Research Journal of Applied Sciences, Engineering and Technology 7(18): 3763-3770, 2014
DOI:10.19026/rjaset.7.731
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 27, 2013 Accepted: September 27, 2013 Published: May 10, 2014

Research Article

An Efficient Algorithm for Conflict Free Address Auto Configuration in Self Configurable Networks

[1]Mukesh Chand, [2]H.L. Mandoria and [1, 3]R.C. Joshi
[1]Graphic Era University, Dehradun, India
[2]College of Technology, Pantnagar University, India
[3]Indian Institute of Technology, Roorkee, India

Abstract: Evolution of self configurable networks posses unpredictable challenges which are not faced by the traditional wireless networks. No standard solutions are available in the literature to overcome these problems. Due to faster growing field and importance of these networks we cannot ignore the challenges imposed by the networks. Self configurable networks like Adhoc network, wireless sensor network and mesh network, they are in just evolution phases. In Adhoc networks nodes are capable to form a temporary network dynamically without the support of any centralized infrastructure. They are highly cooperative nodes. In WSN networks are formed to fulfil the spatial requirement. And mesh network is more complicated than any other network. Address auto-configuration of nodes is an important issue on self-organizing networks and discussed very little by the researchers. In this study we have discussed about the issues and challenges for the address auto configuration problems in various situations in the self configurable networks and considering delay, throughput, route discovery time, route request time as important factors we have proposed a novel and an efficient algorithm for conflict free address auto configuration in self configurable networks.

Keywords: Auto-configuration, Mobile Adhoc NETworks (MANET), Self Configurable Networks (SCN), Wireless Mesh Network (WMN), Wireless Sensor Networks (WSN)

INTRODUCTION

More and more computing devices are evolving. These devices may vary in size, capabilities, mode of interaction and so on. As a result we are moving toward a world in which computing is omnipresent. Many modern devices (e.g., smart printers, PDAs, smart phones and cameras) support multiple communication channels and almost all of them use wireless technology in some form, such as Bluetooth, Infrared, Wibree, Zigbee, 802.11, IrDA, or ultrasound. New operating systems are supporting the Adhoc networks on preliminary level. Future markets will be filled with these devices with fully functioning capabilities of these networks. Application of these wireless technologies are unlimited including the possible use in a disaster area where all communication system is destroyed, defense and military tactical applications, environmental monitoring, monitoring of remote areas, monitoring of geological and geographical area to predict the earthquake and level of pollution. The use of these devices are also available in daily use of mankind in m-commerce, advertisement of products, social networking, e-learning, business meetings and conferences. Even some preliminary level applications are still available like when you enter in shopping mall by detecting the sensor of your cell phones all products and offers will be transferred to your phone, even when two persons shake hands their business cards are transferred to each other.

A Mobile Adhoc NETwork (IEEE 802.11 and its variant) environment is characterized by energy-limited mobile nodes, bandwidth-constrained, variable-capacity wireless links and dynamic topology, leading to frequent and unpredictable connectivity changes. These networks are infrastructure less, self-organizing wireless networks. Each node can be workstations and has routing capabilities (Broustis *et al*., 2006) to be able to forward packets on behalf of other nodes. Nodes are typically composed of homogeneous nodes that communicate over wireless links without any central control.

Wireless sensor networks (IEEE 802.15 and its variant) are traditionally different than the Adhoc network in terms of application and routing because sensor networks are data centric networks, specially designed for specific application. Nodes are semi-mobiles or immobile. There is no need of mobile nodes but there are some situation if some area is not covered during the deployment then these nodes can be rearrange to cover the area. But speed is very less in comparison to Adhoc nodes. Data rate is lower and

Corresponding Author: Mukesh Chand, Graphic Era University, Dehradun, India

varies from 1-100 kbs. And transmission range is also varies to too few meters. Address auto configuration is not a big issue because it is data centric networks but in some situation we need unique identification based transmission (Biao *et al*., 2009; Dongkyun *et al*., 2007). An ideal sensor network must have following features like attribute based addressing, location aware based routing, immediate response in the critical situations like drastic change in monitoring data and on demand query handling.

Mesh networks are extended form of Adhoc network to utilize the full capacity of network. These networks maintain all possible routes to each neighbour with the help of directional antennas to transmit and receive the data simultaneously. These networks are very good for multicasting based applications in which we have multiple sender and multiple receivers groups. Routing solutions of sensor and Adhoc networks are not applicable in mesh network. It has special routing protocols for the network like ODMR (On demand multicast routing protocol for mesh network), DCMR (Dynamic core based Multicast routing protocol, (NSMR) Neighbour Supporting Adhoc Multicast Routing protocol and CAMP (Core Assisted Mesh Protocol)) (Saeed *et al*., 2012). These networks are important due to their versatile and robust nature.

In this study we will discuss about the issues and challenges in self auto configurable networks, the related work regarding the auto address configuration for self auto configurable networks (Awerbuch *et al*., 1991; Jaehwoon *et al*., 2009), algorithms for conflict free auto address assignment for different situations, the simulation setup for various scenario in self configurable networks, the results and outcomes and the conclusion of this study.

Issues and challenges: Wireless Adhoc Network serves as a temporary wireless network in which node changes its IP address with the help of an intelligent auto-configuration protocol. The main role of the IP address auto-configuration protocol is to manage the address space and also the protocol must be able to allocate a unique network address to un-configured node (Tamilarasi *et al*., 2007; Ghosh and Datta, 2009).

In the Internet, a network client is typically configured to use a server as its partner for network transactions. These servers can be found automatically or by static configuration. In ad hoc networks, however, the network structure cannot be defined by collecting IP addresses into subnets (Hansson *et al*., 2001). There may not be servers, but the demand for basic services still exists. Address allocation, name resolution, authentication and the service location itself are just examples of the very basic services (Dana *et al*., 2008; Khazaal *et al*., 2009) which are needed but their location in the network is unknown and possibly even changing over time. Due to the infrastructure-less nature of these networks and node mobility (Rahman and Aravind, 2012; Jian and Li, 2009), a different addressing approach may be required. In addition, it is still not clear who will be responsible for managing various network services. In this situation address auto configuration will play an important role.

It seems very likely that the most common applications of adhoc networks require some internet connection. However, the issue of defining the interface between the two very different networks is not straightforward. If a node in the network has an internet connection, it could offer internet connectivity to the other nodes. This node could define itself as a default router and the whole network could be considered to be "single-hop" from the Internet perspective although the connections are physically over several hops (Asl *et al*., 2009). In internet based application address auto configuration is very important issue.

In Adhoc network where there is no infrastructure. Individual node has the capability to form a new network. So in this case various small networks may be formed which are not in range of each other. But due to the mobility features merging of two independent networks may be common. And in the same way splinting of one big network to many more small networks are also possible. In these situation conflict free address auto configuration protocol is necessary.

Wireless sensor nodes should be self organized and coupled with the fact that operation of the network is unattended. The network organization and configuration should be performed automatically and more often due to nodes failure. In most application scenarios, sensor nodes are stationary. Nodes in other traditional wireless networks are free to move, which results in unpredictable and frequent topological changes.

In traditional sensor networks, data is requested from a specific node. Sensor Networks are data centric i.e., data is requested based on certain attributes, i.e., attribute-based addressing. But there are some situation in which we have to access the data according to the location based service. In this case we need address auto configuration to cope with the changes in topology or movement of the node.

LITERATURE REVIEW

There are various solutions are proposed by the researcher for conflict free address auto configuration for self configuration networks are available. Wang and Zhong (2013) proposed cluster tree architecture, for the hierarchical IPv6 address configuration algorithm where the IPv6 configuration for cluster members in different clusters can be performed simultaneously. Author analyzed the performance parameters of the proposed scheme. Mohsin and Prakash (2002) proposed an extended solution of the previous research for the problem of merging and partitioning of mobile Adhoc

networks. He used the consideration of binary split of the network.

Xiaonan and Shan (2013) proposed a scheme on achieving all-IP communication between wireless sensor networks and IPv6 networks based on sensor nodes' location information. Author proposed the sensor node's IPv6 address structure based on location information, the IPv6-address configuration algorithm based on the proposed IPv6 address structure, the mobility handoff algorithm and the routing algorithm in the link layer. Bernardos *et al*. (2010) used the PACMAN algorithm, an efficient distributed address auto-configuration mechanism originally designed for Adhoc networks, he extended the work for wireless mesh networks with an experimental study-using mobile nodes and assuming worst-case scenarios. And he analyzed its behavior as an IP address auto-configuration mechanism for community of wireless mesh networks.

Galand and Marce (2004) has given a reference architecture for a self-configuration router is given, allowing the community to have a common understanding on the expected functionalities of self configurable networks router. An evaluation of the existing proposals to address part of all the issues raised by self-configuration is also presented. Ng *et al*. (2003) proposed a prototyping P2P system, BestPeer is presented. The BestPeer is unique in several ways. Firstly, it combines the power of mobile agents into P2P systems to perform operations at peers' sites. Secondly, it is self-configurable. A node can dynamically select the set of peers with which it can communicate directly based on some optimization criterion. Thirdly, the BestPeer provides a Location Independent Global named Lookup server (LIGLO) to identify peers with dynamic (or unpredictable) IP addresses. The BestPeer is evaluated on a PC cluster consisting of 32 Pentium II running Java-based storage managers. The experimental results show that the BestPeer provides excellent performance compared with traditional non-configurable models. Further experimental study reveals its superiority over Gnutella's protocol.

In this study we proposed an algorithm for merging and partitioning of self configurable networks. Which is effective, fast responsive and light weighted in terms of battery backup.

METHODOLOGY

Proposed CMJ algorithm: When two independent networks are merging then this leads the high degree of probability that some nodes are using common addresses; it will create the problem of address conflict. It should be resolved before merging. Proposed algorithm is a solution to resolve the problem of address confliction in self configurable networks.

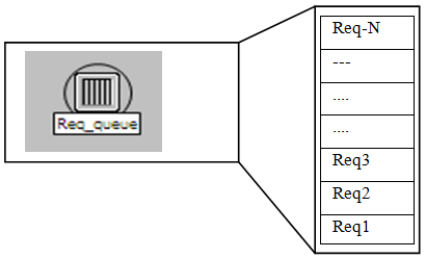

Fig. 1: Request queue

Table 1: Parameters table

	Merging and partition parameter		
Description of selection	M	P	S
No instance occur	0	0	0
Partition activated	0	1	1
Merging activated	1	0	1
Undefined (waiting for stabilization of the network)	1	1	-

Initially the algorithm starts with collecting requests from the participating nodes, request queue as shown in the Fig. 1.

During the initialization phase first we will check that whether it is a case of partition or merging of the network. The status of the node is set according to the formula as in Eq. (1). The possibilities of selection are shown in the Table 1. The selection of merging and partition algorithm is based on the Eq. (1). Then selection process will start:

$$S = M^{|} * P + P^{|} * M \quad (1)$$

where,
S = Status of the node
P = Partition
M = Merging

Selection process:

```
If (Incoming signal)
      Then
Call Process1;
Else
                  If (Weak_signal)
            Then
Call process2;
```

Process 1 (merging of self configurable networks): After the execution of the selection process if it is a case of merging then algorithm for process 1 will execute. During the merging of the networks if numbers of networks are more than two, then in this case first two networks will merge to form a single network and then repeat this process till existing networks are merged to form a single network. The situation of self configuring networks leads to different scenarios to work the algorithm and further subdivided into three subcategories which are as follows:

Process 1:
Set Request_counter = 0;
1. If (incoming_signal) then
Current_status = Call Authentication_algo;
Set Status = Current_Status;
If (status found trusted)
Request_Counter = Request_Counter + N; (N> = 0)
2. If (Request_Counter = = 0) then
Set M = 0;
Else
Set M = 1;
3. If (M = = 1) then
Call Merging_Procedure (); //Case1|| Case2
Set Request_Counter = 0;
Else
Exit ();

Case 1: Address confliction in merging of individual SCN:

When two nodes except the Network head node, are conflicting then at the time of merging two Network head will share the routing table of their internal domain, cluster head of both networks will create a temporary routing table before merging the network.

Case 2: Address confliction in merging a single node to SCN.

If there is a conflict between a Network Head node and a normal node then algorithm A2 should be used to remove the conflict.

Address conflict in merging of individual SCN:
1. $CH\_SCN1_{HELLO} \rightarrow CH\_SCN2$
2. $CH\_SCN2_{REP+ACK} \rightarrow CH\_SCN1$
3. $CH\_SCN1_{IP[i]} \leftarrow_{EXCHANGE} \rightarrow CH\_SCN2_{IP[i]}$ //Exchange of the Address Tables
4. Make a M_ IP_ table in the buffer for each SCN.

Set
Conflict = false;
Array C1 = null;
//Array of conflicted IP address in SCN_1
Array C2 = null;
SCN_ 1. node [i]. NH_IP_hostnumber = SCN_1. node [i]. IP_hostnumber;
SCN_2. node [i]. NH_IP_hostnumber = SCN_1. node [i]. IP_hostnumber;
5. If (IP conflicts = 1) then go to step7.
If (SCN_1. node [i]. IP_hostnumber = = SCN_2. node [j]. IP_hostnumber)
Then
Set
Conflict = true;
Add M (C1, SCN_1. node [i]. IP_hostnumber);
Add N (C2, SCN_2. node [j]. IP_hostnumber);
Else
GOTO step_7;
6. If two nodes have conflict then the steps are shown below:

Leave an entry blank on the MS IP Table.
- If (conflict)

Then
If (i<s1) //s1 is the Size of SCN1
Set
SCN_1. C1 [i]. IP = null;
If (j<s2) Then //s2 is the Size of SCN2
Set
SCN_2. C2 [j]. IP = null;
Update M_IP_table; //update M_IP_table from entries in array C1 and C2 EX.
S1 = 7; S2- = 7.
- If (S1> = S2)

Then
Set
SCN_1. node [i]. IP_hostnumber = previous IP_ hostnumber
// Enter the previous IP of SCN_1's M_IP_Table.
SCN_2. node [i]. IP_hostnumber = Random number
Else
Set SCN_1. node [i]. IP_hostnumber = Random number
SCN_2. node [i]. IP_hostnumber = previous IP_ hostnumber
7. If (S1> = S2)
Then
Set
SCN_merged. node [i]. NH_IP_hostnumber = SCN_1. node [i]. NH_IP_hostnumber;
8. Assign the M_IP_Table to the network head of SCN_1 and drop the IP table from the network head of SCN_2 is M.
$Merged\_SCN_G = SCN\_1_G + SCN\_2_M$; // if S1> = S2
$Merged\_SCN_M = SCN\_1_G + SCN\_2_M$; //if S1<S2
9. The node M broadcasts the updated information to other nodes in the network.

Address conflict in merging a single node to SCN:
1. $Node\ [i]_{HELLO} \rightarrow CH\_SCN$
2. $CH\_SCN_{REP+ACK} \rightarrow Node\ [i]$
3. $IP\_Node\ [i] \rightarrow CH\_SCN$
4. If (IP_Node [i] = = IP_SCN [n])
   Then
      Set IP_Node [i] = IP_SCN [n+1]
   IP_SCN [n] = IP_SCN [n+1]

Process 2 (partitioning of self configurable networks): Process 2 is for partitioning of network, when a large network is going to divide in two or more networks. Partitioning process is simple if partition is graceless in this case network head will update the table periodically and empty values are marked and de-allocate it for further use.

Process 2:
1. Exit_Counter = 0;
2. If (Weak_Signal)

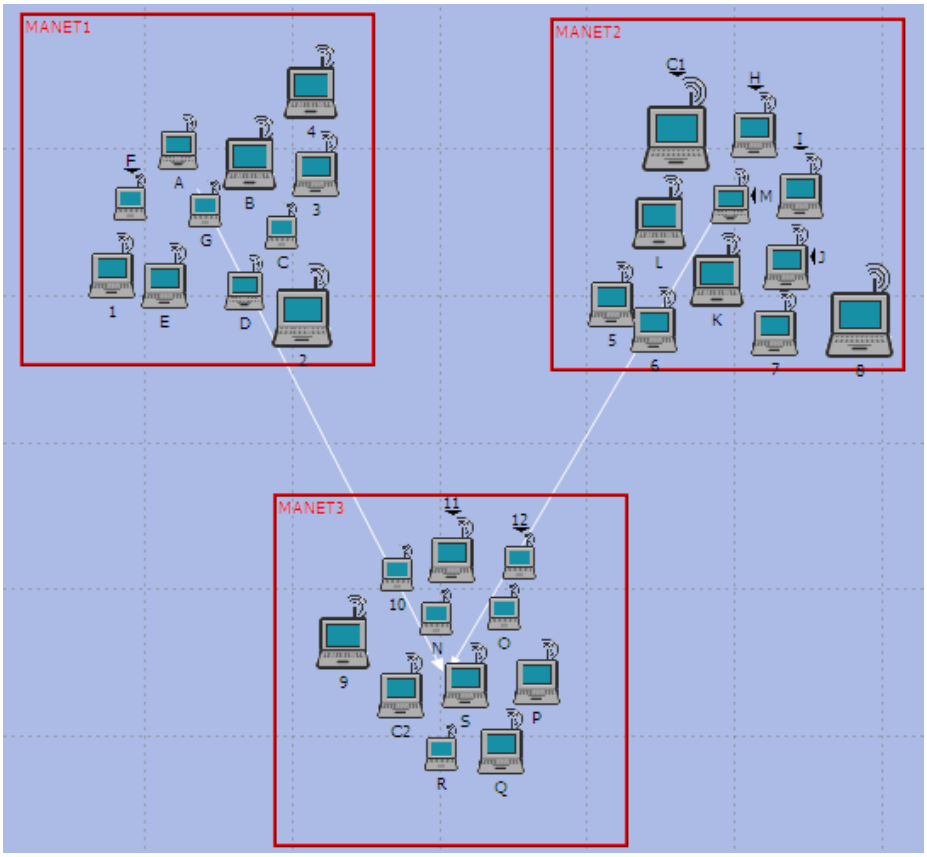

Fig. 2: Simulation scenario

Table 2: Simulation parameters at a glance

Parameter	Value
Transmission power	0.005
Packet reception power	-95 dBm
Simulation time	3600 sec
Number of nodes	33 mobile nodes
Pause time	0 sec
Environment size	(10*10) km
Traffic type	CBR
Routing protocol	AODV
Packet size	Default
Speed	(0-20) m/sec
Trajectory	Random way point trajectory

Set Exit_Counter = Exit_Counter + N;
3. If (Exit_Counter = = 0) then
Set P = 0;
Else
Set P = 1;
4. If (P = = 1)
Call Graceless_Partition method;
Set Exit_Counter = 0;
Else
Exit;

Simulation setup: Proposed CMJ algorithm is implemented in Opnet Modeler, which is industry leading simulation software (Opnet Modeler Wireless Access Suite for Network Simulation, year). A Simulation scenario is designed as shown in Fig. 2. In this scenario three different self configurable networks are given after some time they starts moving and there transmission ranges of individual networks become closer to each other and then merging process starts. All nodes have unique IP addresses in its corresponding networks. Simulation area is considered of 10*10 km^2 for the simulation. We have used eleven mobile nodes in each individual networks. Individual nodes are moving with random mobility. Due to merging process duplicity of addresses will check according to the CMJ algorithm. Table 2 shows the simulation parameters at a glance, these parameters and their value is taken due to the most of the researchers are taking these values for better comparison and understanding.

RESULT ANALYSIS AND DISCUSSION

Performance of the CMJ algorithm is investigated and discussed below.

Total route errors sent: When SCN1 and SCN2 started moving and finally merge to SCN3 then IP conflicts occurred. Packets are falsely routed to node C, C1 and node C2. The number of total route errors sent increases because of these conflicts. With the help of proposed algorithm the above problem does not occur. In the result analysis for the total route errors sent of the

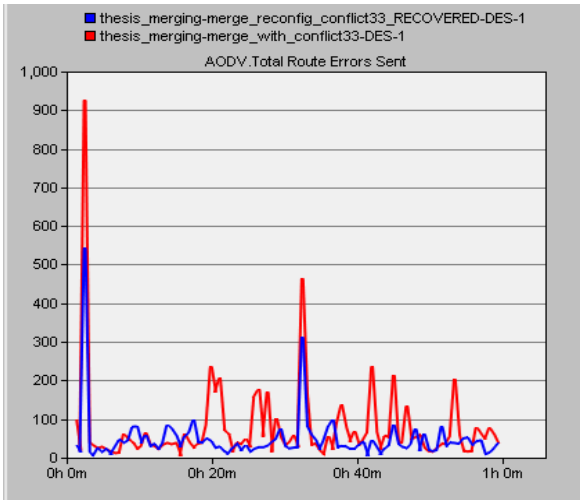

Fig. 3: Total route errors sent

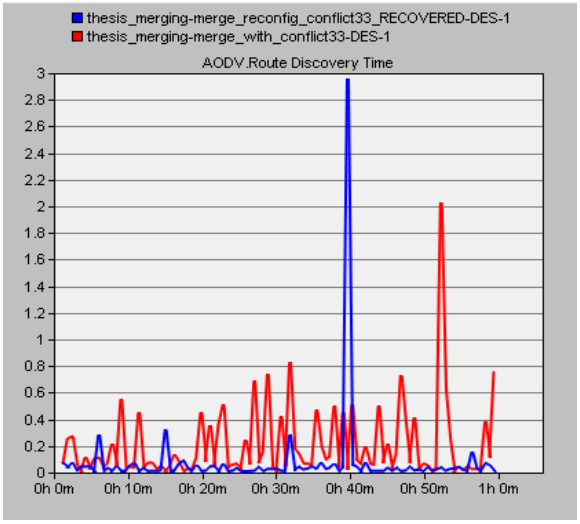

Fig. 4: Route discovery time (sec)

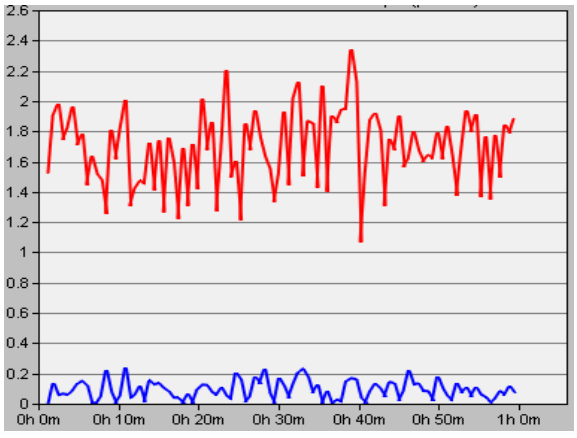

Fig. 5: Route retries attempts

scenario, the Value of total route errors sent on IP-conflict is near about 1.4 and the value of total route errors sent after reconfiguration it is 0.4 on the start of the simulation but after some time where the value of total route errors sent for the IP-conflict is 1.2 and after reconfiguration according to the proposed algorithm, it is 0.2 as shown in Fig. 3. With the help of proposed algorithm by removing duplicate IPs and assigning unique IPs total route errors sent decreases from 93 to 13%.

Though route errors has no comparison table but it shows that due to decrease in route error sent values there is tremendous improvement in discovery time and delay.

Table 3: Performance comparison with previous research for merging of networks

	Route discovery time/delay (%)	Route request retries/ convergence time (%)
Kim *et al*. (2005)	20	2.7
Zhou *et al*. (2003)	31	3
Proposed algorithm	15	2
Wang and Zhong (2013)	26	2.2
Carlos *et al*. (2010)	22	2.6

Route discovery time: Those routed packets go to the IP address 192. 0. 1. 27 falsely routed to all the nodes having this IP address. Bulk of acknowledgement received from these conflicted nodes. In our case node C, Node C1 and node C2 are the nodes having duplicate address. So route discovery time increases (90%). In the result analysis for the route discovery time of the scenario, Value of route discovery time on IP-conflict is near about 0.3 sec and value of route discovery time according to CMJ algorithm is 0.05 sec (as shown in Fig. 4) on the start of the simulation but after some time value of route discovery time for the IP-conflict is 0.8 sec and after reconfiguration it is 0.01 sec. Taking more investigation samples and on analyzing them we concluded that route discovery time according to CMJ algorithm is reduced to 15% and is better in the case of IP-conflict. Performance of CMJ algorithm is observed to be efficient in comparison to previously available conventional models.

Route retries attempts: When the mobile nodes starts moving and go out of range before merging than to detect the route to the neighbour's total route retries attempts increases to 61%. The proposed algorithm reduces the total route retries attempts to 2% as from the Fig. 5. The value is observed to be good and improved and given in Table 3.

Delay: When data packets arrive in a smooth and timely manner the user sees a continuous flow of data but if data packets arrive with large and variable delays between packets the performance of the network is degraded. From the Fig. 6, Value of delay is near about 0.05 sec when the network is not partitioned and value of is 1.3 sec when the network is partitioned on start of the simulation but after applying CMJ algorithm the value of delay is reduced to 31% on average.

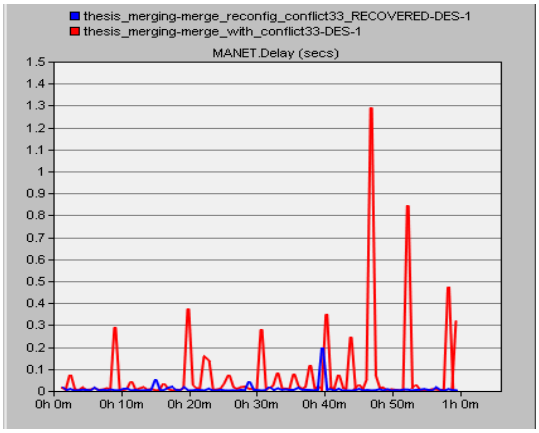

Fig. 6: Delay

Table 4: Performance comparison with previous research for partition of networks

	Delay (Avg.) (%)	Throughput (%)
Johanson (1991)	40	25
Aparna and Reza (2011)	38.2	27.5
Proposed algorithm	31	96.4
Bai *et al*. (2003)	33	70

Avg.: Average

Throughput: In the simulation we have found that routing traffic received by each node participating in the Adhoc network increases. The reason for this is the numbers of requests are increases when a network is partitioned because all the nodes keep sending requests until they reach at a threshold value. Nodes in this Adhoc network are not aware of the partition because the nodes departure abruptly. This problem is solved with the help of proposed algorithm in which each node has to intimate about their leaving which increases the degree of reusability of IP addresses assigned to the nodes and the routing traffic sent by each node participating in the Adhoc network also increases. The reason for this is the numbers of requests are increases when a network is partitioned because all the nodes keep sending requests to find its neighbour until they reach at a threshold value. Nodes in this Adhoc network are not aware of the partition because the nodes departure abruptly.

Through put of the network is calculated on the basis of the formula:

Throughput = (Total traffic received/Total traffic sent) *100

And in comparison with the previous conventional algorithms results are improved and better as shown Table 4.

CONCLUSION

In this study a new methodology for authentication based auto-configuration of IP addresses in mobile Adhoc networks is proposed. The proposed algorithm is categorized with the authentication process and three possibilities where conflict may occur when different independent network merge to form a single network. The performance is evaluated when duplicate addresses are present in the case of merging with duplicate address by applying the proposed algorithm. From the result analysis it is observed that there is significant performance improvement in the network by applying the proposed algorithm for secure merging in comparison to the previously available models. Further work is in progress to test the algorithm in the case of high degree of mobility and scalability of the network nodes.

REFERENCES

Aparna, M. and M. Reza, 2011. Throughput analysis by varying the network size in mobile ad hoc network. Proceeding of International Conference on Computational Intelligence and Communication Networks (CICN), pp: 737-739.

Asl, E.K., M. Damanafshan, M. Abbaspour and M. Noorhosseini, 2009. EMP-DSR: An enhanced multipath dynamic source routing algorithm for mobile Adhoc networks based on ant colony optimization. Proceeding of 3rd Asia International Conference on Modelling and Simulation, (AMS '09), pp: 692-697.

Awerbuch, B., A. Bar-Noy and M. Gopal, 1991. Approximate distributed bellman-ford algorithms [computer network routing]. Proceeding of 10th IEEE Annual Joint Conference of the IEEE Computer and Communications Societies, Networking in the 90s, (INFOCOM '91), pp: 1206-1213.

Bai, F., N. Sadagopan and A. Helmy, 2003. IMPORTANT: A framework to systematically analyze the Impact of Mobility on Performance of Routing Protocols for Adhoc Networks. Proceeding of 22nd Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies (INFOCOM, 2003), 2: 825-835.

Bernardos, C.J., M. Calderon, I. Soto, A.B. Solana and K. Weniger, 2010. Building an IP-based community wireless mesh network: Assessment of PACMAN as an IP addresses autoconfiguration protocol. Comput. Netw., 54(2): 291-303.

Biao, Z., C. Zhen and M. Gerla, 2009. Cluster-based inter-domain routing (CIDR) protocol for MANETs. Proceeing of 6th International Conference on Wireless on-Demand Network Systems and Services, (WONS), pp: 19-26.

Broustis, I., G. Jakllari, T. Repantis and M. Molle, 2006. A comprehensive comparison of routing protocols for large-scale wireless MANETs. Proceeding of 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (SECON '06), 3: 951-956.

Carlos, J.B, M. Calderon, I. Soto, A.B. Solana and K. Weniger, 2010. Building an IP-based community wireless mesh network: Assessment of PACMAN as an IP addresses autoconfiguration protocol. Comput. Netw., 54(2): 291-303.

Dana, A., A.M. Yadegari, A. Salahi, S. Faramehr and H. Khosravi, 2008. Notice of violation of IEEE publication principles a new scheme for the on-demand group mobility clustering in mobile Ad hoc networks. Proceeding of 10th International Conference on Advanced Communication Technology, (ICACT), pp: 1370-1375.

Dongkyun, K., H.J. Jeong, S. Oh and J.C. Cano, 2007. Improving the accuracy of passive duplicate address detection algorithms over MANET on-demand routing protocols. Proceeding of 8th International Symposium on Autonomous Decentralized Systems (ISADS '07), pp: 534-542.

Galand, D. and O. Marce, 2004. A functional architecture for self-aware routers. Proceedings of the ACM Symposium on Applied Computing, pp: 352-356.

Ghosh, U. and R. Datta, 2009. An authenticated dynamic IP configuration scheme for mobile ad hoc networks. Proceeding of IFIP International Conference on Wireless and Optical Communications Networks (WOCN '09), pp: 1-6.

Hansson, A., J. Nilsson, M. Skold and U. Sterner, 2001. Scenario based comparison of cellular and ad-hoc tactical radio networks. Proceedings of IEEE Communications for Network-centric Operations: Creating the Information Force Military Communications Conference (MILCOM, 2001), 1: 545-549.

Jaehwoon, L., A. Sanghyun, Y. Hyun, Y.S. Kim and J.S. Jin, 2009. Address auto configuration and route determination mechanisms for the MANET architecture overcoming the multi-link subnet model. Proceeding of International Conference on Information Networking, (ICOIN), pp: 1-5.

Jian, L. and F.M. Li, 2009. An improvement of the AODV protocol based on reliable delivery in mobile Ad hoc networks. Proceedings of 5th International Conference on Information Assurance and Security (IAS '09), pp: 507-510.

Johanson, P., 1991. Scenario-based performance analysis of routing protocols for mobile ad-hoc networks. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp: 195-206.

Khazaal, H.F., C. Papageorgiou, I. Politis, T. Dagiuklas and N.N. Khamiss, 2009. Video over MANET: The impact of obstacles, node mobility speed and background traffic on the perceived video quality. Proceeding of 3rd International Conference on New Technologies, Mobility and Security (NTMS), pp: 1-5.

Kim, M.J., M. Kumar and B.A. Shirazi, 2005. A lightweight scheme for auto-configuration in mobile ad hoc networks. Proceeding of IEEE International Parallel and Distributed Processing Symposium, pp: 4.

Mohsin, M. and R. Prakash, 2002. IP address assignment in a mobile ad hoc network. Proceedings of IEEE Military Communications Conference (MILCOM), 2: 856-861.

Ng, W.S., B.C. Ooi, K.L. Tan, X.Y. Wang, B. Ling and A.Y. Zhou, 2003. Novel Peer-to-peer system based on self-configuration. Ruan Jian Xue Bao J. Software, 14(2): 237-246.

Opnet Modeler Wireless Access Suite for Network Simulation, year. Retrieved form: http:// www.riverbed.com/products-solutions/ products/ network-planning-simulation/Network Simulation. html.

Rahman, M.A. and A. Aravind, 2012. Connectivity analysis of mobile Ad hoc networks using destination guided mobility models. Proceeding of 3rd FTRA International Conference on Mobile, Ubiquitous and Intelligent Computing (MUSIC), pp: 5- 12.

Saeed, N.H., M.F. Abbod and H.S. Al-Raweshidy, 2012. Mobile ad hoc networks routing protocols taxonomy. Proceeding of Future Communication Networks Conference, pp: 123-128.

Tamilarasi, M., V.R. Shyam Sunder, U.M. Haputhanthri, C. Somathilaka, N.R. Babu, S. Chandramathi and T.G. Palanivelu, 2007. Scalability improved DSR protocol for MANET. Proceeding of International Conference on Computational Intelligence and Multimedia Applications, 4: 283-287.

Wang, X. and S. Zhong, 2013. A hierarchical scheme on achieving all-IP communication between WSN and IPv6 networks. AEU-Int. J. Electron. Commun., 67(5): 414-425.

Xiaonan, W. and Z. Shan, 2013. All-IP communication between wireless sensor networks and IPv6 networks based on location information. Comput. Stand. Inter., 35(1): 65-77.

Zhou, H., L.M. Ni and M.W. Mutka, 2003. Prophet Address allocation for large scale MANETs. Proceeding of 22nd Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies (INFOCOM 2003), 2: 1304-1311.