a used address will be reduced, which results in the decrease of probability of collisions, and, reduces the network control load.

D. NETWORK MERGING EVENTS:

To detect merging events, the neighbours in the network check if the signature in the message is the same as its own, after receiving the Hello message. The joining node, now, asks for the host node (source of the first listened Hello message) to send the address filter of the network, using an Address Filter (AF) message. After the host node receives the AF, it checks the bit I. If I=1, it indicates that the message has originated from the joining node. Further, the host node replies to the request with a AF with R bit set as 1, suggesting that the AF is in reply to a previous filter request. When the joining node receives an AF reply message, the address filter is stored, a random available address is chosen, and the network is flooded with an AREQ to allocate the latest address which, then, updates the filter messages of the other nodes.

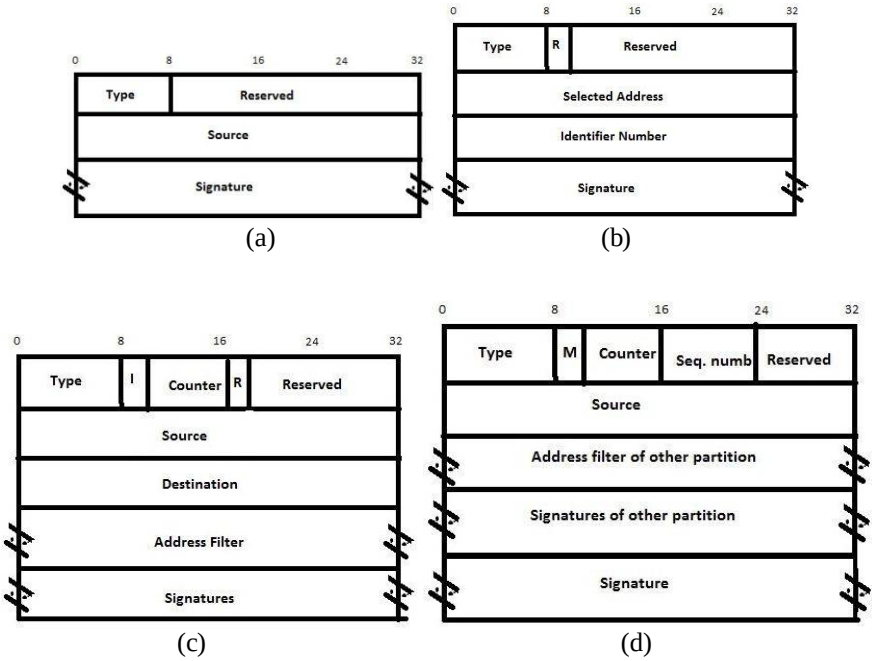

Fig 4: Messages for FAP for initialization, node joining, and partition merging (a) Hello (b) AREQ (c) AF (d) Partition

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

IV. PSEUDO CODE

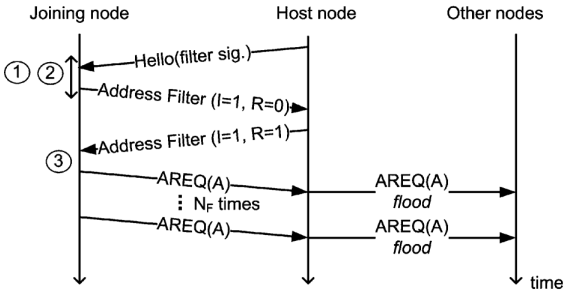

Fig. 5: FAP Scheme for Node Ingress

FAP Scheme for Node Ingress:

Step 1: Wait for Hellos for Time $(T_L)^*$

Step 2: Identify a joining node procedure

Step 3: Store filter and select an available address; such as A.

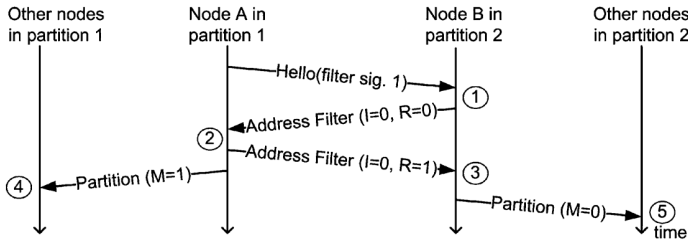

Fig. 6: FAP Scheme for Partition detection and merge

FAP Scheme for Partition detection and merge:

Step 1: Detect a merge event due to a different filter signature in the Hello

Step 2: Merge filters

Step 3:Merge filters and check for collisions because partition 1 is greater than partition 2

Step 4: Merge filters

Step 5: Merge filters and check for collisions because M=0

V. SIMULATION RESULTS

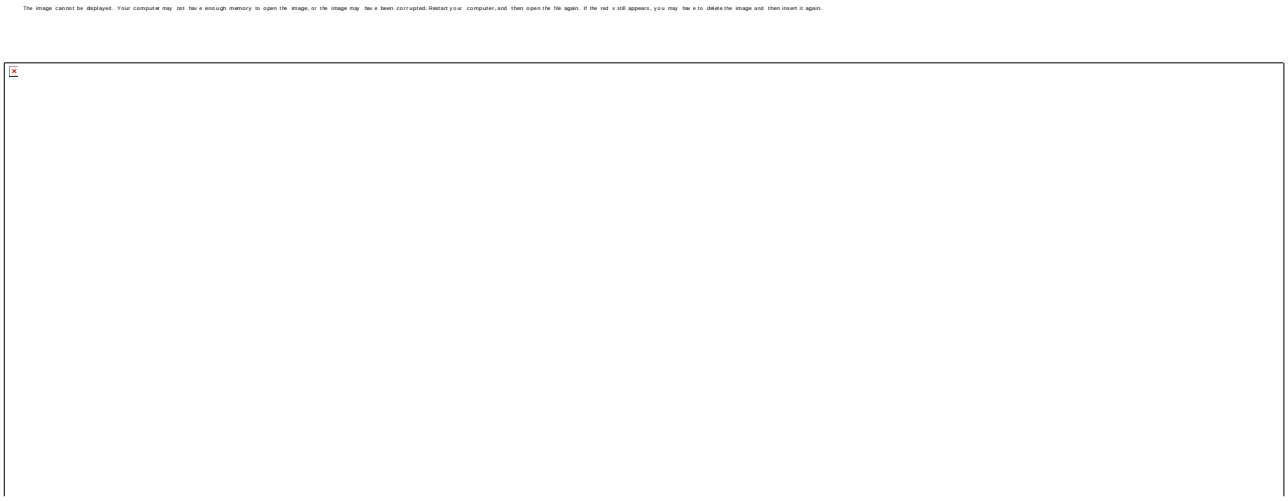

Fig. 7: Impact on the network on the number of nodes, density, number of transmissions of flooding messages.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

(a) Control overhead as per the number of nodes (b) Average delay as per the number of nodes (c) Number of collisions as per the number of nodes (d) Control overhead as per the network density, where N=36 nodes (e) Number of collisions as per the Network density N=36 nodes (f) Control overhead, as per N_F, N=100 nodes (g) Average delay as per N_F, N=100 nodes (h) Number of collisions, as per N_F, N=100 nodes

VI. CONCLUSION AND FUTURE WORK

In this paper we proposed a filter based addressing protocol which is distributed, and a self managed addressing protocol that fits mainly for dynamic adhoc networks with fading channels, frequent partitions, joining nodes etc., With the small number of control messages it will easily detect the partition accurately using the hash of the filter. Moreover, our filter-based protocol increases the protocol robustness to message losses, which is an important issue for ad hoc networks with fading channels and high bit error rates.

REFERENCES

1. Abulshah,Ashfaq Khokhar,and Mohsen Guizani, "A Survey of Secure Mobile Ad hoc Routing Protocol",in IEEE communications surveys and tutorials,vol 10,no 4, pp 78-93, 2008
2. B.Parno,A.Perrig,and V.Gligor,"Distributed detection of node replication attacks in sensor networks,"in Proc.IEEE
3. Symp.Security Privacy,May 2005,pp.49-63. M. Fazio, M. Villari, and A. Puliafito, "IP address autoconfiguration in ad hoc networks: Design, implementation and measurements," Comput. Netw,vol. 50, no. 7, pp. 898–920, 2006.
4. N. H. Vaidya, "Weak duplicate address detection in mobile ad hoc networks," in Proc. 3rd ACM MobiHoc, pp. 206–216, 2002
5. S. Nesargi and R. Prakash, "MANETconf: Configuration of hosts in a mobile ad hoc network," in Proc. 21st Annu. IEEE INFOCOM, vol. 2, pp. 1059–1068, Jun 2002
6. H. Kim, S. C. Kim, M. Yu, J. K. Song, and P.Mah, "DAP: Dynamic address assignment protocol in mobile ad-hoc networks," in Proc. IEEE ISCE, pp. 1–6, Jun. 2007
7. Deke Guo,Member IEEE JieWu, Fellow IEEE Honghui Chen, Ye Yuan, and Xueshan Luo;" The Dynamic Bloom Filters", IEEE transactions on knowledge and data engineering, vol. 22, no. 1, pp-120-132,Jan 2010
8. H. Zhou, L. Ni, and M. Mutka, "Prophet address allocation for large scale MANETs," in Proc. 22nd Annu. IEEE INFOCOM,vol. 2, pp. 1304–1311, Mar. 2003
9. Natalia Castro Fernandes, Marcelo Duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte", An Efficient and Robust Addressing Protocol for Node Auto configuration in Ad Hoc Networks", IEEE transactions on networking, vol. 21, no. 3, pp 845-856, Jun 2013

BIOGRAPHY

K. Sekar is an Associate Professor in the Department of Computer Science and Engineering, S.V. College of Engineering, Tirupati, Andhra Pradesh, India. He has published several papers in several national and international Journals and presented papers in Conferences. He is pursuing his Ph.D in S.V.University, Tirupati. His areas of Interest are Software Engineering, Computer Programming, Data WareHousing and Computer Networks.