*International Journal of Advanced Trends in Engineering and Technology (IJATET)*
*Impact Factor: 5.665, ISSN (Online): 2456 - 4664*
*(www.dvpublication.com) Volume 2, Issue 1, 2017*

# COLLABORATIVE DECISION TECHNIQUE FOR BLACKHOLE ATTACK PREVENTION IN MANET

**K. Thangadurai*, I. Pradeep Kumar** & M. Shankar*****
Department of Information Technology, M.P.N.M.J Engineering College, Chennimalai, Erode, Tamilnadu

**Cite This Article:** K. Thangadurai, I. Pradeep Kumar & M. Shankar, "Collaborative Decision Technique for Blackhole Attack Prevention in MANET", International Journal of Advanced Trends in Engineering and Technology, Page Number 60-65, Volume 2, Issue 1, 2017.

**Abstract:**

Mobile Ad hoc Network (MANET) is really an economical network and provides communication in a dynamic environment. The security is essential for this kind of decentralized network. To overcome the disputes, there is a need to build a prevailing security solution i.e. IDPS (Intrusion Detection & Prevention System) that achieves both extensive protection and desirable network performance. MANET may be unprotected against collaborative effect of Blackhole attack. One of these attacks is the packet dropping Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination by that due to this attack, data loss will occur. The damage will be serious if malicious node in a network working as an attacker node absorbs all data packets delivered through them. In this paper we proposed a simple IDPS Algorithm against dropping attack and measure the network performance after applying IDS. The proposed approach is provides zero attacker infection and also improves the routing performance of network. The simulation of blackhole attack is done in free ware simulator network simulator 2 (ns-2) and measured the packet loss in the presence of attacker and in presence of Intrusion Detection System against malicious attack. The proposed solution improved network performance and provides better performance than normal due to presence of reliable paths that is not available in normal AODV routing.

**Key Words:** Packet Dropping Attack, IDS, Routing, AODV, Security & MANET

## 1. Introduction:

Mobile Ad hoc networks in a short foam MANET is a group of autonomous nodes that are a self-managed with none infrastructure. They typically have a dynamic topology specified nodes will simply be a part of or leave the network at any time and that they move around freely which provides them the name Mobile unintentional Networks or MANETs. they need several potential applications, particularly in military Associate in attention rescue operations like connecting troopers within the battle field or establishing a short lived network in situ of one that folded when a disaster like an earthquake. In these networks, besides acting as a number, every node additionally acts as a router and forwards packets to the proper node within the network once a route is established. To support this property nodes area unit use routing protocols like AODV (Ad hoc On Demand Distance Vector Routing Protocol). Mobile ad-hoc networks area unit sometimes at risk of totally different security threats and malicious node attack is one among these. During this attack, a offender nodes that absorbs and drops all information packets makes use of the vulnerabilities of the on demand route discovery protocols. In keeping with the routing strategy routing protocols are often classified as Table-driven or Proactive routing protocols and on demand or supply initiated. (DARPA) Packet Radio Network (PRNet) and SURAN project. Being freelance on re-established infrastructure, mobile unintentional networks have blessings like rate and easy readying, improved flexibility, and reduced prices. Mobile unintentional networks area unit acceptable for mobile applications in either hostile setting wherever no infrastructure is out there or briefly established mobile applications, that area unit price crucial. In recent years, application domains of mobile unintentional networks have gained a lot of and a lot of importance in non military public organizations and in industrial and industrial areas. The standard application eventualities embody rescue missions, enforcement operations, cooperating industrial robots, traffic management, and academic operations in field. Security in Mobile Ad-Hoc Network is that the most significant concern for the fundamental practicality of network. The supply of network services, confidentiality and integrity of the info are often achieved by reassuring that security problems are met [2]. MANETs usually suffer from security attacks attributable to its options like open medium, dynamic its topology dynamically, lack of central watching and management, cooperative algorithms and no clear unconscious process. These factors have modified the battle field state of affairs for the MANETs against the safety threats.

## 2. Related Work:

The previous work done in field of security against blackhole attack is mentioned in this section. We are doing a work on attacks mentioned in Akshai Aggarwal, Savita Gandhi et. al. [1] "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs" in that work they proposed a Trust Based Secure On Demand Routing Protocol called "TSDRP". Ad hoc On-demand Distance Vector (AODV) routing protocol has been modified to implement TSDRP for making it secure to thwart attacks like Blackhole attack and DoS attack. To evaluate the performances.

Dr. A. A. Gurjar, A. A. Dande, [3] "Black Hole Attack in Manet's: A Review Study" in this title we discuss Black hole attack is one of the possible attacks in MANET. In black hole attack, a malicious node sends the route reply message to the source node in order to advertise itself for having the shortest path to the destination node. The malicious node reply will be received by the requesting node before the reception of the any other node in the network. When this route is created, malicious node receives the data packet, now it's up to the malicious node whether to drop all the data or forward it to the unauthenticated nodes.

Hesiri Weerasinghe and Huirong Fu, [4] "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation" In this title , via simulation, we evaluate the proposed solution and compare it with other existing solutions in terms of throughput, packet loss percentage, average end-to end delay and route request overhead. The experiments show that (1) the AODV greatly suffers from cooperative black holes in terms of throughput and packet losses, and (2) our solution proposed in presents good performance in terms of better throughput rate and minimum packet loss percentage over other solutions, and (3) our solution proposed in can accurately prevent the cooperative black hole attacks.

Harjeet Kaur, Manju Bala, Varsha Sahni [5] "Study of Blackhole Attack Using Different Routing Protocols in MANET" This research effort focused first the comparative investigations of routing protocols under the various types of attack then to create scenario and simulate and investigate the performance metrics viz. Packet delivery ratio, average jitter, average throughput and end to end delay of reactive, proactive and hybrid routing protocols such as AODV and AODV with blackhole attack, OLSR and OLSR with blackhole attack and ZRP and ZRP with blackhole attack for the different scenario under the different conditions.

Nitesh A. Funde, P. R. Pardhi [6] "Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey" in this title we have focus different techniques to prevent black & gray hole attacks in MANET. Mobile ad hoc network (MANET) is a self-configuring network of mobile nodes formed anytime and anywhere without the help of a fixed infrastructure or centralized management. It has many potential applications in disaster relief operations, military network, and commercial environments. Due to open, dynamic, infrastructure-less nature, the ad hoc networks are vulnerable to various attacks. AODV is an important on-demand distance vector routing protocol for mobile ad hoc networks. It is more vulnerable to black & gray hole attack. In MANET, black hole is an attack in which a node shows malicious behaviour by claiming false RREP message to the source node and correspondingly malicious node drops all the receiving packets.

Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, Rajib Das [7] "Security Measures for Black Hole Attack in MANET: An Approach" In this title, we give an algorithmic approach to focus on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. Our aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting & removing Black hole node(s) in the MANET at the beginning. Also the objective of this title is to provide a simulation study that illustrates the effects of Black hole attack on network performance.

Ei Khin and Thandar Phyu [8] "Impact Of Black Hole Attack On Aodv Routing Protocol" In this title, we are simulating and analyzing the impact of black hole attack on Ad Hoc On-Demand Distance Vector (AODV) protocol. The simulation is carried on NS-2 and the simulation results are analyzed on various network performance metrics such as packet delivery ratio, normalized routing overhead and average end-to-end delay.

Rupinder Kaur and Parminder Singh [9] "Review Of Black Hole And Grey Hole Attack" This title deals with the study of analysis of delay occurs by these attack in Wireless Mesh networks and its types and also discuss about previous study by which we get idea about attack occurs in networks and also study various techniques to detect and prevent network from black hole and grey hole attack. Then we discuss about their result by using simulator OPNET.

Jaspal Kumar, M. Kulkarni, Daya Gupta [10] "Effect of Black Hole Attack on MANET Routing Protocols" In this title we have analyzed the effects of Black hole attack on mobile ad hoc routing protocols. Mainly two protocols AODV and Improved AODV have been considered. Simulation has been performed on the basis of performance parameters and effect has been analyzed after adding Black-hole nodes in the network. Finally the results have been computed and compared to stumble on which protocol is least affected by these attacks.

Ashish Sharma, Dinesh Bhuriya, Upendra Singh, Sushma Singh [11] "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing" In this title we are focus black holes attack. TAODV is a secure routing protocol based on trust model for mobile ad-hoc network. We have taken TAODV routing protocol approach to focus on analyzing and improving the security of Black hole in AODV routing protocol. AODV is a popular routing protocol for mobile ad-hoc network. Our aim is on ensuring the security against black hole attack. The metrics energy, throughputs and packet delivery ratio are used to determine the performance of AODV, AODV with black hole attack and Trusted AODV. By using simulation tool on ns2, the energy of Black hole is more as compare to TAODV and throughput of TAODV is better compare to black hole AODV, similar to packet delivery ration is better compare to black hole AODV. Before Mobile unintentional network (MANET) has emerged as a replacement frontier of technology to provide anyplace, anytime communication, because of its readying nature, MANETs area unit a lot of at risk of

malicious attack. Because of the absence of centralized administration security is that the main issue in mobile unintentional network and attackers' area unit terribly simply changed the particular behavior and performance of network. Our main aim to watch the performance of network while blackhole attacker present in network and applied correct methodology to secure network against attack.

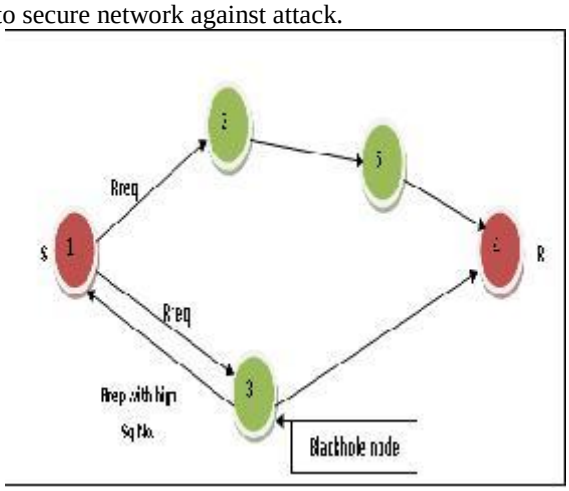


Figure 1: Illustration of Black Hole Attack

**3. Problem Statement:**

The absolute security within the mobile unintentional network is incredibly onerous to realize attributable to its basic characteristics, like dynamic topology, open medium, restricted vary and practical resources. The most downside that happens from attack is it consumes and changed the particular behavior of packets and because of the absence of centralized controller it's terribly tough to seek out that node or nodes within the network making an abnormal behavior. So we design a Collaborative Decision Technique for Blackhole attack Prevention in MANET and secure the network.

**4. Proposed Work:**

On the basis of problem statement we apply intrusion detection and prevention technique in MANET that must be deployed to facilitate the identification and isolation of attacks. Due to nature of mobility and open media MANET are much more prone to all kind of security risks as covered. Here we detected and prevent the network from blackhole attacker node, that attack is a active attack and that attack explanation with the help of example, we assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 intermediate node between Node 1 and Node 4 so initially in case of route requesting time Black Hole Node 3 immediate send false RREP, Where sender node receive route reply packet, sender node sends actual data packet through Black Hole Node 3, Black Hole Node 3 Receives data packets, if data packets are UDP then this packets Capture by the Black Hole Node and if TCP type packet then Block This type Packets By Malicious Node. So our Network has infected. In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets. In this section provide the detection and prevention mechanism against blackhole attack, As nodes in mobile ad hoc networks have a limited transmission range, they expect their neighbours to relay packets meant for far off destinations. These networks are based on the fundamental assumption that if a node promises to relay a packet, it will relay it and will not cheat. The reputations of the nodes, based on their past history of relaying packets, can be used by their neighbours to ensure that the packet will be relayed by the node. An intrusion detection and prevention scheme (IDPS) to detect and defend against malicious nodes' attacks in MANET is presented in the network.

The IDPS are breaks into two part IDS (intrusion detection system) and IPS (Intrusion Prevention System), IDS are apply for behavior analysing of the network that time we apply AODV routing protocol and one blackhole attack node, that node mislead at the time of sender broadcast routing packet in the network so black hole node certainly response reply to the sender node and then sender node send's data packet through black hole node without any other information tacking of routed node , that black hole node capture the data packet and can't send that packet to actual receiver node so this type of mislead detect through file processing technique and analyse the network behavior and get blackhole attacker node number and mislead time or attack time after that scheme in next step we execute protection of black hole attack module, for that design collaborative decision making system, in this system at least two node collectively watch the all neighbour node's and if more than two protector node simultaneously identified attacker node than watch the profile of attacker node and collaborative take the decision for separation of attacker node from network after that protector node broadcast the blocking message to all connected node so in future no any node can communicate

with attacker and current sender search new path without participating attacker node, that mechanism more secure as compare to local intrusion prevention mechanism. In NS-2 part very first we create mobile node and set all the required parameter of the mobile network like antenna type is Omni directional antenna, MAC type 802.11 wireless communication, routing protocol as AODV (Ad-hoc on demand distance vector) routing and then we create sender node and receiver node after all the parameter setting we also attach application layer data FTP and CBR (Constant bit rate) if each parameter setting then routing protocol execute that time if and mislead node present like blackhole node so that deviated the routing function and drop actual data packet. So our motive to protect and detect that type of misbehavior through the network then we apply at least two IPS node in the network that prevent through mis happen in the network and improve the performance of the network.

**5. Proposed Algorithm:**

In this section provide formal description of our proposed work, in this algorithm two or more protector node independently watches the traffic and node behaviour and collaborative take action against blackhole attacker node. Through the proposed IDPS we detect the attacker behaviour and protect blackhole attack under MANET.

Algorithm: Blackhole Detection and Prevention IDPS
Input:
M: Mobile node's S: Sender node's R: Receiver Node's
I: Intermediate node's B: blackhole node's Spn: Prevention node's
Output: PDR, Throughput, Overhead blackhole node detection
Algorithm Steps:
S← initiate route message S_brodcast(S,R, Routing)
While (I in range && radio range == true) do
If I update routing table && Sequence_no == higher
Then
False route send to S
S← receives route message Send data(S,I, tcp, udp)
Else
I receives route packet && forward to next hop If next hop == R
R send acknowledge packet to S S← receives route message Send data(S,I, tcp, udp)
End if End do
IDPS: Intrusion detection and prevention Spn← watch-neighbours
While Spn>=2 && neighbour node in range do I set as suspicious B
If B update routing && set sequence number == higher
Then
Spn← Watch I behaviour
If I drop || not forward to next hop Then Spn
i← Take decision for B blocking
Spn : Send acknowledge to S node for route updating S_brodcast(S,R, Routing not in route)
S← established path to R && eliminate B node Send data(S,R, tcp, udp)
End if End if End do

**6. Simulation Environment:**

The simulation will do on the NS-2 (version ns -3.31) on the basis of some simulation parameters mentioned n table1.

Table 1: Simulation Parameter

| | |
|---|---|
| Simulator Used | NS-2.31 |
| Number of nodes | 50 |
| Dimension of simulated area | 800m×800m |
| Routing Protocol | AODV |
| Simulation time | 100 sec. |
| Traffic type (TCP & UDP) | CBR (3pkts/s) |
| Packet size | 512 bytes |
| Number of traffic connections | 10 |
| Node movement at maximum Speed | random (20 m/s) |
| Transmission range | 550m |
| Attack Type | Black Hole |
| Prevention Technique | Collaborative IDPS |

**7. Performance Evaluation:**

There are following different performance metrics have been considered to make the comparative study of these routing protocols through simulation.

**1) Routing Overhead:** This metric describes how many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets.

**2) Average Delay:** This metric represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination. It is measured in seconds.

**3) Throughput:** This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps

**4) Packet Delivery Ratio:** The ratio between the amount of incoming data packets and actually received data packets in dynamic network.

**5) Blackhole Node Detection:** Check the behaviour of generated profile and if detect the profile is not match with normal behaviour than identified the node number and time of capture the data file that gives the blackhole attacker node

**B. Total Data Capturing Analysis by Black Hole Node:**

In this parameter we calculate total number of data captured by the blackhole node that help to calculation of percentage of attack in the network.

**C. Security Percentage Measurement:**

After getting the blackhole node information we collaborative set prevention node that protect the data capturing and blocking the data from attacker, that helps to calculate network parameter and provide percentage of security, presence of blackhole node.

**8. Results Discussion:**

The simulation results are evaluated on the basis of simulation parameters. The parameters are common for all the four scenarios.

**A. Packet Delivery Fraction Analysis:** The packets percentage is measures through performance metrics Packet Delivery Fraction (PDF). In this graph the PDF performance is examine in normal AODV, Black hole attack, existing security scheme TSDRP and proposed Prevention scheme. Here the attacker PDR performance in presence of black hole attacker is only 10%. That shows the degradation in network performance. The proposed prevention scheme is provides the protection against attack and provides performance equivalent to normal routing performance.

**B. Throughput Analysis:** The throughput performance of network is calculated by number of packets per unit of time received at destination or number of bits received at destination. In this graph the throughput performance is measures in same four scenarios. The performance of proposed detection and prevention scheme is provides t he better result in presence of attacker in MANET. The throughput in presence of attacker is almost negligible but in case of proposed scheme throughput performance is maximum, which provides the better routing performance in dynamic network.

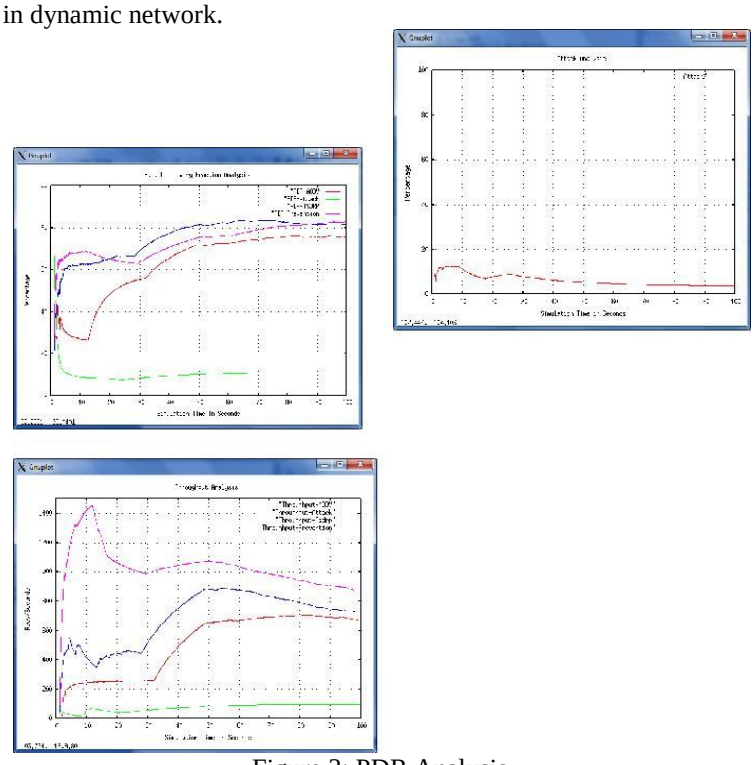

Figure 3: PDR Analysis

**C. Attack Percentage Analysis:**

The attacker individual presence in MANET is dumping the whole performance of network. The attacker is only one aim, is to drop the whole packets in network. The attacker is able to performance routing

misbehaviour against normal routing performance. In this graph the attacker loss is only evaluated in black hole presence. The attacker is drop about 5% to 6% percentage of data drop in network and also by this remaining performance is also affected.

**D. Over all Summarized Performance Analysis:**

The summarized routing performance in given simulation time is mentioned in table 2. In this table of protocols are mentioned. The clear performance is shows that the highest number of packets sends and receiving in network is mentioned in proposed prevention scheme. The reason of performance improvement as compare to normal routing is not available reliable path but in proposed scheme it is possible, that improves network performance in MANET.

Table 2: Overall Analysis

| Parameter | Normal -AODV | Blackhole Attack | TSD - RP | Proposed- Prevention |
|---|---|---|---|---|
| SEND | 7479 | 5243 | 7065 | 7915 |
| RECV | 5670 | 432 | 5752 | 6563 |
| ROUTINGPKTS | 5333 | 5897 | 9919 | 4673 |
| PDF | 75.81 | 8.24 | 81.4 | 82.92 |
| NRL | 0.94 | 13.65 | 1.72 | 0.71 |
| Average | 379.63 | 32.26 | 147 | 126.54 |
| Throughput | 675.52 | 95.82 | 735. | 872.61 |

**9. Conclusion and Future Work:**

The security in MANET is the major constraint because of absence of centralized administration. The blackhole attack as we know consume all data packets and degrades routing performance in network. In this research we simulate the scenario of attack, security and normal routing in networks and find its affects. In our study, we used the AODV routing protocol. But the other various routing protocols could be simulated also. This work is resolve collaborative effect of attackers in the network. But the detection of the attacker is possible through proposed IDPS security scheme. Our solution looks the path in the AODV level. As malicious node is the main security threat that effect the performance of the AODV routing protocol. Effect on packet loss is clearly visualized in throughput and other metrics. As malicious node is the main security threat that effect the performance of the AODV routing protocol. Its detection is the main matter of concern. Therefore the proposed IDPS algorithm work will be excellent to detect and defense the network from malicious attack. Improvement for overcoming the effect of attack should orient towards controlling the delay. The other attacker like flooding attack is also dropping the packets by occurring the condition of jamming in the network. In future some techniques should be proposed for securing network against both of these attackers. Also blackhole like packet dropping and flooding for AODV routing algorithm can be implemented in real life scenario and its analysis can be compared with the simulation analysis results.

**10. References:**

1. J Akshai Aggarwal et. al. “Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs” 2014 Fourth International Conference on Advanced Computing & Communication Technologies, 978-1-4799-4910-6/14 2014 IEEE DOI 10.1109/ACCT.2014.95
2. Irshad Ullah and Shahzad Anwar “Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols” IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, May 2013.
3. Dr. A. A. Gurjar, A. A. Dande, “Black Hole Attack in Manet’s: A Review Study” International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 3, March 2013.
4. Hesiri Weerasinghe and Huirong Fu, “Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008.
5. Harjeet Kaur, Manju Bala, Varsha Sahni “Study of Blackhole Attack Using Different Routing Protocols in MANET” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.
6. Nitesh A. Funde, P. R. Pardhi “Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013
7. Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, Rajib Das, “Security Measures for Black Hole Attack in MANET: An Approach” 2012 Assam University.
8. Ei Ei Khin and Thandar Phyu “Impact Of Black Hole Attack On Aodv Routing Protocol” International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.
9. Rupinder Kaur and Parminder Singh “Review Of Black Hole And Grey Hole Attack” The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014.