Advances in Mechanical Engineering and its Applications (AMEA)
Vol. 2, No. 3, 2012, ISSN 2167-6380

www.worldsciencepublisher.org

An Effective Address Allocation and Routing Mechanism for Confidential Communication in MANET

[1]Vishesh Kumar Singh, [2]Arun Kumar Giri

[*1, 2] Shobhit Institute of Engineering & Technology, Gangoh, Saharanpur, India

Email: visheshkumarsingh@gmail.com

Abstract – A Mobile Ad Hoc Network (MANET) consists of a set of identical mobile nodes communicating with each other via wireless links. The network's topology may change rapidly and unpredictably. In mobile ad hoc networks, however, there is no fixed infrastructure and nodes do not have access to a centralized server to acquire IP addresses. And, due to node mobility, network partitions and merges are frequent occurrences. Such events create the possibility of duplicate addresses within the network. Therefore, a centralized approach cannot be applied in these networks; a distributed and dynamic mechanism is needed for nodes to acquire and maintain a unique IP address in mobile ad hoc networks. Further, due to unavailability of centralized server and frequent mobility of nodes any malicious node can enter in network which causes the malfunctioning of network. If we are performing any confidential communication such as in Military Operation, Research Activity Communication then any malicious node can breach the confidentiality or may mal-function the network by disconnecting the route or denial of the services. So with a dynamic address allocation scheme, we also need a confidential routing mechanism. In this paper we proposed routing mechanism by using various parameters like efficient address allocation using DAD and the trust based forwarding scheme of node selection for setting up a route by using request reply technique over it.

Keywords– Address Allocation; DAD; IP Address; Request Reply Method; Trust Counter

1. Introduction

1.1. MANET

MANET (Mobile Ad Hoc Networks) is a wireless network in which all movable nodes can communicate with each other without depend on a fixed infrastructure. Here packet forwarding and routing is achieved by intermediate nodes. In routing protocols, a routing path is acquired when a source desires to send data packets to destination. In order to send and receive packets between two nodes, they should have their unique address in the network. Since IP is also used in MANETs, a unique IP address should be assigned to each node. Therefore, IP address auto configuration schemes have been developed to remove the overhead of manual configuration.

1.2. IP Assignment

In general, we can categorize the IP assignment solutions to be either reactive or proactive. Reactive protocols require a consensus among all the nodes of the network on the new IP address that is to be assigned, whereas in the proactive approach, each node can independently assign a new IP address without asking permission from any other node in the network.

1.3. DAD

Mobility is one of the reasons for partitioning of the network. When a node having unique IP address in one partition, moves into another partition, there may arise a chance of duplication of the IP address. Since, IP address has to be unique, address conflicts need to be detected through a DAD (Duplicate Address Detection) procedure. Duplicate Address Detection (DAD) is the methodology introduced for monitoring the repetition of IP addresses by the individual nodes itself.

1.4. Multicast

Multicast is the characteristic which shows the multiple nature of packet transmission. The packet in multicast environment can be transmitted in both forward and backward direction. In multicast network a node can send the packet to multiple destinations. A node working as source node at any time can send packet in forward direction to many particular destinations and the receiver node can send back the packet to source as reply.

1.5. Trust Based Forwarding Scheme

A trust based security protocol based on a MAC-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. A trust based packet forwarding scheme for detecting and

isolating the malicious nodes uses the routing layer information. It uses trust values to favour packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In this scheme the source node can be able to select the more trusted routes rather than selecting the shorter routes. It isolates the malicious nodes from participating in the network. So the potential damage caused by the malicious nodes is reduced.

1.6. Problem Identification

In wireless network the effective dynamic address allocation with no address duplication for each node is the major constraints. The scheme should be such that it can handle various networks problem such as partitioning, node failures, and binding with reactive and proactive routing protocols etc. Further, the current wireless network is very much prone to the malicious node due to mobility of node and unavailability of centralized server. Due to malicious node networks allow many different types of attacks. Although the analogous exploits also exits in wired networks but it is easy to fix by infrastructure in such a network. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. In this the attacks are classified as modification, impersonation, fabrication, wormhole and lack of cooperation. So, for effective address assignment and to make communication possible in confidential manner we have to make a sufficient mechanism to solve the above problems.

1.7. Paper Organization

Our purpose to organize this paper is to provide a unique IP address to each node and to create a suitable route through which the communication can be made possible in confidential manner. In this paper the solution is divided in three phase: (1) First phase deals with the unique IP address allocation with the help of RA2DA2 [19] method which uses the reactive approach with DAD to solve the various allocation problems, (2) Second phase deals with the detection of malicious node present in the network with the help of trust based forwarding scheme [20] in which the malicious nodes are isolated from participating in the network. So the potential damage caused by the malicious nodes is reduced, (3) Third phase discuss about the REQUEST-REPLY approach to select the appropriate and good performance nodes/routes from available routes after isolating the malicious nodes. Using all these three parameters we are proposing a routing mechanism which will solve the problem of unique IP address allocation with the isolation of the malicious node from the route for proper and confidential communication.

2. Literature Survey

In an autonomous ad hoc mobile network the nodes can be uniquely identified by an IP address with the only premise that this address must be different from that any other node in the network. The configuration process is the set of steps through which a node obtains its IP address within the network. There are three mechanisms in [1] to set addresses: Stateless and Stateful and Hybrid. Instead of the assignment of addresses by a second entity, stateless auto-configuration allows the nodes to construct addresses by themselves, usually based on a hardware ID or a random number. Mobility is one of the reasons for partitioning of the network. When a node having unique IP address in one partition, moves into another partition, there may arise a chance of duplication of the IP address. Since, IP address has to be unique, address conflicts need to be detected through a DAD (Duplicate Address Detection) procedure. Duplicate Address Detection (DAD) is the methodology introduced for monitoring the repetition of IP addresses by the individual nodes itself. [3] Presents the importance of detection of IP address conflicts and different schemes introduced for detection.
Weak DAD, presented in [4], is an approach to prevent a packet from being routed to a wrong destination, even if duplicate addresses exist. Nodes in the network are identified not only by the IP address, but additionally by a key, which can be based on a hardware ID or a random number. If a node receives a packet containing an IP address that is stored in its routing table, but with a different key, an address conflict is detected. It will only work with the proactive one that updates the routes constantly, but with a reactive one there will be nodes that could never detect the duplicity of IP addresses. In the Strong Duplicated Address Detection (DAD) scheme [5] the node chooses two IP addresses: temporary and tentative. It will only use the temporary address for the initialization while it detects if the tentative one is unique or not. The detection method consists of sending a message ICMP destined directly to this address. If it receives a response, this IP address is being used so the process will be resumed. If it does not receive a response, the message will be sent a certain number of times to make sure that the address is unique. It would not work for temporary disconnections or losing of the network. In Address auto-configuration with address Reservation and Optimistic duplicated address Detection (AROD) [6], the address reservation is based on the existence of nodes that have an IP address reserved to deliver it to the new nodes that enter. Two types of nodes will exist: (1) Agents type 1 with a reserved IP address, apart from the IP address that has its network interfaces. When a node joins the network, this reserved IP will be assigned to it immediately. (2) Agents type 2, which do not have reserved IP addresses. If a node that joins newly asks one of these for an IP address, this node borrows the reserved address of one of its neighbours who is of type 1, and it is assigned to the new one immediately. HCQA [7] is a dynamic address configuration protocol for mobile ad

hoc networks that provides address assignment to mobile nodes during the formation and maintenance of a network. The protocol assigns unique addresses and can be combined with a variety of routing schemes. Further, the address authority aids in the detection of duplicate addresses and handles address resolution after network partitions and merges. In Zeroconf [8] problem of node configuration in the absence of servers dedicated to such a task has been the focus of the Zeroconf working group of the Internet Engineering Task Force (IETF). However, the solutions proposed by the Zeroconf working group are not directly applicable to MANETs. Zeroconf solutions are intended to assign link-local unique IP addresses to nodes connected in the following topologies: (1) a single network segment to which all nodes are connected so that each can directly communicate with the other through link-layer broadcasts and multicasts. (2) Multiple network segments connected to the same router. These two topologies capture only a small subset of possible MANET topologies. All MANET nodes are not guaranteed to be reachable from each other through at most one intermediate node. Hence, link-level broadcasts are not guaranteed to reach all MANET nodes. As a result, duplicate address detection (DAD), as described in the Zeroconf solutions is not feasible. In MANETconf [9] a new node entering the MANET request for configuration information from its neighbours. One of these neighbours initiates the IP address allocation process for the new node. This approach handles network partitioning and subsequent merging. Mohsin and Prakash [10] propose a stateful protocol which uses Multiple Disjoint Allocation Tables. In this approach every node has a disjoint set of IP addresses that can be assigned to new nodes, is said that as node owns these pool of IP addresses hence no quorum is required to make a decision. This approach uses a proactive scheme for dynamic allocation of IP addresses in MANETs. This protocol employs the approach described in MANETconf to solve network partitioning. The major drawback of this protocol is that the synchronization depends on the existence of a reliable broadcast and such a thing does not exist in a distributed mobile environment, thus one can question the robustness of this protocol. An improvement of [10] can be found in [11], where Thoppian and Prakash propose a dynamic address assignment based on a so-called buddy system that manages mobility of nodes during address assignment, message loss, and network partitioning and merging. However, the IP address allocation can generate a high overhead of control messages while it does a global search and the address recovery (to avoid missing addresses) requires diffusion messages by a flooding process. In addition, union and partition may incur in high overhead because of the global nature of this protocol. Extensible MANET Auto-configuration Protocol (EMAP) [12] is based on the idea of a protocol of REQUEST/REPLAY messages. The main advantage of this protocol is the possibility of doing it extensible, i.e., it can include new functionalities in the future that are analyzed in a theoretical way, such as Domain Name Server (DNS). The route discovery mechanism among nodes is similar to the Ad Hoc On-Demand Distance Vector (AODV) [13] protocol.

The protocol in [14] proposes a scheme where the nodes are classified into coordinator and common nodes. The first coordinator assigned to initiate the IP address assignment is the so-called C-root. The coordinators manage the IP address pool and they are responsible for assigning an IP address to a node which has just joined the network. The nodes that wish to join the network will interchange HELLO messages to find the coordinator node nearest and to obtain a new IP address from that coordinator node. To maintain the IP address pool efficiently, the coordinator nodes are distributed in a tree topology called C-tree by exchanging HELLOs. In D2HCP [15] protocol each node is responsible for managing a range of addresses. When a new node wants to begin participating in the network, one of the nodes within the network gives half of its address range to the new node. In the case of any adjacent node not having free addresses, but free addresses do exists, a request to a network node that has free addresses is done. In this operation mode is based on distributed nature of the protocol. To keep updated information about free addresses owned by each node, the traffic control packets from OLSR [16] protocol is used in D2HCP. It does not consider network partition and merging and this protocol have been designed to work together with OLSR which is proactive in nature. Passive Auto configuration for Mobile ad hoc Networks (PACMAN) [17] is a passive auto-configuration protocol for MANET. It uses elements from stateless and stateful protocols, so it could be considered somewhat hybrid. Its operation is based on each node assigning itself an address when joining the network, and passive monitoring of communications for the duplicate address detection. The method used to choose the own IP address consists of a probabilistic algorithm. In [18] a routing mechanism is proposed by using various parameters like efficient address allocation over mesh based and tree based multicast through the random casting method of node selection and finally set up a path by using request reply technique over it. The proposed routing mechanism will be helpful for disaster area and enhance quality of service of communication. RA2DA2 [19] present a reactive address allocation scheme for dynamic IP address assignment with DAD for address conflict detection. In this solution uses the concept of reactive allocation and takes into consideration the previously unsolved issues like partitioning and merging and abrupt departure of nodes from the system. It also show the binding nature of its technique with any of the routing protocols types i.e. reactive or proactive routing protocols. In [20], a trust based packet forwarding scheme has been designed for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favour packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In ND-MIM [21] establishes the main route by the mechanism based on AODV, then backup route search process is taking place while data is transmitted to reduce the transmission delay. This process finds the route that is node-disjoint and have less interference from the main route by not selecting nodes participated in the

main route using Hello packet. When either of the main route or the backup route is broken, data is transmitted continuously through the other route and the broken route is recovered by the route maintenance. In [22], trust based Adhoc On-Demand routing protocol has been proposed. It introduce extra field in the route request format. This field indicating trust value is updated on every successful data transmission. The forthcoming data transmission is based on the route selection value calculated for each RREQ path. This route selection value is used to select most trusted path. In [23], [24], [25], [26], [27], [28] a novel work for mobile ad hoc network and artificial bee colony has been proposed. This paper gives quality of service needed for the mobile ad hoc network and an improved local search method for artificial bee colony. The paper has made an excellent approach for solving the real world problem.

3. Proposed Work

In this paper we have proposed a confidential routing mechanism with unique IP address assignment. The solution is divided in three phases:

3.1 First Phase: Unique IP Address Assignment

There are various techniques for unique IP address allocation. But for allocating the IP address we have chosen RA2DA2 [19] method due to his various properties.

Table1. Classification of Allocation Schemes

Classification	Binding Nature (With Reactive & Proactive routing Protocol)	Partition Handling	Overhead
ManetConf	No	Yes	Low
EMAP	Yes	No	Low
D2HCP	No	No	Medium
SDAD	No	Yes	High
WDAD	No	Yes	Low
PACMAN	Yes	Yes	High
RA2DA2	Yes	Yes	Low

From the Table 1 we can conclude that the RA2DA2 scheme is better technique due to his binding nature and partition handling capability.

RA2DA2 scheme is divided in two parts. First parts deals with the Duplicate Address Detection technique in which the scheme introduced two new terms for two nodes i.e. MAIK (main address information keeper), & BAIK (backup address information keeper). Both nodes used DAD and keep the state information of the network including network identifier, IP address of all the nodes with their lifetime. This information is helpful in network partitioning and merging and makes the solution to be bind with any of the routing protocols type's i.e. reactive or proactive routing protocols.

Second parts deals with the Reactive Address Allocation Technique in which a newly node proposes a candidate IP address for his IP address assignment. If the proposal is accepted by all the nodes that are part of the MANET, the proposed address is assigned to the newly arrived node. Otherwise, another candidate IP address is chosen and the process is repeated (for a finite number of times). Every node has to register with the MAIK which confirms its IP address allocation through acknowledgement and start its lifetime. At the end of life time each node has to re-register itself for further communication. When merging of network occurs then MAIK is responsible for detecting IP address conflict. The newly joined node becomes the MAIK and previous MAIK becomes the BAIK.

3.2 Second Phase: Removal of Malicious Node

For finding and removing the malicious node from the network we have used trust based forwarding scheme [20]. In this protocol, by dynamically calculating the nodes trust counter values, the source node can be able to select the more trusted routes rather than selecting the shorter routes. This protocol marks and isolates the malicious nodes from participating in the network. So the potential damage caused by the malicious nodes is reduced. It makes changes to the AODV routing protocol. An additional data structure called Neighbours' Trust Counter Table (NTT) is maintained by each network node.

For a node n_k, if $Tc_k < Tc_{thr}$, where Tc_{thr} is the trust threshold value and Tc_k is the calculated threshold of each individual node through the above scheme, then that node is considered and marked as malicious. The same trust based forwarding scheme procedure is repeated for the other routes R2, R3 etc and either a route without a malicious node or with least number of malicious nodes, is selected as the reliable route.

3.3 Third Phase: Request/ Reply Approach

The Source node want to communicate first prepares RR packet and then broadcast that packet to its available child nodes, after finding the best routes by eliminating malicious node through the trust based forwarding scheme. The child node further broadcast this packet to their child nodes and this process will be continued until the packet does not reach to destination node, during this process the RR flag is set. And when the destination node received the RR Packet, it prepares a RP packet and sends

them to its parent. The parent nodes further send this packet to their parents and the process will be continued until the packet does not reach to the source node, and during this process the RP flag is set.

RR packet contains the following information in Table 2:

Table2. RR Packet

Source Node Address	Previous Node Address		Next Node Address
Sequence No	Route Request (RR) Flag	Power	Antenna Gain

1. Source Node Address: It is the address of the node originating the packet.
2. Previous Node Address: It is the address of previous node that RR packet has visited during its forward movement.
3. Sequence Number: The sequence number assigned to every packet delivered by the source that uniquely identify the packet.
4. Routing Request Flag (RR Flag): This flag is set for the duration of forward travel of RR packet from source to destination.
5. Power: This is the power at which a node has transmitted the packet to neighbour.
6. Antenna Gain: This is gain of antenna at the forwarding node to forward RR packet to its neighbour.

RP packet contains the following information in Table 3:

Table3. RP Packet

Receiver Node Address	Previous Node Address		Next Node Address
Sequence No	Route Reply (RP) Flag	Power	Antenna Gain

1. Receiver Node Address: It is the address of the node receiving the RR packet and sending RP packet.
2. Source Node Address: It is the address of the node from which the node receives the RR packet.
3. Power: This is the power at which a node has send reply packet to source.
4. Sequence Number: The sequence number assigned to every packet delivered by the receiver that uniquely identify the packet.
5. Route Reply Flag (RP Flag): This flag is set for the duration of reverse travel of RP packet from destination to source.
6. Antenna Gain: This is gain of antenna at the replying node to send RP packet to source.

4. Algorithm

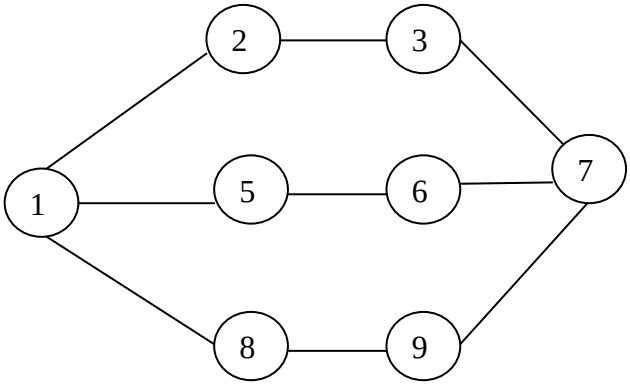

Figure1. Network Structure

Suppose that in figure 1 source node 1 want to communicate with destination node 7 and the trust threshold value Tc_{thr} for determining the malicious node for every node be 0.5.

Step1. The IP address assignment of all nodes can be done by using RA2DA2 method as shown in Table 4.

Table4. IP Address Allotted Table

Nodes	Allocated IP Address of the Nodes
1	195.180.200.6
2	194.170.30.15
3	195.180.200.3
5	198.200.130.52
6	195.180.200.6
7	195.180.200.7
8	198.200.130.55
9	198.130.50.165

Step2. Perform Trust Based forwarding scheme on available nodes.

1. After calculating the trust of each node by using trust scheme [20] and comparing the trust Tc_k of each node n_k with the trust threshold $Tc_{thr,}$ suppose we get the Table 5.

Table5. Assigned trust for the nodes

Trust Values	Nodes							
	1	2	3	5	6	7	8	9
Trust (Tc_k)	0.7	0.51	0.63	0.49	0.71	0.6	0.4	0.39
Threshold	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5

2. The nodes whose trust Tc_k values are greater than threshold trust Tc_{thr} are reliable nodes and whose trust Tc_k values is less than threshold trust Tc_{thr} are malicious node and must be isolated. The available paths to reach from source node 1 to destination node 7 are, 1-2-3-7, 1-5-6-7, and 1-8-9-7 as shown in figure 2.

These three paths have some intermediate nodes to reach from source node 1 want to communicate with destination node 7. Each path may have malicious nodes in it to reach, from source to destination node. A route without a malicious node or with least number of malicious nodes is selected as the reliable route.

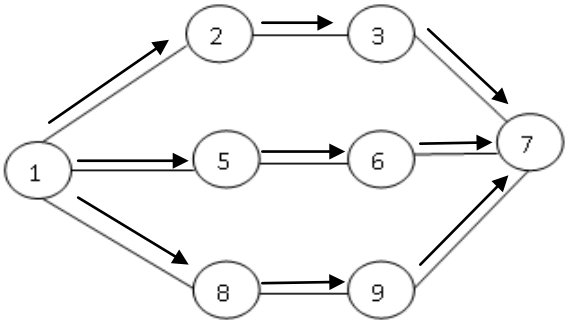

Figure2. Available Paths

3. Now from the available paths only those paths are being selected which have no or minimum number of malicious node. For this we find out the no. of malicious node in each route.

Table6. Malicious Nodes in Routes

Route No.	Routes	Number of Malicious Node
01	1-2-3-7	0
02	1-5-6-7	1
03	1-8-9-7	2

4. From the Table 6 it is cleared that path no 2 and 3 can't be selected since it has malicious node. Path number 1 is free from malicious node, so it can be selected for the communication i.e. 1-2-3-7.

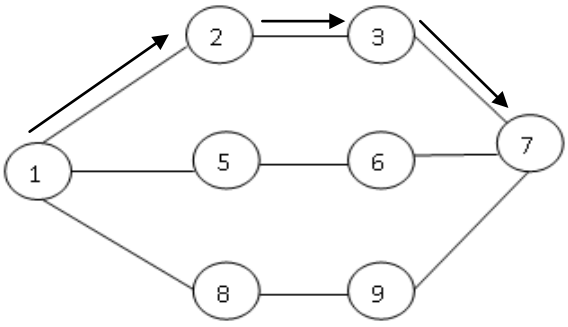

Figure3. Selected Path

If any how there is no path without malicious node then select the path with minimum number of malicious node i.e. path number 2 and so on.

Step3. Now the route Request/Reply Request for the packet forwarding from source node to destination node can be done with the selected path as follows:
1. The source node 1 broadcast a RR packet to available nodes. And the nodes further forward this packet to other nodes.
2. The above process will continue until the packet did not reach at the required destination.
3. After receiving RR packet, the destination node sends back a RP packet to the node from which it receives RR packet. And the nodes further sends back this packet to appropriate node.
4. This process is continued until the RP packet reached to the source.
5. After completion of 1-4 the routes are selected for communication between source and destination.

5. Discussion

In [4], [9], [10], [11], and [15] the duplicate address detection is done by Proactive Routing Protocol. They all are totally dependent on proactive scheme in which each node maintains a routing table with an entry for every other node in the network.
In [6], [12], [14], and [15] the major issue of MANET i.e. network portioning and merging is not discussed. [5] Does not work well for temporary disconnections. In [8] DAD is not possible.
In [7] has one main problems, the overhead produced by the SDAD process and periodic messages of Address Authority creates overhead.
More than above there is needed to avoid malfunctioning of the network in presence of malicious node for confidential communication. [20],[21],[22] has given some of the technique for reliable communication.
In our approach all the above problem has been solved by using proper techniques. The unique IP address allocation problem has been solved by RA2DA2 technique, confidentiality problem and detection of malicious node has been solved by Trust based forwarding scheme and the routing of the packet from source node to destination node is done through Request Reply method.

6. Conclusion

In this paper we presented a routing mechanism by using various parameters like efficient address allocation using DAD and the trust based forwarding scheme of node selection for setting up a route by using request reply technique over it. We have addressed the issue of unique IP address assignment to nodes in MANETs in the absence of any static configuration or centralized servers. This purpose has been achieved through a reactive approach in managing duplicated addresses, as well as through appropriate choices in the use of network resources, in terms of quantity of information stored in the nodes. The protocol assigns unique addresses and can be combined with a variety of routing schemes. A trust based packet forwarding scheme is used for detecting and isolating the malicious nodes using the routing layer information for the confidential communication. Finally, the paper discuss about the REQUEST-REPLY approach to select the appropriate and good performance nodes/routes from available routes.

Acknowledgement

I will like to thanks the Guest editor Tarun Kumar Sharma of special issue "NICA", world science publisher who have given me the opportunity for this special edition. And also I will like to give my heartily thanks to the reviewer for his kind comments, which makes my paper up to the mark.

References

[1] L.J. Garcia Villalba, J. Garcia Matesanz, A.L. Sandoval Orozco, J.D. Marquez Diaz, Auto-Configuration Protocols in Mobile Ad Hoc Networks, Sensors 2011, submitted.

[2] Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, and E. Lear, Address Allocation in Private Internets, RFC 1918, Internet Engineering Task Force, Network Working Group, February 1996.

[3] S. Zahoor ul Huq, K.E. Sreenivasa Murthy, B. Sathya Narayana, D. Kavitha, Study of Detection of IP Address Conflicts in MANETS, Global Journal of Computer Science and Technology, April (2010) 23-26.

[4] N. H. Vaidya, Weak duplicate address detection in mobile ad hoc networks, Proc. of ACM MobiHoc 2002, Lausanne, Switzerland, June (2002) 206-216.

[5] C. Perkins, J. Malinen, R. Wakikawa, E. Belding Royer, and Y. Sun, IP Address Auto configuration for Ad Hoc Networks, I-D draft-ietf-manetautoconf-01.txt, November (2001).

[6] N. Kim, S. Ahn, Y. Lee, AROD: An Address Auto configuration with Address Reservation and Optimistic Duplicated Address Detection for Mobile Ad Hoc Networks, Computer Communication, (2007) 1913-1925.

[7] Sun Y., Belding Royer E.M., 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, June (2003).

[8] S. Cheshire, and B. Aboba, Dynamic Configuration of IPv4 Link Local Addresses, draft-ietf.zeroconf-ipv4-linklocal-03.txt (expires December 22, 2001), Internet Engineering Task Force, Zeroconf Working Group, June (2001).

[9] S. Nesargi and R. Prakash, MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network, Proceedings of INFOCOM 2002, (2002).

[10] M. Mohsin, and R. Prakash, IP Address Assignment in a Mobile Ad Hoc Network, Proc. IEEE MILCOM 2002, Anaheim, CA, Oct (2002).

[11] M.R. Thoppian, R. Prakash, A Distributed Protocol for Dynamic Address Assignment in MobileAd Hoc Networks, IEEE Trans, Mobile Comput, 5 (2006) 4-19.

[12] F. Ros, P. Ruiz, C.E. Perkins, Extensible MANET Auto- Configuration Protocol (EMAP), Internet Draft, March 2006, accessed on 25 November (2010).

[13] C. Perkins, and E. Royer, Ad Hoc on Demand Distance Vector Routing, 2nd IEEE Workshop on Selected Area in Communications, Feb (1999) 90-100.

[14] J.P. Sheu, S.C. Tu, L.H. Chan, A Distributed IP Address Assignment Scheme in Ad Hoc Networks, Int. J. Ad Hoc Ubiquitous Computing, March (2008) 10-20.

[15] L.J. Garcia Villalba, J. Garcia Matesanz, A.L. Sandoval Orozco, J.D. Marquez Diaz, Distributed Dynamic Host Configuration Protocol (D2HCP), Sensors (2011), submitted.

[16] P. Jacquet, P. Mühlethaler, T Clausen, A. Laouiti, A. Qayyum, and L. Viennot, Optimized Link State Protocol for Ad Hoc Networks, IEEE INMIC Pakistan (2001).

[17] K. Weniger, PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks, IEEE J. Sel. Area Commun, (2005) 507-519.

[18] A.K. Vatsa, Prince Chauhan, Meenakshi Chauhan, and Jyoti Sharma, Routing Mechanism for MANET in Disaster Area, IJNMT, May (2011) 49-60.

[19] Vishesh K. Singh, A.K. Tiwari, R. Dixit, RA2DA2: Reactive Address Allocation and Duplicate Address Detection Techniques in MANET, International Journal of Advanced Research in Computer Science and Software Engineering, July (2012) 281-287.

[20] A. Rajaram, Dr. S. Palaniswami, Malicious Node Detection System for Mobile Ad hoc Networks, International Journal of Computer Science and Information Technologies, (2010) 77-85.

[21] Rajendra Kumar Gupta, Node Disjoint Minimum Interference Multipath (ND-MIM) Routing Protocol for Mobile Ad hoc Networks, International Journal of Advanced Research in Computer Science and Software Engineering, March (2012) 128-131.

[22] R. S. Mangrulkar, Pallavi V Chavan, S. N. Dagadkar, Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT, International Journal of Computer Applications, October (2010) 36-39.

[23] Avanaksh Singh Sambyal, Prikhshayat Singh, Routing Misbehavior in MANets and How it Impact QoS!, Advances in Computer Science and its Applications, World Science Publisher, United States, March (2012) 84-88.

[24] Tarun Kumar Sharma, Millie Pant, V.P. Singh, Improved Local Search in Artificial Bee Colony using Golden Section Search, Journal of Engineering, 1:1(2012) 14-19.

[25] Tarun Kumar Sharma, Millie Pant, V.P. Singh, Adaptive Bee Colony in an Artificial Bee Colony for Solving Engineering Design Problems, Advances in Computational Mathematics and its Applications, 1:4(2012) 213-221.

[26] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini and V.Venkateswara Reddy, Authentication techniques for engendering Session passwords with colors and text, Advances in Information Technology and Management, 1:2(2012) 71-78.

[27] C.Narasimha and B.Jalaja Kumari, Secured Multicasting Over MANET's through EGMP, Advances in Information Technology and Management, 1:2(2012) 90-96.

[28] M. Sreedevi,.C.Narasimha and R.Seshadri, Efficient Data Delivery Over MANET's through Secured EGMP, Advances in Asian Social Science, 2:3(2012) 512-516.

Vitae

Vishesh Kumar Singh is working as Assistant Professor in CSE at Shobhit Institute of Engineering & Technology, Saharanpur, (U.P.), INDIA. He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech (CSE) from PSIT, Kanpur (U.P.). He has worked as software engineer in software industry. He has been in teaching from more than three years. During his teaching he has been active member of many Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Crawler.

Arun Kumar Giri received the M.Tech.degree in Computer Science Engineering from Shobhit University in 2010. He is also pursuing his Ph.D. Presently; he is working as Assistant Professor and HoD in Computer Science & Engineering department in Shobhit Institute of Engineering & Technology, Gangoh, Sahranpur, India. He is also Lab In charge of the college. He is also working as Training and Placement Co-ordinator for his college. He has a decade of experience in teaching and research areas. His areas of interests are MANET (Mobile Ad-Hoc network), DIP.