Journal of Computer Science 10 (7): 1120-1129, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1120.1129 Published Online 10 (7) 2014 (http://www.thescipub.com/jcs.toc)

TRUSTWORTHY ENABLED RELIABLE COMMUNICATION ARCHITECTURE IN MOBILE AD HOC NETWORK

[1]Saravanan Dhavamani, [2]Chandarasekaran Ramasamy and [3]M.G. Sharavana Kumar

[1]Department of Computer Science and Engineering,
Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India
[2]Department of CSE, Annamalai University, Chidambaram, Tamil Nadu, India
[3]Research Scholar, Anna University, BIT Campus, Tiruchirappalli, Tamil Nadu, India

Received 2013-12-26; Revised 2014-01-21; Accepted 2014-02-12

ABSTRACT

Ad hoc networks are widely used in military and other scientific area. There are various kind of routing protocols are available to establish the route, with the proper analyzation one can choose the routing protocol to form their own network with respect to number of nodes and security considerations. The mobility of nodes makes the environment infrastructure less. It also has a certain number of characteristics which makes the security difficult. A trust recommendation mechanism has designed to keep track of node's behavior to establish the trustworthiness of the network. Meanwhile with this trustworthiness a node can make objective judgment among another node's trustworthiness to maintain whole system at a certain security level. The motivation of the work is to understanding the behavior or routing protocol and the trustworthiness.

Keywords: Ad hoc, Mobility Trustworthiness, Routing

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of multi-hop wireless mobile nodes; wireless network can be classified into two types, Infrastructure and Infrastructure less. Mobile nodes can move when communication occurs. The base stations are fixed the node gets mobile and it goes out the base station rage and it get connected to the another base station (Saravanan *et al*., 2011). Communication of nodes among others without centralized control. Due to mobility of nodes the network may be highly error prone and hence it goes down frequently. So routing in MANET is a complicated task due to dynamic environment.

This study exhibits the overview of the routing protocols by representing the characteristics, pros and cons and comparative analysis. The aim is to provide performance analysis of several routing protocols and to enable the trustworthiness.

Primary goals of routing protocols in ad hoc wireless network:

- Minimum route acquisition delay
- Quick route reconfiguration
- Loop-free routing
- Distributed routing approach
- Minimum control overhead
- Scalability
- Provisioning of QoS
- Support for time-sensitive traffic
- Security and privacy

1.1. Random Placement

Random node placement (Bobade and Mhala, 2012) means, in simulation environment the nodes were placed randomly within the specified terrain. The terrain size can also be varying. That is, the number of nodes is placed randomly within the physical terrain.

Corresponding Author: Saravanan Dhavamani, Department of Computer Science and Engineering,
Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India

1.2. Grid Placement

Grid node placement (Setty *et al*., 2010) starts from some dimensions of numerical values (0,0) or (1,1) or (10,10) likewise. Here the nodes are placed in grid format where each node has some grid unit which has also numerical values, it denotes some distance between each nodes in meters. The number of nodes can be in square of the integers like 4,9.

1.3. Uniform Placement

The uniform node placement (Setty *et al*., 2010) is based upon the number of node placement in the terrain. According to the number of nodes the terrain size was divided into a single cell and each cell has a single node while the distance between the nodes is somewhat random but it has uniform density.

1.4. Related Work

Since MANET has the attribute of dynamic node movements and dynamic network topology changing, it is difficult to maintain the route. Packet delivery among the nodes that are in the network is also difficult; hence it requires flexible routing mechanism. In order to overcome these difficulties, the protocols uses several parameters such as energy consumption, error rates. Developing routing protocol is a broad research area in MANET; basically routing protocols are classified into three categories proactive, reactive and hybrid. More over there are other routing protocols also available such as Flow oriented and hierarchical routing protocols (**Table 1**). These protocols give the clear way to establish the route in terms of scalability, mobility and energy consumption.

1.5. Routing Protocols

Routing mechanism involves data transfer from source to destination node. The mechanism follows two steps route establishment and transfers the packets. In order to obtain an efficient routing there are several metrics to be considered. There are two types of routing are available in MANET static and dynamic, if any node added in the static routing, the administrator acknowledgment is needed. In Dynamic routing administration acknowledgement does not need to add or remove the node, whenever the node addition takes place it simply adds the node.

1.6. Reactive Routing Protocols

In reactive routing protocols there are three basics protocols are there, Ad hoc On-Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing (DSR) and Temporal Ordered Routing protocol (TORA). On-demand routing protocol will establish the route when there is a necessity of sending packets over a network. If route is unknown or breakage, the source node is take care of the packets to reach the destination by floods the route request packets to the networks for path finding, it leads to network clogging. Reactive routing protocols are best suited for limited resource environment. Comparing with table driven routing protocols, On-Demand contains low overhead.

1.7. Proactive Routing Protocols

A proactive routing protocol preserves the route to all destination of all time it does not care about whether the routes are needed or not. Each and every node maintains correct route, by sending control messages so that the route will always open to communicate and hence bandwidth wastage occurs. Each node in the protocol maintains routing information so it is not suitable for larger networks. There is a possible of slow reaction when any link breakage or failures occurs. The major advantage of the routing it quickly obtain routing information and establish the routes.

1.8. Ad hoc On-Demand Distance Vector Routing Protocol (AODV)

Ad hoc on demand distance vector routing algorithm facilitates multi hop, dynamic routing, added to that AODV avoids bellman ford counting infinity problem, more over it was designed in such a way that mobile nodes will respond even when link breakages among nodes. To avoid loop free condition AODV in corporate destination sequence number for every route (Uma *et al*., 2013). In AODV there are some identification such as RREQ, RREP and REER to indicate request, reply and error respectively. RREQ is used to obtain a route when a fresh destination is required, in case a node needs to find the destination that node have to broadcast the RREQ message to all nodes, if the node found the destination, Unicasting enables the newly obtained route, by default the RREP messages sends back to the destination for all nodes which receives the RREQ message in order to find the destination. If destination found RREP message able to send the source node, to find the link breakage, the activated nodes and the respective links has been continuously monitored. If any link break found the REER message is to be sent in order to find the link loss. The REER message is used to identify the link breakage and to find which nodes are unreachable.

1.9. Dynamic Source Routing (DSR)

Dynamic source routing Protocol is a reactive routing protocol. It eliminates table update messages required in table driven approach, hence it enables simplicity and efficiency. The uniqueness of DSR is self configuring and self organizing routing protocol. There are two mechanisms that DSR incorporate that is route discovery and route maintenance. DSR updates the nodes regularly in order to find a new route. If new nodes found the node gets redirected to the newly obtain route. The node itself find the route to reach the destination since the information about the route was merge in the packet to get reach the specified destination from the sender. DSR has the mechanism to enable the efficiency, which is route discovery and route maintenance.

Route discovery has two messages such as Route Request (RREQ) and Route Reply (RREP). The role of these two mechanisms is when nodes want to communicate with the destination node, it will broadcast the RREQ packet in the network, once the RREQ reaches the destination and destination node will replay the packet to the route node (Uma *et al*., 2013).

1.10. Temporally Ordered Routing Algorithm (TORA)

TORA is designed to minimize reaction to topological changes. TORA is a distributed routing algorithm for mobile, multi hop wireless network. TORA uses link reversal algorithm which enable on-demand routing protocol (Uma *et al*., 2013). TORA has three functionality namely creating routes, mentioning routes and erasing route. When there is need to communicate their only exist the route. Directed acyclic graph takes care of route establishment, which uses query update mechanism. To withdraw the route establishment TORA uses Clear (CLR) packet throughout the network. Route establishment sends Query (QRY) packets to route the required flag. QRY packet contains the destination id of the node that to be communicate. To reply the query is known as Update (UPD) packet.

1.11. Optimized Link State Routing (OLSR)

This protocol is popularly used for large and dense network, The concept used in the protocol is that Multipoint Relays (MPRs). During flooding process the selected nodes of MPRs forward broadcast message, this technique reduces the message transparency (Uma *et al*., 2013). The efficient link state routing for mobile ad hoc network. Minimizing the number of control messages flooded in the network lead to accomplish the second optimization. MPR node may chose communicates only with links between itself and its MPR selectors. Thus OSLR provides optimal routes.

2. MATERIALS AND METHODS

2.1. Node Comparisons

2.1.1. Trust Worthiness

2.1.2. Behaviour-Based Trust Formation

Figure 1 depicts the collective performance of the node by past tasks and from that decides the new role of the node in the upcoming tasks. The basic idea is to deliver the behaviour based trust formation according to the node behaviour. A node has different behaviours in the network such as communicating, routing data processing. A node may involved in more than one tasks, this situation may lead to misbehaviour of node, so continuous evolution of different tasks of the node can be put together to predict the node's future behaviour (Karthik and Dhulipala, 2011).

2.2. Process

For each node after the task completion the behaviour of node has evaluated, the result is then combined with the old trust degree to form a new one. This newly generated result is then applied to next task (Velloso *et al*., 2010).

2.3. Authentication

Obviously authentication is concerned with cryptography. Symmetric cryptography, which demands secure key exchange. Key management is important thing for that secure formation needed, key pre-distribution before deployment, key creation and distribution after deployment is more important. μTESLA is for broadcasting, which is used to delayed disclosure of symmetric keys to achieved an asymmetry needed by valid authentication and to authenticate the report in an interleaved, hop-by-hop fashion in order to detect data injection or modification.

Actual output observation, difference calculation is comes under general behaviour evaluation. Although behaviour evaluation is task-specific, energy efficient and fault tolerance are basic requirements.

2.4. Behaviour Evaluation in Routing

Node behaviour can easily identify by simply packet drop or not, if packet drop is there it is consider to be inefficient way of communication otherwise it is good when no packet drops occurs. In the same way Behaviour of routing can be evaluated by two ways, adding active feedback mechanism to protocol or by observing node's behaviour.

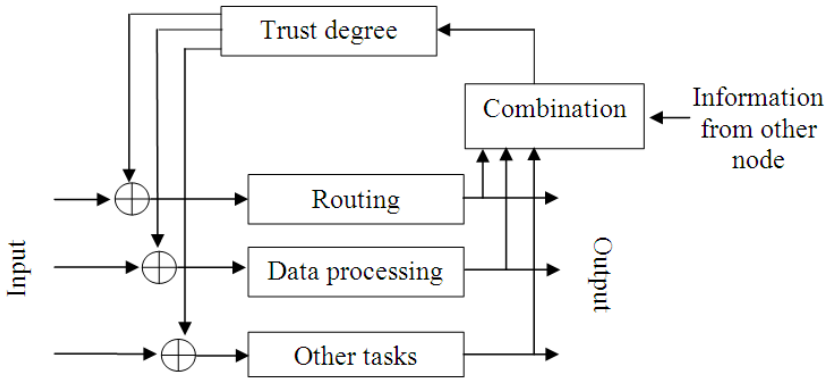


Fig. 1. Trust formation

Table 1. Pros and cons for routing protocol

Type of routing	Pros	Cons
Pro active	This type protocols maintains new lists of destinations and the respective routes by periodically distributing routing tables throughout the network	1. Respective amount of data for maintenance 2. Slow reaction on reformation and failures
Re active	This type of protocols finds a route on demand by flooding the network with Route Request packets.	1. For route finding it requires High latency time 2. Network clogging can be occur due to Excessive flooding
Hybrid	Proactive + Reactive	1. Depends on number of other nodes activated 2. Reaction to traffic demand depends on gradient of traffic volume
Flow oriented routing	Finds route on demand by One option is to unicast consecutively when forwarding data while promoting a new link	1. Discovery of new routes without prior knowledge takes a long time 2. Missing knowledge on routes
Hierarchical routing	The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attributation for respective levels.	1. Advantage depends on depth of nesting and addressing scheme. 2. Reaction to traffic demand depends on meshing parameters.

Even though the mechanism exists, there are some pretty much undesirable with some complex sort of problem, such as selective dropping, which may due to malicious attack. In a network a valid Acknowledgement (ACK) of packet does not receive within a defined period, it is assumed that has been lost, if packet loss rate exceeds with certain threshold, the network can be assumed the influence of misbehaving nodeThe trust formation works in the same formation by deduction of misbehaviour node can find by the neighbouring node. When a node sent a packet to neighbour node, the information can be obtain locally, then the node listen to neighbour's communication. If the node does not forward the same packet to the next hop it is considered as a misbehaving. The trustworthiness can be identify by passive listing and receiving.

2.5. Design of the Experiment and Simulation Setup

For this experiment the carefully designed base configuration for analyzing the routing protocols with respect to traffic and the node variation accordingly and also mobility at a time to stress the network is different. In addition the design of the condition such as network topology and type of routing are taken into account.

This experiment has carried out with the help of NS2, with the careful chosen of terrain dimension with the nodes densities such as 5,10,20,50,100,150, with respect to all the nodes the throughput and delay time has calculated. For all those different set of nodes the terrain size has differs listed in the **Table 2-4**, simulation time also differs according to the different nodes and terrain size. There are some set of metrics has carried out such as total simulation time, number of packets send, number of packets received, packet delivery ratio and finally through put This experiment used a static utilization of IPv4 networking protocol.

2.6. Parameter Analysis

There are various kinds of performance evaluation are there with respect to the parameters of the routing protocol. In this study there are three kinds of parameters are used to analyze the overall network performance, the parameters are delayed, network and throughput.

Table 2. Analysis of ADOV

	AODV				
Considerations					
Terrain size	1500×1500	1500×1500	1600×1500	1500×1500	2500×2500
Number of nodes	5.000000	26.000000	50.000000	100.000000	150.000000
Packet size	1040.000000	1040.000000	1040.000000	1040.000000	1040.000000
Total simulation time	100.000000	540.000000	810.000000	1300.000000	1830.000000
Number of Packets Send	8840.000000	84330.000000	136690.000000	347948.000000	627195.000000
Number of packets receive	7553.000000	78330.000000	116533.000000	202252.000000	288096.000000
Packet delivery ratio	0.854412	0.928851	0.852535	0.581271	0.45934
Through put	82940.000000	150857.000000	149622.000000	161801.000000	163726.000000

Table 3. Analysis of DSDV

	DSDV				
Considerations					
Terrain size	1500×1500	1500×1200	1600×1600	1500×1500	1800×1800
Number of nodes	16.000000	26.000000	50.000000	100.000000	100.000000
Packet size	1060.000000	332.000000	1060.000000	1040.000000	1040.000000
Total Simulation time	429.809000	549.971000	819.997000	1309.990000	1309.990000
Number of packets send	67085.000000	89299.000000	175586.000000	1051798.000000	1051798.000000
Number of packets receive	60483.000000	75281.000000	116125.000000	222958.000000	222958.000000
Packet delivery ratio	0.901588	0.843683	0.661357	0.211978	0.211978
Through put	149163.000000	45444.000000	150113.000000	177005.000000	177005.000000

Table 4. Analysis of DSR

	DSR				
Considerations					
terrain size	1000×1200	1300×1200	1000×1200	1000×1200	1500×1500
Number of nodes	5.000000	6.000000	7.000000	8.000000	26.000000
Packet size	1040.000000	1040.000000	1040.000000	40.000000	84.000000
Total simulation time	110.000000	79.269100	200.000000	100.000000	280.119000
Number of packet sent	12278.000000	11511.000000	15957.000000	15939.000000	57583.000000
Number of packets receive	7336.000000	6668.000000	9372.000000	9359.000000	36885.000000
Packet delivery ratio	0.597491	0.579272	0.587328	0.587176	0.640554
Through put	69358.000000	87483.000000	48734.000000	3743.000000	11060.000000

3. RESULTS

3.1. Throughput Analysis

3.1.1. Without Mobility

With the same configuration the simulations ran for three types of node placement grid, random and uniform node placement respectively. By observing the results the performance of the simulation varied in both terms of throughput and delay without mobility. Comparing these results it should concluded that random node placement has high throughput in 600 m^2 of terrain size. Similarly in 800 m^2 grid has high throughput in the same configuration. These results obtained for static mobile simulations as in **Fig. 2a and b**.

3.2. With Mobility

In this simulation random waypoint mobility was applied for movement of mobiles for the above configuration. The nodes and various parameters are the same only thing is mobility is added for 600 m^2 and 800 m^2. By observing it is noticed that the throughput of random node placement was high in 600 m^2 terrain size and in 800 m^2 terrain size grid node placements has high throughput as in the **Fig. 3a and b**.

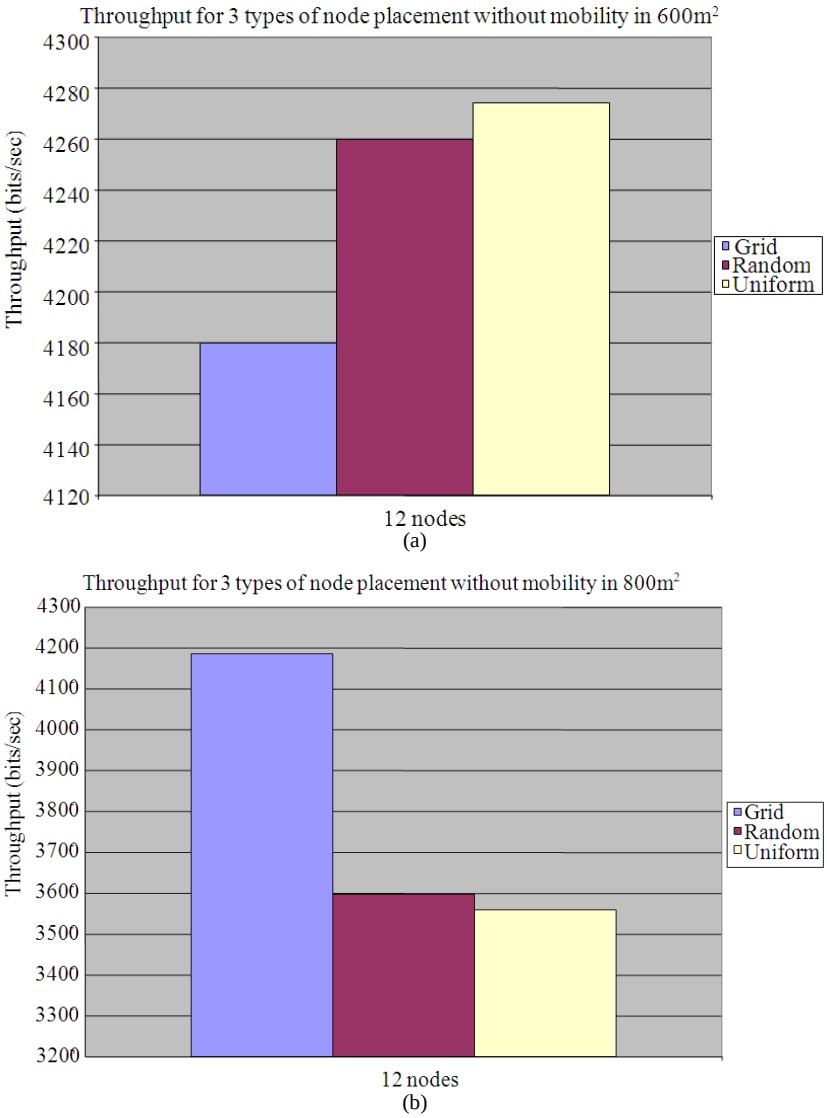


Fig. 2. (a) Throughput for 600 m^2 (b) Throughput for 800m^2

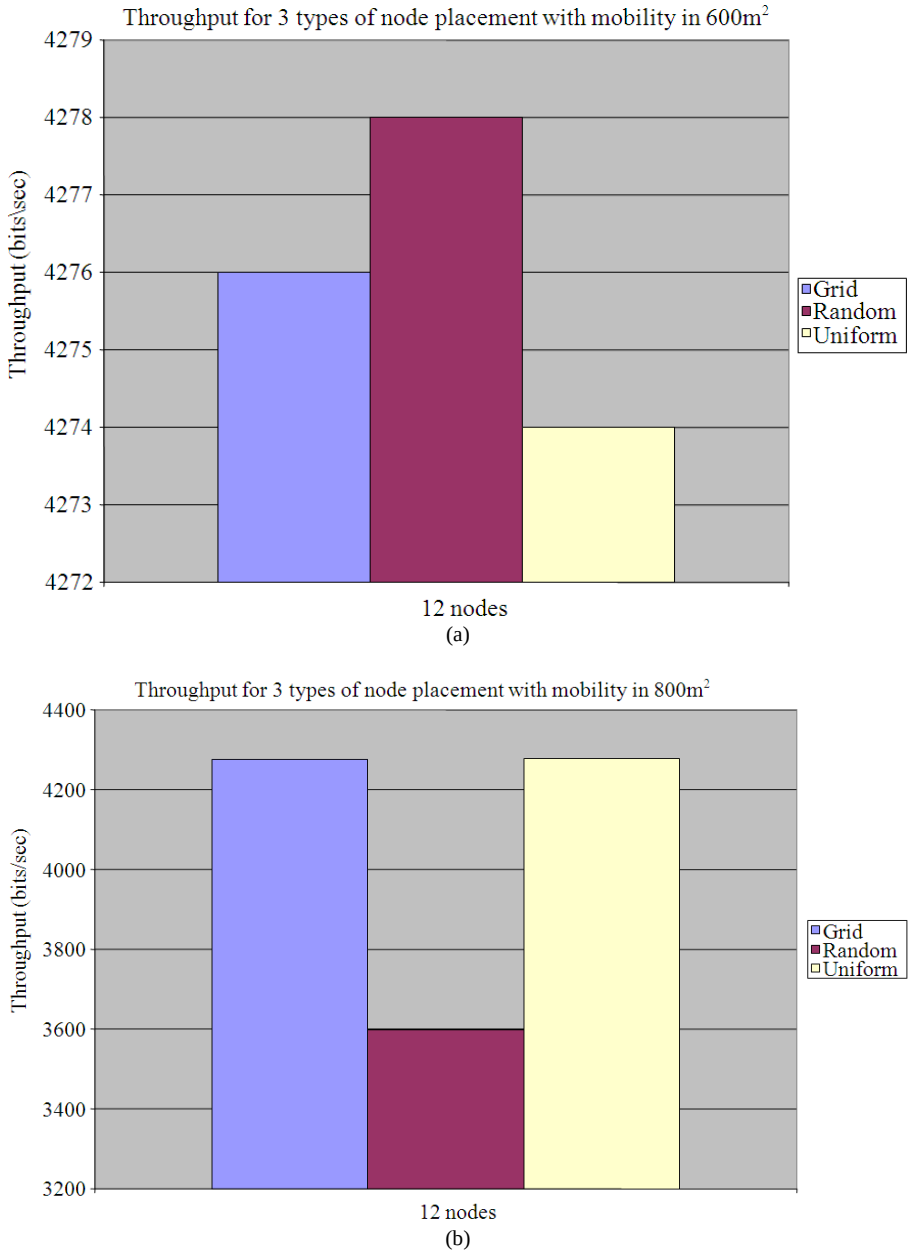


Fig. 3. (a) Throughput for 600m^2 (b) Throughput for 800m^2

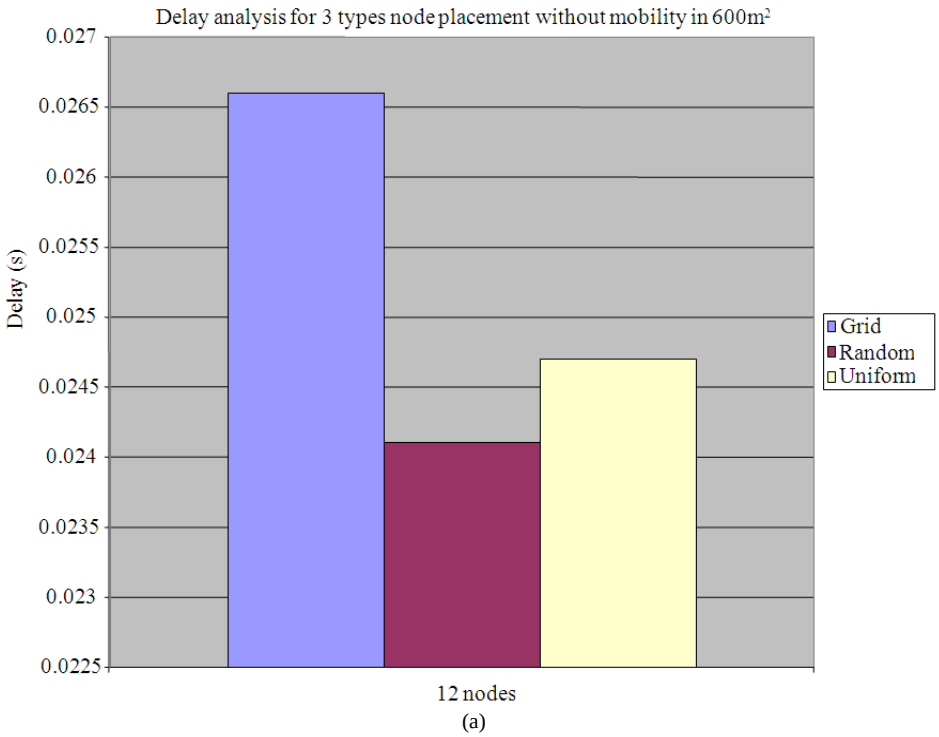
3.3. Delay Analysis

3.3.1. Without Mobility

By observing these simulation in 600 m^2 grid node placement has high delay and 800 m^2 random node placement has high delay in static mobile node simulations without changing the configuration as in **Fig. 4a and b**.

3.4. With Mobility

By observing these simulation with mobility in 600 m^2 grid uniform placement has high delay and in 800 m^2 random node placement has high delay in static mobile node simulations without changing the configuration as in the **Fig. 5a and b**.



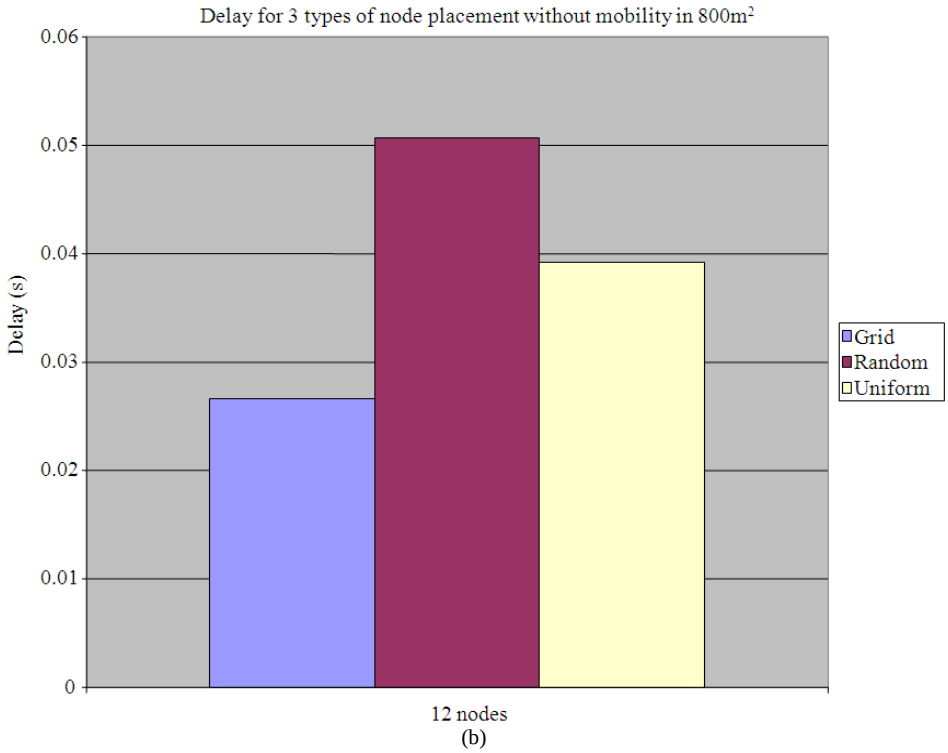


Fig. 4. (a) Delay for 600m^2 (b) Delay for 800m^2

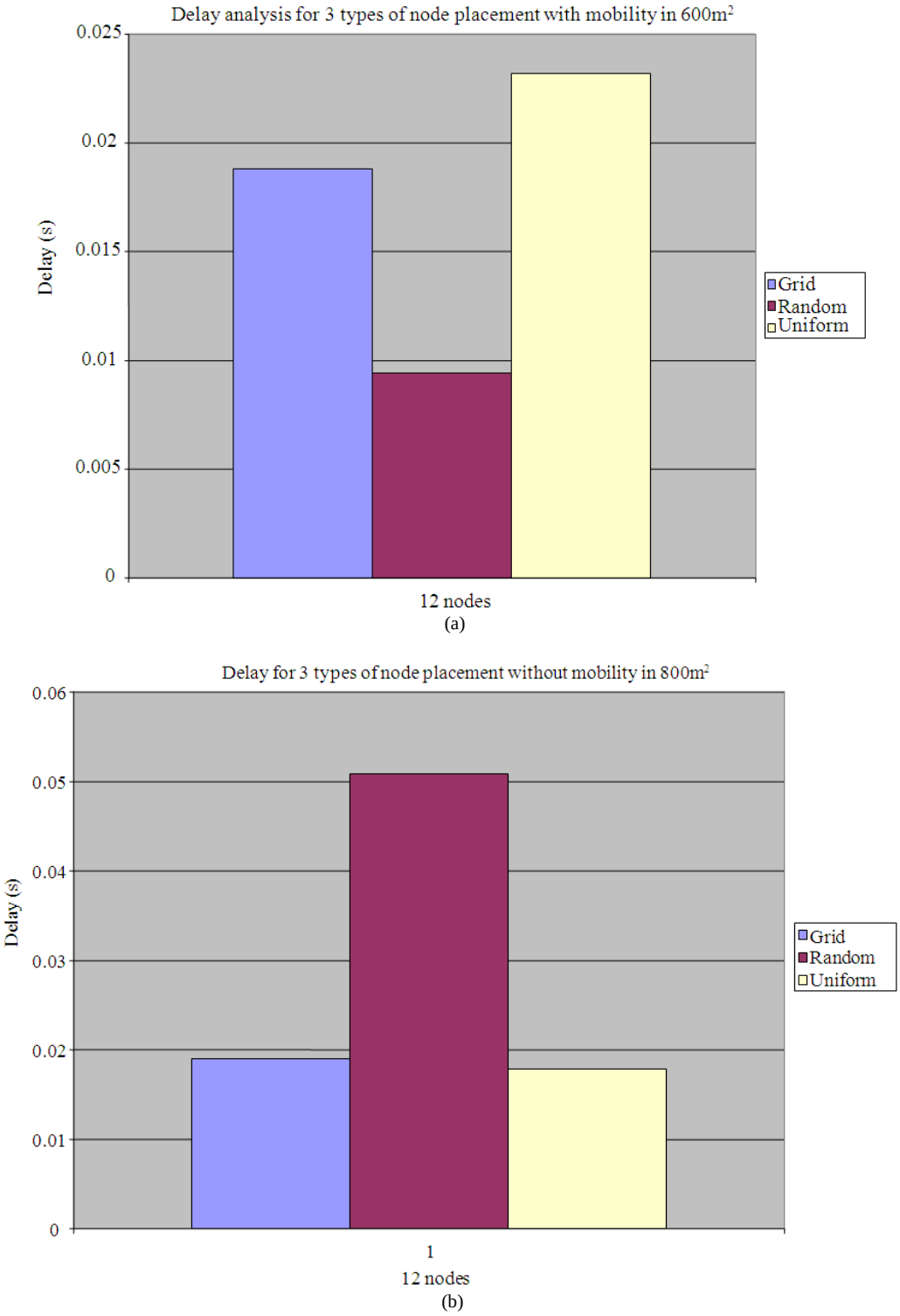


Fig. 5. (a) Delay for 600m^2 (b) Delay for 800m^2

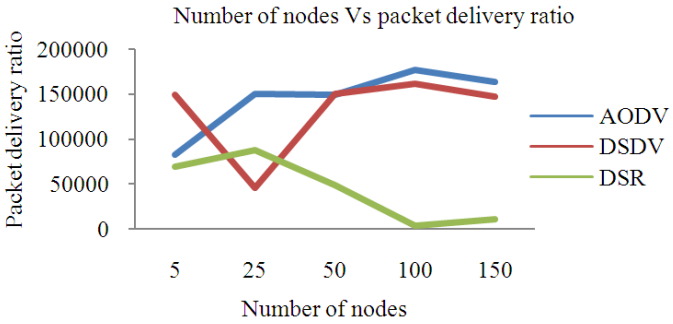


Fig. 6. Analysis of AODV, DSDV, DSR

4. DISCUSSION

From the result obtain from the simulation tool NS2 the graph has drawn and the nodes that are placed in random manner. **Figure 6** clearly depects that the analysis of the AODV, DSDV, DSR. The graph **Fig. 6** shows that the AODV is the best among the DSDV and DSR the thorough put has maximum with the specified number of nodes.Trustworthiness of the system enbaled by keep on track of the nodes behaviour, based on the misbehaviour the node's trust analyzed and if any behaviour activity has been avoided and hence network enables the trustworthiness. By refereing (Dhulipala *et al*., 2013) the trustworthiness has brought to this work.

5. CONCLUSION

From this scalability study and simulation experiments with trust worthiness, the work can be concluded that making some changes in the terrain size and the type of node placement with same configuration may vary the performance of any type of ad hoc network and the trustworthiness has achieved by the behavioral based trust formation, the formation of trustworthiness verifies the node behaviour at each and every process. The performance of AODV, DSR, TORA and OLSR ad hoc routing protocols under varies load with the help of NS2; More over the pros and cons of the routing protocols are also clearly shown in the study. The future Enhancement of this work with added security consideration it can be extend in to more number of nodes in the network to ensure the trustworthiness.

6. REFERENCES

Saravanan, D., R.M. Chandrasekaran, B.V. Prabha and V.R.S. Dhulipala, 2011. Trust worthy architecture implementation for mobile ad hoc networks. Int. J. Comput. Sci. Eng., 3: 2601-2609.

Bobade, N.P. and N.N. Mhala, 2012. Performance evaluation of AODV and DSR on-demand routing protocols with varying MANET size. Int. J. Wireless Mobile Netw., 4: 183-196.

Setty, S.P., K.N. Raju and K.N. Kumar, 2010. Performance evaluation of AODV in different environments. Int. J. Eng. Sci. Technol., 2: 2976-2981.

Velloso, P.B., R.P. Laufer, D.D.O. Cunha, O.C.M.B. Duarte and G. Pujolle, 2010. Trust management in mobile ad hoc networks using a scalable maturity-based model. IEEE Trans. Netw. Service Manage., 7: 172-185. DOI: 10.1109/TNSM.2010.1009.I9P0339

Uma, M., R. Chandrasekaran and V.R.S. Dhulipala, 2013. Study and analysis of routing protocols in mobile ad-hoc network. J. Comput. Sci., 9: 15-19. DOI: 10.3844/jcssp.2013.1519.1525

Karthik, N. and V.R.S. Dhulipala, 2011. Trust calculation in wireless sensor networks. Proceedings of the 3rd International Conference on Electronics Computer Technology, Apr. 8-10, IEEE Xplore Press, Kanyakumari, pp: 376-380. DOI: 10.1109/ICECTECH.2011.5941924

Dhulipala, V.R.S., N. Karthik and R.M. Chandrasekaran, 2013. A novel heuristic approach based trust worthy architecture for wireless sensor networks. Wireless Personal Commun., 70: 189-205. DOI: 10.1007/s11277-012-0688-1