A Novel Approach towards the Node Isolation Attack in the MANET

Abhijeet More
Pillai HOC College of Engineering and Technology, Rasayani, Mumbai, India.
abhijeetdmore242@gmail.com

Dr. Ashok M. Kanthe
Head of Computer Department Pillai HOC College of Engineering and Technology, Rasayani, Mumbai, India.

Abstract

The Mobile Ad-hoc Network (MANET) is self-arranging communication network of the Versatile node. The MANET does not have any earlier structure of communication. The Mobile Ad-Hoc network creates a network with the help of intermediate nodes. The MANET network is an open network environment so that intermediate node can participate in communication. The MANET has a many security problems, because of the public nature of the network. The malicious node can quickly enter into the system. The security issue mainly contains a denial of service attacks like Node Isolation Attack, packet drop, black hole, gray hole assault, and so forth. The Node Isolation Attack (NIA) is a Denial of Service (DOS) attack against AODV. The aim of this attack is to isolate all communication information of node or group of nodes. The attack in which the attacker node is avoids the getting communication, information about the network to victim node. This proposed algorithm works on the removal of Node Isolation Attack in MANET. This proposed algorithm implemented in Network Simulator 2.35. The concept of Node Isolation is utilized for identification malicious node introduce into the system. The proposed algorithm is finding attacker node from the system, which is hurtful to the system and increment the generally the execution of the system.

Keywords – Node Isolation Attack, Denial of Service, mobile ad-hoc networks, overhead, gray hole attack, Packet drop attack, AODV Protocol.

1. Introduction

The Mobile ad hoc network is self-organized communication network where physical network downfall, the temporary network is created [1]. The temporary network has no any centralized monitoring system to maintain the network. The main purpose of this network is an emergency communication to the stations. As stated this does not have any monitoring system, the nodes are acting as routers as well as intermediate nodes or stations. The routing of the message in the network is based on intermediate nodes present in the network. This is an open network, so any node can join this network and starts the communication. This network uses different routing protocols to route the message to the appropriate destination. When source wants to communicate destination node, it uses either saved path or creates a new path to the destination [2]. On this concept routing protocols have two types first one is Proactive and second one is Reactive protocol. The proactive protocols are Distance Sequence Distance Vector (DSDV), Optimized link state routing (OLSR) and reactive protocols are Ad hoc On Demand Distance Vector (AODV). This paper mainly focuses on the reactive protocol, because on demand the creation of a path may harmful to the network. The network has many node , it is very difficult to differentiate between the true nodes and fake nodes.

2. Related Work

Nadav Schweitzer et al proposed Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes which based on OLSR protocol [3]. This paper gives solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Also, this paper gives extension to their solution regarding to all DOS attacks in MANET. But this paper has normal increases overhead as increases size of the network.

Vishvas Kshirsagar, et al proposed Analytical Approach towards Packet Drop Attack in Mobile Ad-hoc Networks [4]. This paper states the mathematical model of detection of attack, also gives mathematical model proof with scenarios.

Jin-Hee Cho et al proposed on the tradeoff between altruism and selfishness in MANET trust management, in which considered the trade-off between nodes, individual welfare vs. global welfare and identify the best design condition of this behavior model to balance to selfish vs. altruism behaviors [5].

K. Urmila Vaidhya et al proposed A Novel Technique for Defending Routing Attacks in OLSR in the MANET [6], it investigates the various routing attacks that can be launched in OLSR. Analyzing the attack, we propose a mechanism to secure the OLSR protocol from specific routing attack known as a node isolation attack in MANET.

Abhijeet More, et al proposed A Detection and Remove the Node Isolation Attack in the MANET. This paper survey to an how to detect and remove the node isolation from a network[11].

3. AODV Protocol

Ad-hoc on-demand Distance Vector (AODV) protocol is reactive protocol [7, 8]. In AODV protocol routers are created when they are needed rather than table driven approach. AODV do not store any network structure for routing. AODV protocol has a different method for routing the data over the networks; methods are route discovery, route table management, route maintenance and local connectivity management. In route discovery method source node directly communicates to the destination node if there is no intermediate node between a source node and destination node. Each node stores the information in tabular format. The table contains the fields like destination IP address or node ID, next hop, number of hops, the destination sequence number means the highest sequence number, active neighbors in this route and time to leave for a particular route.

Route discovery starts when the source node table contains no information available by broadcasting a route request (RREQ) packet to all the neighboring nodes within range of the source node, RREQ travel through intermediate nodes until valid path for destination node is not found.The RREQ packet contains the source node IP address, sequence number, broadcast identity, destination IP address and hop count. The sequence numbers are always incremented only when RREQ packet, or Request Reply (RREP) has sent. The RREP is created by an intermediate node on the path to the destination node. A source node may receive a multiple RREP message, but valid fresh and shortest is selected to accurate and secure path between a source node and destination node. Once a path is set up between a source node and destination node, the actual data has been sent. RREP contains the source IP address, destination IP address, and a destination sequence number, hop count and life time.

In path maintenance, repeatedly RREQ message is sent to check whether a neighbor's link is active or not.The RREQ message does not effect on sequence numbers. If intermediate link fails, it generates RRER message and send the source node, the source node restarts route discovery and finds appropriate route to the destination node

4. Node Isolation Attack

The Node Isolation Attack (NIA) is a Denial of Service (DOS) attack against AODV. The aim of this attack is to isolate all communication information of node or group of nodes. The attack in which the attacker node is avoids the getting communication, information about the network to victim node. The basic idea of this attack is the attacker node prevents link information of a specific node or group of node from being spread to the whole network. Thus, other nodes who could not receive the link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

The attacker node creates an imaginary link by propagating dummy RREQ messages and attract all other nodes to select the attacker node as intermediate node. Thus the only node must forward and generate a RREQ message to the destination node is attacker node. This attacker intermediate node drops all messages contains network information and cannot generate a RERR message for the destination node. The attacker node can prevent spreading the communication information on the network. The figure 1 shows the node isolation attack.

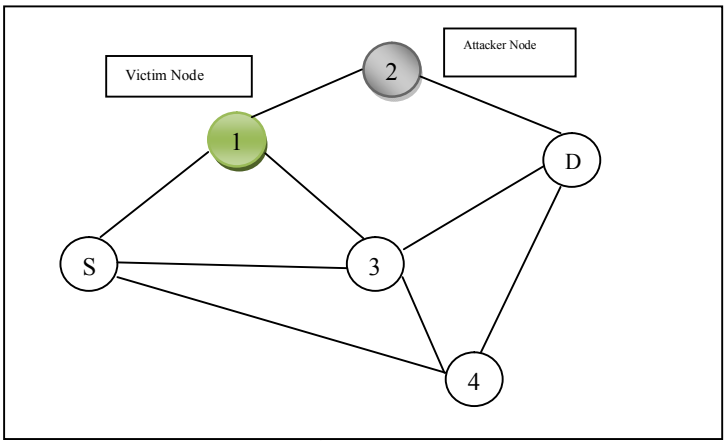


Fig:1 Node isolation Attack

Consider the network scenario of six mobile nodes, the node S wants to communicate with the destination node D. The source S starts the establishing the path between Node S to node D by sending a RREQ message along with the TC message as per working of AODV protocol. While establishing the path between the source and destination node, the intermediate nodes are helping to establish a path. Due open environment of the network there are also malicious nodes available. The attack in which the attacker node 3 has avoided the getting communication, information about the network to victim node 2. The attacker node 3 prevents link information of a node 2 being spread to the whole network as shown in figure 1. Due to isolation attacker node, if shortest path is available in the network, they are also longest path being selected for the communication. Also victim node is available for the communication. But due to node isolation attacker node hide the presence of victim node in the network.

5. A Novel Mechaism Against Node Isolation Attack

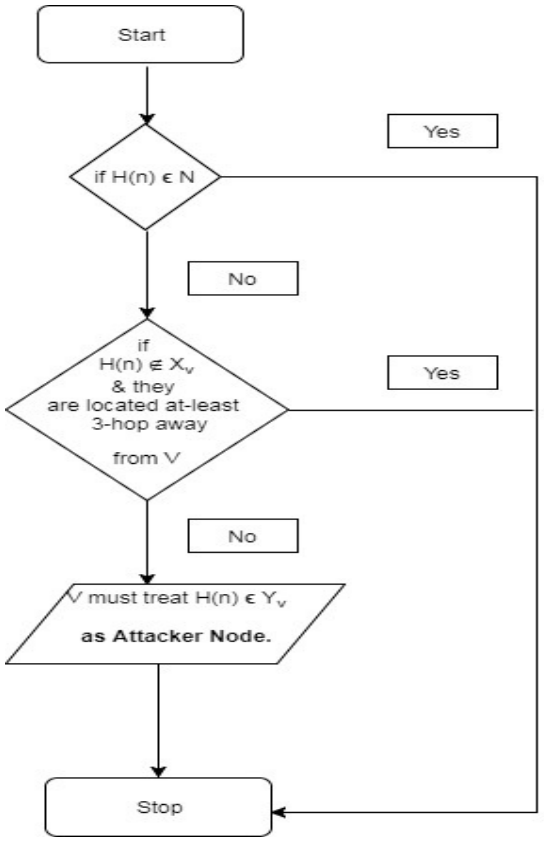
Mobile ad-hoc network, is frequently changing communication environment may affect the performance the MANET. The Security problem can reduced by removing the malicious node present in the network and increase the overall the performance of the network. Assuming there are some rules for testing RREQ message. If they are satisfied the sender is trustworthy.
The three rules are:
1) A victim must confirm that all nodes declared in the RREQ message of attacker must not be among the victim's 1-hop neighbors
2) For each node in the RREQ message, check:
a. Existence of 1-hop neighbors not mentioned in RREQ message
b. Also, they are located at-least 3-hop away from the victim
c. If the above conditions are satisfied, then check whether the attacker has appointed any other intermediate node to cover those nodes
3) The Victim must treat a RREQ message containing all the 1-hop neighbors as an attack

A. Algorithm for detecting node isolation attacker node: (at each node)

Step 1: (periodically RREQ message received at each node)
Consider H (n) is a RREQ message all nodes & N is set of all nodes
if H (n) $\in$ N
Yes, Goto step 5
No , Goto step 2
Step 2: [Consider V is victim node and X_v is set of 1-hop neighbors actually]
if H(n) $\notin X_v$
Yes, Goto step 5
No, Goto step 3

Step 3: Also, they are located at-least 3-hop away from V
Step 4: [Y_v is sets of 1-hop neighbors shown in H (n)]
V must treat H (n) $\in Y_v$ **as Attacker Node**
Step 5: Remove the attacker node and broadcast the message to all nodes.
Step 6: Stop.

B. Flowchart for detecting node isolation attacker node:



6. Simulation Work and Result Analysis

The proposed algorithm is simulated in Network Simulator (NS-2) [9]. NS-2 is open source network simulation tool. The802.11 MAC layer implemented in NS-2 is used for simulation. The protocol used is AODV. The various parameters are considered to compare the results. The wireless channel type with Omnidirectional antenna type is used to link. This simulation uses 802.11 MAC type. The 200 × 200 m2 simulation area is used.

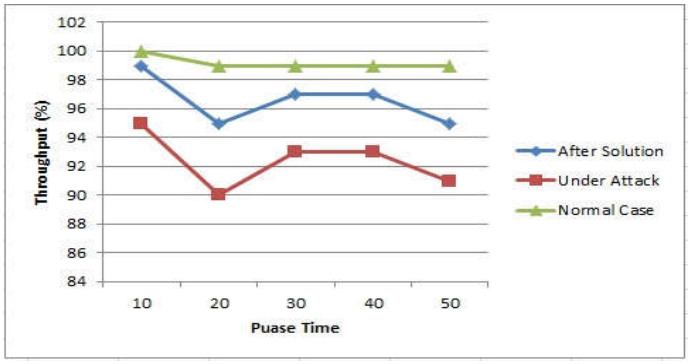
Simulation Parameter	Used in Simulation
Simulator	NS-2.35
Number of Nodes	Variable
Protocol Studied	AODV
Number of Sources	Variable
Maximum Speed	Variable
Pause Time	Variable
Simulation Area	200 × 200
Data Payload	512Bytes/packet
Link Layer Type	LL
Antenna Type	Omni antenna
Channel Type	Wireless Channel
DoS attack	Node Isolation Attack
CBR Rate	50 Kbps
Traffic Type	CBR(UDP)
Radio propagation model	Two Ray Ground

Table 1: Simulation Parameters

A. Effect of Pause Time on Throughput

Figure 2 shows the graphs generated between the throughput and the pause time. Figure 2 shows that when the network is under attack, the average of the packet delivery ratio is 42 % and when it's under attack with the solution it improved up to 80 %. When we applied solution on the packet drop attack the throughput is increased because utilization of the network is increased. The throughput is directly proportional to utilization of network that is maximum use nodes gives maximum throughput. The malicious node is included in the establishment of a path.

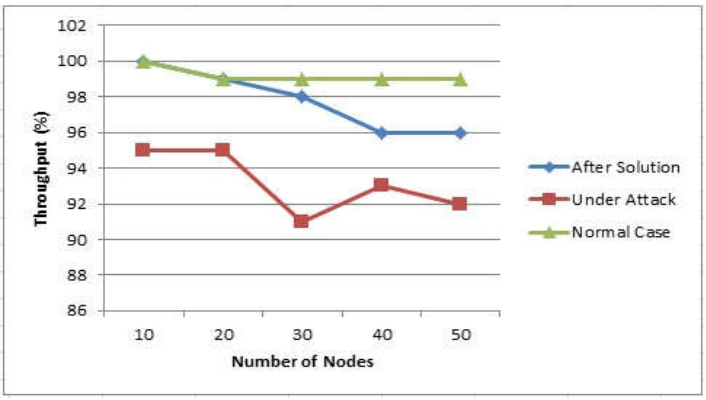
Fig 2: Pause Time Vs Throughput



B. Effect of Number of Nodes on Throughput

Figure 3 shows the number of nodes Vs. throughput. Figure 3 shows, when the network is under attack, the average of the packet delivery ratio is 40% and when it's under the solution it improved up to 83%. When any node wants to communicate with another node, there will a maximum number of secure next hops for the communication because of removal of node isolation from a network.

Fig 3: Number of Nodes Vs Throughput



7. COMPARISION OF PROPOSED ALGORITHM AGAINST EXISTING WORK

A. Comparison incase of Number of attacker node:

Figure 4 shows that number of attacker node vs throughput. The base paper [3] throughput results are below the proposed paper throughput results. As increasing numbers of attacker node the result of the proposed paper is decreasing, as in base paper [3] results are increasing.

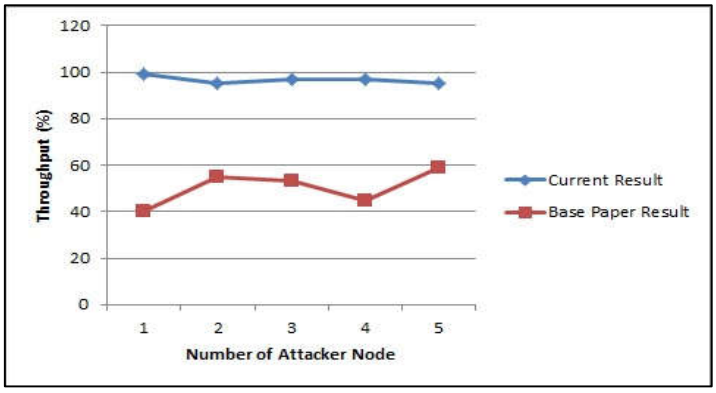


Fig 4: Number of attacker node Vs Throughput

B. Comparison incase of Density of node:

Figure 5 shows the Density of nodes vs. throughput. The base paper [3], while an increasing number of nodes in the network, constantly decreasing the throughput. In case of proposed paper while an increasing number of nodes in the network, constantly decreasing the throughput but 30% less than base paper.

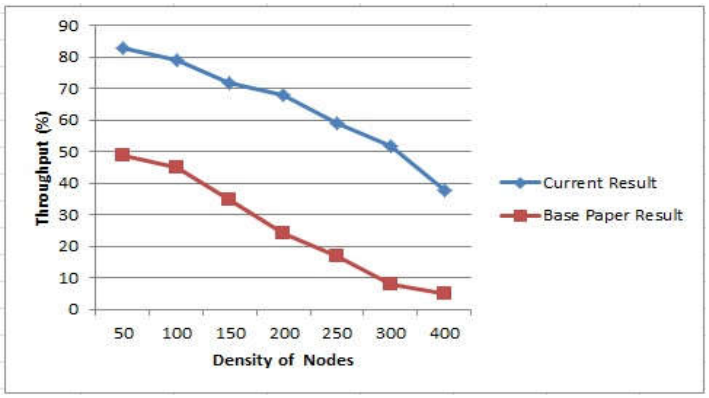


Fig 5: Density of nodes Vs Throughput

8. Graphical Result

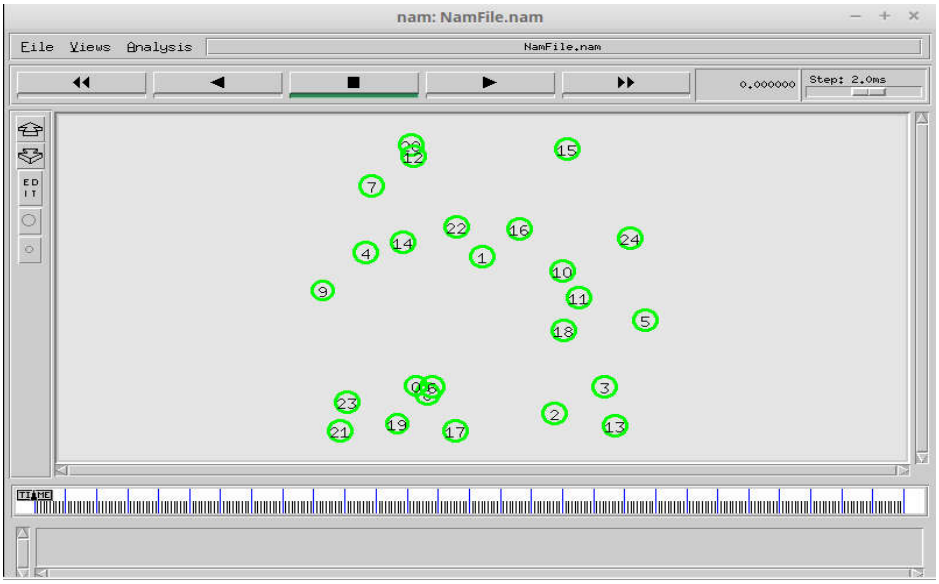


Fig 6: Deployment of nodes

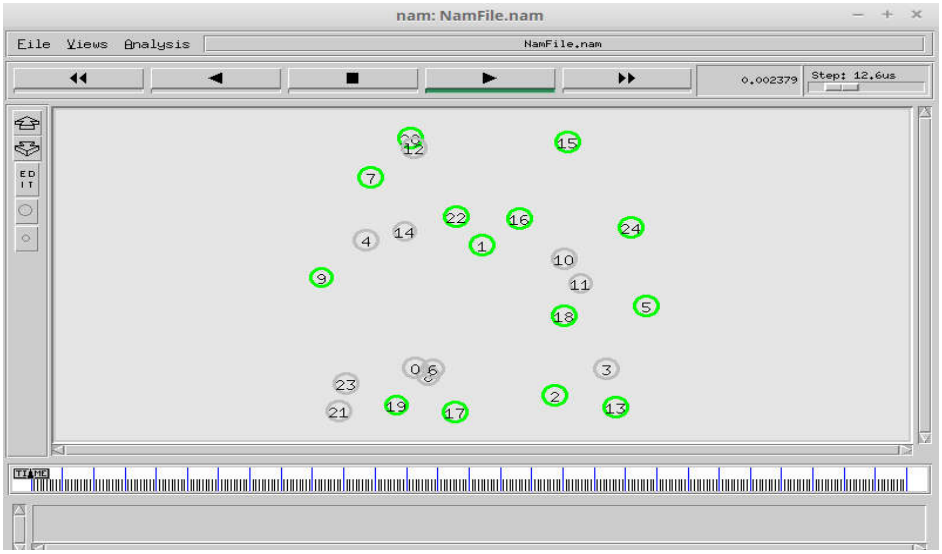


Fig 7: node Isolate

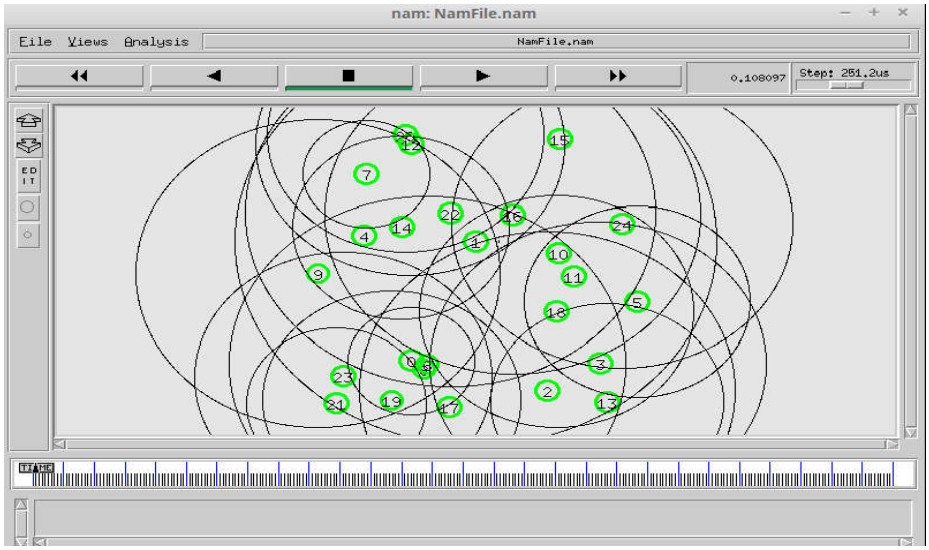


Fig 8: flow and packet transmission between nodes after removal of Isolation

9. Conclusion

Mobile ad-hoc network is oftentimes changing communication environment may influence the execution the MANET. The Security problem can reduced by removing the node isolation present in the network and increase the overall performance of the network. The Proposed model is a way of finding attacker node from the network, which is harmful to the network. In proposed model the isolated node is dropped from the network and path is established for future communication by updating link wise information into the routing table.

References :

[1] R. Prasad, S. Dixit, R Van Nee, “Globalization of Mobile and Wireless Communication” March 2011, Springer, P 335

[2] L. Gavrilovska, R. Prasad, Ad-hoc Networking towards Seamless Communications” Springer 2006, p. 284.

[3] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Asaf Shabtai, and Roy David Margalit " Mitigating Denial of Service Attacks in OLSR" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 15, NO. 1, JANUARY 2016.

[4] Vishvas Kshirsagar, Ashok M. Kanthe, Dina Simunic, ”Analytical Approach towards Packet Drop Attack in Mobile Ad-hoc Networks” ,IEEE ICCIC 2014.

[5] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, "The Impact of Packet Drop Attack and Solution on overall Performance of AODV in Mobile Ad-hoc Networks" IJRTE, ISSN: 2249-8958, Volume-2, December-2012

[6] S. NeelavathyPari, D Shridharn, “Mitigation Routing Misbehavior in Self Organization Mobile Ad-hoc Network using K-neighborhood Local reputation System”, IEEE-International Conference on Recent Trade information Technology, ICRTIT, Chennai June-3-5, 2011.

[7] Md. Amir KhusruAkhtar, G. Sahoo, "Mathematical Model for the Detection of Selfish Nodes in MANET" IJCSI, 2010 ISSN 2231 –5292,

[8] C.Perkins,E.B. Royer, S.Das, Ad hoc On-Demand Distance Vector Routing, Proceeding of the 2nd IEEE Workshops on Mobile Computing System and Applications(WMCSA),pp.90-100,1999.

[9] C. Perkins, E. B. Royer and S. Das, “Ad hoc On Demand Distance Vector (AODV) Routing, Internet Draft”, RFC 3561, IETF Network Working Group, July 2003.

[10] Md. Amir Khusru Akhtar, V. S. Shankar Sriman, G. Sahoo, "A Methodology to overcome Selfish Node attack in MANET", Knowledge management and E-learning: An International Journal, Serial Publication-2009.

[11] Abhijeet More, Ashok M. Kanthe " A Detection and Remove the Node Isolation Attack in the MANET "IJTRD, 2017 ISSN 2394-9333.