Implementation of Dempster-Shafer Theory for Trust based Communication in MANET

Geetanjali Batham
M.Tech (Cyber Security)
Madhav Institute of Technology and science
Gwalior,MP,India

Vikas Sejwar
Department of CSE & IT
Madhav Institute of Technology and science
Gwalior,MP,India

ABSTRACT
Mobile ad-hoc network is growing field of research where lots of work done regarding to security of network. Due its infrastructure and mobility of nodes change their position newly node easily enter or exit from networks and it is highly vulnerable to attacks. In this work we study about MANET and various attacks after that various technique to prevent our network from attacks, but all have some issues so overcome this problem we proposed a trust based technique in which communication occurred only between trusted nodes. Implementation of our work done on ns-2.35 and uniqueness of our work proof by packet delivery ratio, throughput and various results.

Keywords
Dempster-shafer, trust, attacks.

1. INTRODUCTION
MANET is a set of mobile services (nodes) which communicates using every one over an infrastructure less, self-configuring and decentralized network. The creation, deletion and operation of the network are complete by the mobile nodes. Because of no predefined infrastructure or central authority MANET is an interesting networking option for connecting mobile nodes rapidly and spontaneously like military application , rescue operation, civilian operation like adhoc meeting or adhoc classroom.[1]

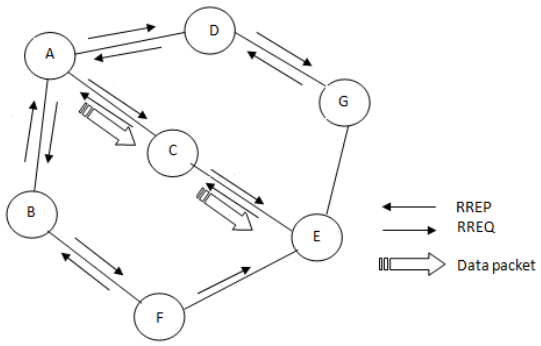


Figure. 1 MANET

Figure 1 shows the MANET architecture. Node A is source node and node E is destination node. Node A broadcast the RREQ to all the neighbor nodes present in the network with their information, all the node which has a route to destination will send the RREP packet containing the source route. RREP packet get by the source node. Data packet is forwarded by the most trusted nodes in the network. Whole process will repeat till packet get reach to the destination. In MANET all the nodes act as a router i.e. they routes the packet via various routing techniques.

If any sort of attack is obtain in MANET than it will affect the present of network and some important information may get stolen. To provide the security in MANET is the most challenging work. For that researcher are developing many new methods such as trust based techniques, etc.

Trust in general is point of particular belief about the entities behavior. According to eschenanuer et al.[2] trust defined as " a set of relation among entities that participate in a protocol". These relation are generated by the previous interaction of entities within a protocol.

Trust management performances as a separate component of security services in network and used to specified and interpret safety procedures and relationships. Trust management includes trust establishing, trust inform and trust revocation. There is slight difference between trust administration and notoriety administration i.e. trust is active while reputation is passive [3].

2. LITERATURE SURVEY
In [4] nilesh et al, describe the trust based method to relieve different attacks in MANET. In proposed system network is formed on the incorrect of cluster and in each cluster only 10 nodes are considered. Highest energy nodes within the cluster is selected as a trusted nodes and communication within the cluster and out of the cluster is carried out complete these trusted nodes.. Then counting packets is compared to the threshold value, if it less than threshold value then particular node is reflected as a malicious node.

In [5] subi et al, presents trust assurance beside Gray Hole attack. Direct trust calculated by beta distribution and indirect trust is calculated by different values(route request packet, route reply packet, route error packet and data packet) of neighboring node and combine by using Dempster-Shafer theory. After that packet dropping is checked by two method, first is average difference and second is by using the ratio of number of sent packet to number of received packet. If the ratio is a smaller amount than the assign threshold value then trust value is deducted by a constant value. If not, during the transmission each node calculate direct trust by combining the value of direct trust from past experience. All the recommendation of each node is calculated by Dempster Shafer theory and total trust is evaluated.

The trust based scheme is designed by chanil park et al in [6]. In this each node of the network calculate the trust value of their neighbor node. Then the recommender node choosen as a member of cluster head. To authenticate the cluster head, recommendation certificate(R-Certificate) given by the recommender node. So, the cluster head which has many R-certificates has high level of trust When member node joins the another cluster, then new cluster refers the trust value of node by the previous cluster head for node evaluation.

In [7] pang et al, describes the voting based algorithm. In which subjective trust is accessing by Bayesian method and evaluates the stability of node through computing the neighbor change ration and residual battery power of mobile nodes. In this scheme, if the node is most trusted among its neighbor node then vote is given to that node. In this, each nodes computes its stability. Then computes the trust of node with respect to neighbor. Each node votes its neighbor according to the voting algorithm. V(i) as the cluster head, if number of votes are same then choose the best stability as its cluster head, if votes and stability are same then choose the lowest ID as cluster head

In [8] P. Annadurai et al, describe the method of identifying malicious node upon the trust value. In the proposed system malicious node is detected by the direct and indirect trust value. Highest energy node is chosen as cluster head which maintains the counter table of every node. If any cluster member misbehaves in the cluster, then counter table decrease the value by one. Its nearby nodes gives the direct trust value about that node and the cluster head also ask the other members of the cluster about the misbehaving node. The other member have trust to the cluster head. By this approach malicious node is find in the cluster.

3. CLASSIFICATION OF ATTACKS

Attack is an act that is performed to evade safety services and break security policies of a system. Transmission of secure data over the network is main issue of MANET. Because of no-infrastructure, de-centralized and open nature of wireless system, MANET is highly

powerless against different attacks. There are two types of attack. 1. Passive Attack:- attempt to monitor the system, so they can use the information but doesn't alter the data. 2. Active Attack:- Attempt to alter the information to affect their operations. There are further are ordered into insider attacks:- performed by the element inside the organization within the association and outsider attack:- performed by the substance outside the organization(unauthorized entity)[9].

A. Black hole attack:- In this attack an attacker node attracts

the target node by presentation that it is having the shortest path to the destination[10]. If they receive the packet they intercept it.

B. Denial-of-service(Dos):- A malicious node generate lots of unnecessary routing request to make the network resources engage so that they could not serve for the network.

C. Impersonation:- A attacker node usages the IP address of other node to impersonate itself while sending the control packets[11].

D. Wormhole attack:- it is a attack performed by two attackers connected by high-speed wormhole link. In this packet flows between tunnel of two attacker and attacker who receive the packet by another attacker replays the packets in network.

E. Gray hole attack:- In this attack, attacker shows that it have a valid route to a destination node if they receive any packets then it drops the blocked packets.

F. Rushing Attack:- In this attack, attacker rapidly forward the route discovery or route request packets then authentic nodes by use of duplicate suppression mechanism. Thus the chances of selection of path introduces by attacker gets increases.

There are several kind of attacks in MANET. But in our proposed work we use these two attacks.

G. Vampire Attack:- In this attack, attackers sends various messages which drains the energy of member nodes which may cause network failure and data loss.

H. Distributed Denial-of-service(DDos):- In this attack, various attacker target a single node. So that various attacker sends the routing request to single node so it will be busy on serving the request and halt at one point.

4. DEMPSTER–SHAFER THEORY

According to Glenn-Shafer "The Dempster–Shafer theory (DST) otherwise called the theory of belief function is mathematical theory of evidence". Belief function is calculated by the evidence collected by the different source that takes into account all the available evidence[12].

A. Value Factors

Value Factor (VF) is a positive real number connected with the significance of evidence.

B. Evidence

An Evidence E is a 2-tuple <m,VF>, where the fundamental probability task characterized by m and distinct by

$m(\Phi) = 0$

and

$$\sum_{A \subseteq \Theta} m(A) = 1$$

C. Belief Functions

In D-S theory, subsets of a given set is represented by proposition. Suppose a finite set of states define by Θ , and let set of all subsets of Θ is denote by 2^{Θ}. In D-S theory Θ is called a frame of discernment. A belief function over θ is describe by a function bel:2^{θ} □ [0,1]. For probability assignment m: 2^{θ}□ [0,1]

$$Bel(A) = \sum_{B \subseteq A} m(B)$$

for all $A \in 2^{\Theta}$, A measure of total belief describes by the Bel(A). for all nonempty C belongs to Θ, The combined evidence is describe by a m(C) which is a basic probability assignment.

One frame of discernment have several believe function and taking into account unmistakable bodies of evidence, Dempster's rule of combination. Which is presented by

$$m(C) = \frac{\sum_{A_i \cap B_j = C} m_1(A_i) m_2(B_j)}{1 - \sum_{A_i \cap B_j = \phi} m_1(A_i) m_2(B_j)}$$
$$C \subseteq \Theta$$

The orthogonal sum is compute by this formula, which characterizes the joined evidence.

Suppose one frame θ have two believe function Bel1 and Bel2, with m_1 and m_2 basic probability assignment . Then the function m: 2^{θ} □ [0,1] defined by m(Φ) = 0 and for all non empty $C \subseteq \theta$, the combined evidence described by the m(C) which is a fundamental plausibility assignment[13].

Suppose evidences E1 and E2 have two independent Value Factor VF1 and VF2 respectively. 1 is formed by combination of these two evidence known as total belief, but as per same time, our belief to either one of these two evidences is less than 1. And we define the Value factors of the combination of two value factor result equals to $(VF_1+VF_2)/2$

D. Extended D-S Evidence model

with Value factors: Suppose E1 = <m1, VF1> and E2=<m2,VF2> are two independent evidences, then the combination of E1 and E2 is

E=<$m_1 \oplus m_2$, $(VF_1+ VF_2)/2$>, where ⊕ is Dempster's rule of combination with value factors.

5. PROBLEM STATEMENT

MANET is now growing field of research where nodes have no fixed infrastructure and because of mobility of nodes it changes topology frequently. New node can easily enters or exit from network so that attack can easily performed in mobile ad-hoc network. Energy also a great problem for this network because of when nodes move and transmitted the packet each time nodes reduce their energy.

In existing technique "Design also, usage of trust based way to deal with alleviate different attacks in MANET" trust based node select on the base of energy that mean highest energy node become trusted node but in this study MANET threaten by vampire attack in which malicious node consume another nodes energy so that if on the basis of energy we select trusted nodes it's not necessary that we get always trusted nodes.

To overcome this problem we proposed a "Trust Calculation using Dempster Shafer for finding true nodes in MANET" in which trust of nodes calculate on the basis of their behavior.

6. PROPOSED WORK

MANET is popular now days because of its highly usable and by using it communication become faster. Attacks easily deploy in this network, so that for secure communication we propose a trust created simple technique so that we save energy of nodes and improve the life time of network. For trust calculation we take normal network scenario trace file in which we take three fields RREQ, RREP, Energy on the basis of these three fields we train our network and find out trusted node. At start we select cluster on the basis of neighbors and energy of nodes below we mention algorithm for initial cluster head selection method.

If((node>>higherenergy)&&(moreneighbour)) {

Initially elect node as a cluster head

Communication start and trust calculation begin }

Now nodes are communicate to each other and Dempster Shafer start working and nodes trust calculation start. On the basis of trust now we choose another cluster head, and secure communication going on.

Trust calculation.

Input: trace file with three column RREQ,RREP,Energy

Output: trust of nodes

Step1: take trace file for trained our network

Step2: now nodes behavior check for each transmission

Step3:
if((RREQval>>RREQthresh)&&RREPval<RREPthres)&&Energy) {

Assign node a value // mass of nodes

Else

Assign node value // mass of nodes on the basis of behavior

Step4: by using output of step3 we create focal set

Step5: update nodes on classifier set

Step6: now we have two set one is true node set and another is malicious nodes set

Step7: block malicious node.

Step8: exit

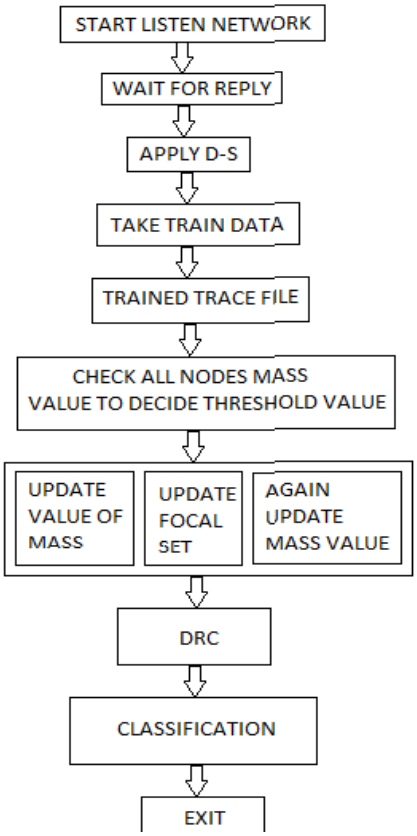


Figure 2. WORK FLOW

7. RESULT AND SIMULATION

Simulation of our technique done on ns-2.35 we take AODV protocol for communication.

Table 1. Simulation Table

Tool	Ns-2.35
Protocol	AODV

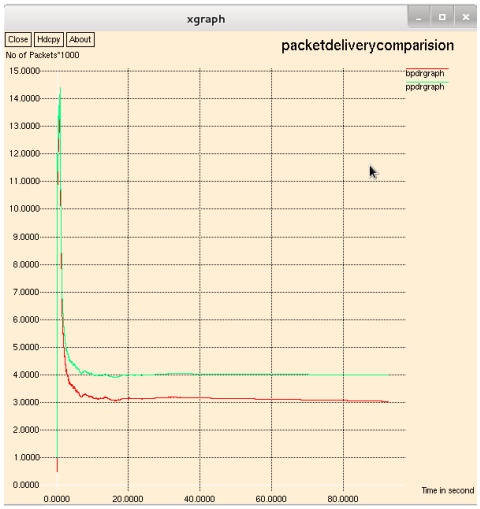
Number of nodes	30
Traffic type	CBR
Area	300*300
Packet size	1000bytes
Simulation time	100ms
Queue size	50
Antenna	Omni direction
Mac	802_11

In our proposed work Dempster-shafer theory is applied for trust calculation of member nodes so if malicious nodes are found they are eliminated so result gets improved.

In graphs, comparison is done. red line shows graph of problem statement and green line shows the graph of proposed work.

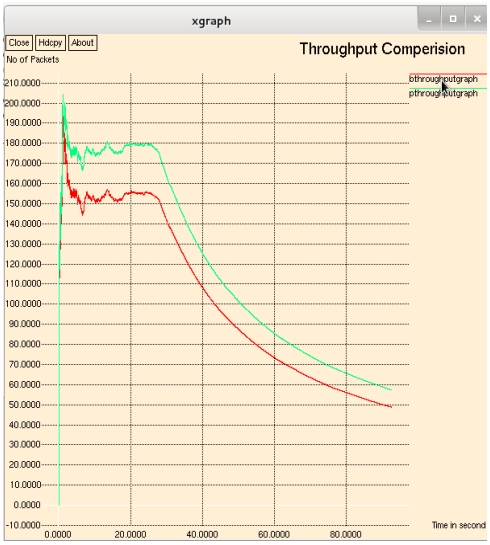
7.1 Packet delivery ratio

"PDR is define as the ratio of data packets gets by the destinations to generated by the sources per unit time"[14].



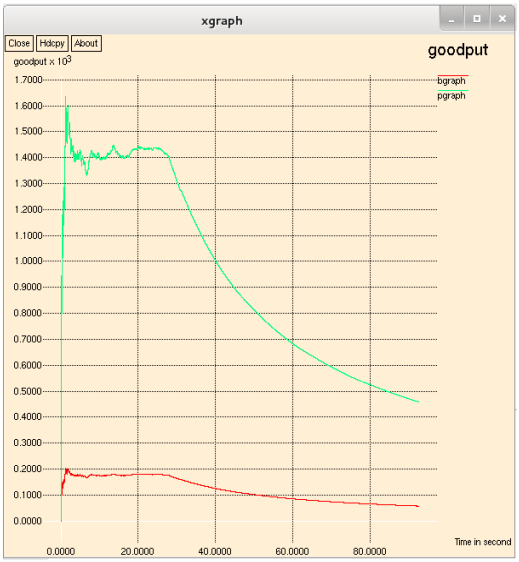
7.2 Throughput

It is defined as the total amount of data packets move from one place to another place in certain time period.



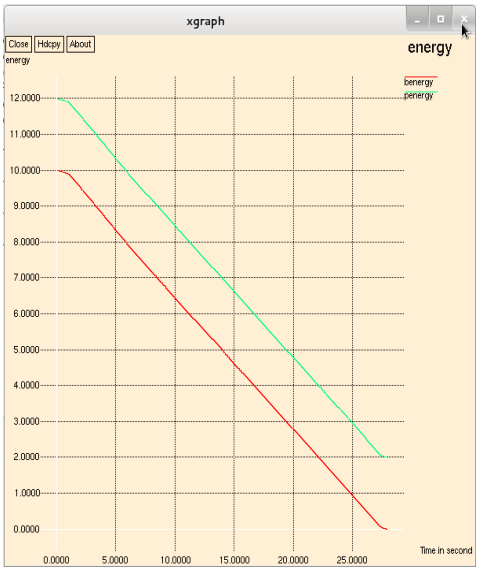
7.3 Goodput

Goodput is defined as the percentage of sent data packets actually received by the intended destinations. Goodput is an important indicator for QoS. We compute goodput as the ratio of the number of successfully received data packets to the number of sent data packets. The lost (dropped) packets include both those dropped by misbehaving nodes and those dropped by various other reasons like full queue, link errors, looping timeouts, etc...



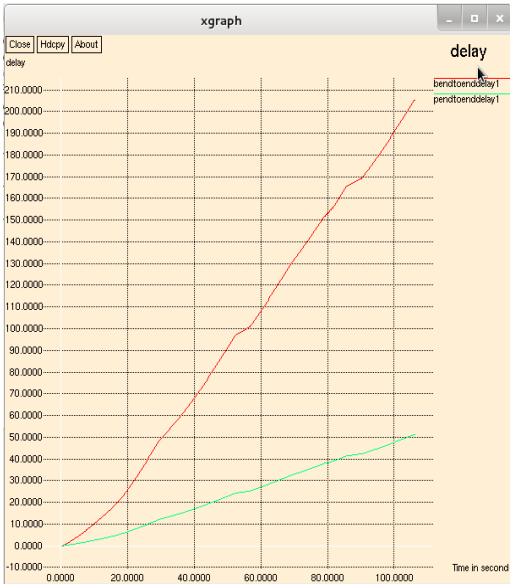
7.4 Energy of nodes

Energy of nodes decreases when nodes sends and receives the RREQ and RREP packets.



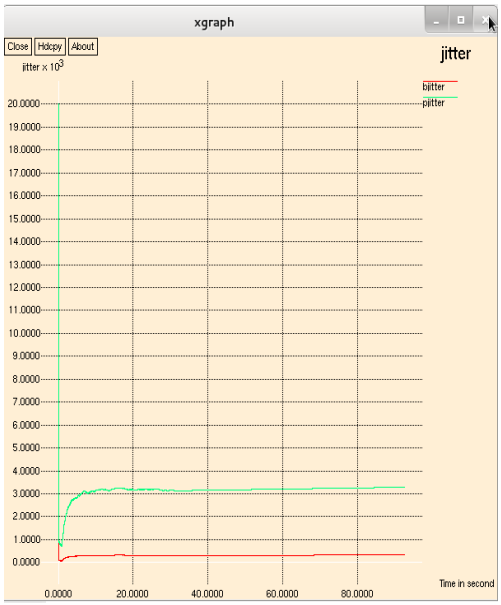
7.5 Delay

The average delay of data packets is the interval time among the time of data packet creation and the time at which last bit reaches to the destination.



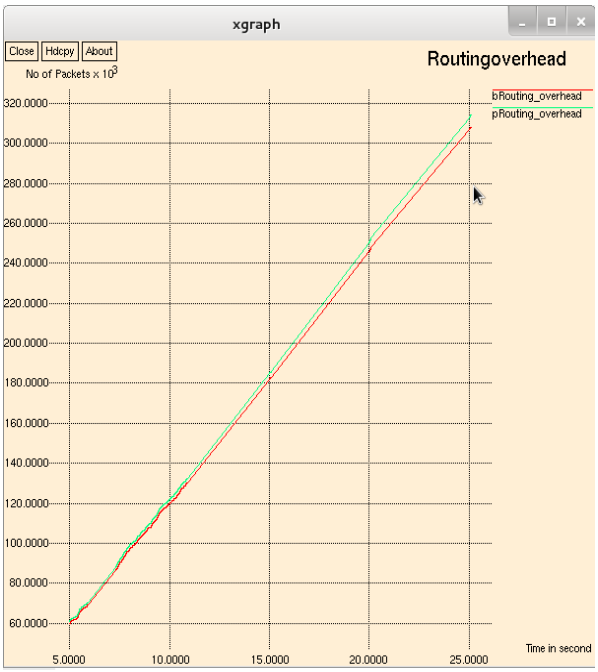
7.6 Jitter

Jitter is defined as a variation/fluctuation in the end to delay of received packets.



7.7 Routing overhead

Routing overhead is number of hopes through which packet transmit to the destination. Both, routing and data packets have to share the same network bandwidth most of the times, and hence, routing packets are considered to be an overhead in the network. This overhead is called routing overhead. A good routing protocol should incur lesser routing overhead.



8. CONCLUSION

MANET is growing field of research where lots of work done regarding security for security by seeing simulation result we concludes that our proposed work better as compare to existing technique. Packet delivery ratio throughput good put jitter result are enhance so that quality of service of our work is increase and energy of nodes decrease slowly so that it improve the life time of network.

9. REFERENCES

[1] Karuturi.Satish, K. Ramesh "Intrusion Determent using Dempster-Shafer Theory in MANET Routing" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 37-41

[2] L. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," Proc. 10th Int'l Security Protocols Workshop, Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.

[3] Savitasemplay, rajnisobti and veenumangat, "Review:Trust management in MANETs" International Journal of applied Engineering Research,ISSN 0973-4562 Vol.7 No.11(2012)

[4] Subi V S, NishanthN "Trust Assurance Mechanism against Gray Hole Attack in Mobile Ad Hoc Network" International Journal of Advanced Trends in Computer Science and Engineering(IJATCSE), Vol.4, No.4 Pages:01-05(2015)

[5] C. Park, Y. Lee, H. Yoon, S. Jin and D. Chio, "Cluster based Trust Evaluation in Ad Hoc Networks", pp. 503-507.

[6] S. Peng, W. Jia and G. Wang, "Voting-Based Clustering Algorithm with Subjective Trust and Stability in Mobile Ad-Hoc Networks", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, **(2008)**, pp. 3-9

[7] P. Annadurai, S. Vijayalakshmi "Identifying Malicious Node Using Trust Value in Cluster Based MANET (IMTVCM)", 20114 International Conference on Control, Instrumentation, Communication and Computational technologies(ICCICCT).

[8] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, Daud Israf, Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm, International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).

[9] Pooja Jaiswal, Dr. Rakesh Kumar, "Prevention of Black Hole Attack in MANET" IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No5, October 2012

[10] Y. R. Tsai and S. J. Wang, "Two-tier authentication for cluster and individual sets in mobile ad-hoc networks," Comput. Netw., vol. 51, no. 3, pp. 883–900, 2007.

[11] Pakleppa, M.; Vorstius, J.B.; Keatch, R.; Tapia-Siles, S.C.; Coleman, S.; Cuschieri, A. "Dempster-Shafertheory applied in state estimation of a pressure driven endoscope for Hydro-colonoscopy", Information Fusion

[12] Sun.L, Srivastava.R, and Mock.T, , 2006 "An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions," Management Information Systems, vol. 22, no. 4,pp.109-142**.**

[13] Zainab Dalaf Katheeth, Prof. K.K. Raman "Performance Evaluation with Throughput and Packet Delivery Ratio for Mobile Ad-hoc Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014