Path Mechanism to reduce packet data loss in Wireless Mesh Networks

Rajinder Singh
Research Fellow
Department of Computer Science and Engineering
Swami Vivekanand Institute of Engineering and Technology

Er. Nidhi Bhalla
Assistant Professor
Department of Computer Science and Engineering
Swami Vivekanand Institute of Engineering and Technology

ABSTRACT

A wireless mesh network (WMN) is a communication network made up of radio nodes organized in a mesh topology. Wireless mesh network often consists of mesh clients, mesh routers and gateways. A wireless Mesh network uses multi-hop communication. Due to multi-hop architecture and wireless nature, Mesh networks are vulnerable to various types of Denial of Services attack. It suffers from Packet dropping at Routing layer. Client nodes are unable to get services from gateway nodes, hence network gets down. The Paper emphasis on the developing of a path protocol when the minimun possible packet dropp occurs in wireless mesh networks. Due to packet droping occurrences the network performance degrades. In the work, we have evaluated the Performance of WMN under packet dropping on the basis of their throughput and Data packet loss.

Keywords: wireless mesh network (WMN), path protocol, packet dropping

Introduction

The proliferation of laptop computers and other mobile devices (PDAs and cell phones) created an obvious application level demand for wireless local area networking. In recent years, a wide variety of mobile computing devices has emerged, including portables, palmtops, and personal digital assistants. At present, most 802.11 Wireless Local Area Networks (WLANs) operate in the infrastructure Basic Service Set (BSS) mode. In it, all stations communicate via single wireless hop with a central entity denoted as Access Point (AP). An AP collocated with portal bridges the 802.11 with a non-802.11 network. Objective of 802.11 is to create the wireless local area network forming BSS (basic service set), BSS's together form the ESS (extended service set). In BSS, user can be mobile user instead of fixed which is the basic objective of 802.11. Also, users can have transition from one BSS to another BSS without the interruption of services called roaming. 802.11 WLAN can be used to provide services at airports, universities, home networking, office networking and outdoor wireless and much more, where the wired infrastructure is not desirable.

To become independent of backbone networks leading to cheap deployments, the traditional single-hop approach needs to be replaced by Wireless Mesh Networks (WMNs). Mesh BSS provides connectivity over multiple wireless hops. Path selection and forwarding operate transparently within the MAC.

WMNs are undergoing rapid commercialization in many application scenarios such as Broadband home networking, Community networking, Building automation, High-speed MAN, Intelligent transport system networks, Enterprise networking and much more.

Wireless mesh networks are becoming popular among Internet Service Providers due to cheap deployment and self healing properties.

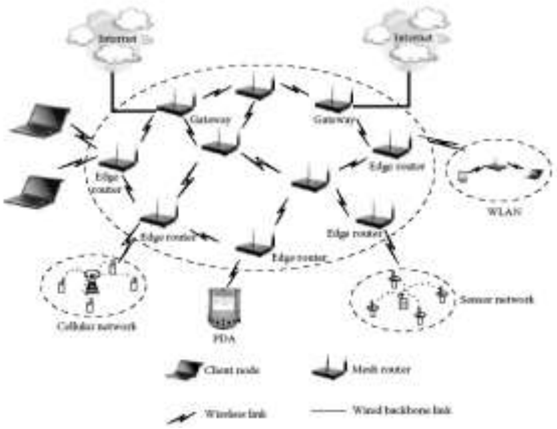


Figure 2.1 Architecture of Wireless Mesh Network [3]

LITERATURE REVIEW

A. Pirzada et al, 2004 described a model of building trust relationship between nodes in an ad hoc network. The nodes passively monitor the packets received and forwarded by other nodes and compute the trust values for their neighbours. The trust values are used for computing the trustworthiness of links. For routing, links with high trust values are chosen so as to avoid the malicious and selfish nodes [7].

A. Patwardhan et al, 2006 has proposed a trust-based data management scheme in which mobile nodes access distributed information, storage, and sensory resources available in pervasive computing environment. The authors have taken a holistic approach that considers data, trust, security, and privacy and utilizes a collaborative mechanism that provides trustworthy data management platform in an ad hoc network for secure authentication, data communication, data access and certificate and key management [8].

B-J.Chang at al, 2008 has proposed a trust-based scheme for multicast communication in a MANET. In a multicast MANET, a sender node sends packets to several receiving nodes in a multicast session. Since the membership in a multicast group in a MANET changes frequently, the issues of supporting secure authentication and authorization in a multicast MANET are very critical. The proposed scheme involves a two-step secure authentication method. First, an ergodic continuous Markov chain is used to determine the trust value of each one-hop neighbor. Second, a node with the highest trust value is selected as the certificate authority (CA) server. For the sake of reliability, the node with the second highest trust value is selected as the backup CA server. The analytical trust value of each mobile node is found to be very close to that observed in the simulation under various scenarios. The speed of the convergence of the analytical trust value shows that the analytical results are independent of the initial values and the trust classes [9].

G.Vigna et al, 2004 proposed an approach to detect intrusions in AODV that works by stateful signature-based analysis of the observed traffic. Sensors are placed on selected nodes for promiscuous sensing of radio channels. Each sensor has database of attack signatures and looks for a signature match in the traffic. A match triggers a response, usually an alert [10].

H.Yang et al, 2006 have proposed the SCAN protocol that addresses two issues simultaneously; (i) routing (control packets) misbehavior, and (ii) forwarding (data packets) misbehavior . Each node monitors its neighbors independently and the nodes in a neighborhood collaborate with each other through a distributed consensus protocol [11].

J. S. Baras et al, 2005 proposed a trust management scheme for self-organized ad hoc networks, where the nodes share trust information only with their neighbors . For establishing and maintaining trust among the neighbors authors have proposed a voting mechanism [12].

Jay dip, 2011 has proposed mechanism relies on local observation of each node in a WMN. Based on the local information in each node and using a finite state machine model of the AODV protocol, a robust statistical theory of estimation is applied to identify selfish nodes in the network. Using statistical estimation technique, analysis of variance and some additional fields in the headers of the AODV packets, this protocol is able to achieve a higher detection rate with a very low rate of false positives [13].

Jaydip Sen et al, 2011 proposed a self-organized trust establishment scheme for nodes in a large-scale MANET in which a trust initiator is introduced during the network bootstrapping phase . It has been proven theoretically and shown by simulation that the new nodes joining the network have high probability of successful authentication even when a large proportion of the existing nodes leave the network at any instant of time. A distributed detection mechanism of malicious packet dropping attack in MANETs has been proposed in , where local anomaly detection is utilized to make a more accurate network-wide (i.e. global) detection using a cooperative detection algorithm [14].

L.Santhanam et al, 2006 presented a mechanism to judge a node's behavior based on observed traffic reports submitted to local sink agents, dispersed throughout the network .The sink nodes apply a set of forwarding rules to isolate a selfish node based on the number of times it is caught in selfish acts. The scheme is independent of the routing protocol or network architecture, and is suitable for multi-channel wireless mesh network [15].

M.Conti et al, 2006 has proposed a scheme in which a node exploits its local knowledge to estimate the reliability of a path. Unlike the conventional method of denying selfish users, it provides a degraded service to these nodes by selective slow packet forwarding [16].

N.A Benjamin et al, 2010 proposed that WMNs can be used to transmit vital information arising from the wireless body sensor network (WBSN) to a backbone network. The integration of WBSN and WMN technologies results in wireless sensor mesh network (WSMN) and this type of network can be utilized for remote health monitoring of patients. The battery-powered, memory-constrained sensors transmit the sensed information to their nearest mesh nodes and the mesh nodes, in turn, use multi-hop routing to transmit the information to the backbone network devices like PDA or the servers for health monitoring applications. The authors have investigated performance of such a WSMN for patient health monitoring applications, in terms of parameters like delay, and throughput under varying number of patients and doctors [17].

R. Mahajan et al, 2005 illustrated a mechanism named CATCH, which consists of two modules: (i) anonymous challenge message (ACM), and (ii) anonymous neighbor verification (ANV). In the security scheme, first an ACM message from an unknown sender is sent to all its neighbors. As the sender is unknown, all the nodes further broadcast the ACM message.In the ANV phase, a tester node sends cryptographic hash of a random token for rebroadcast and also records other hashes sent by other nodes. The tester node releases the secret token to another node which successfully authenticates itself [18].

S. Buchegger et al, 2002 proposed the CONFIDANT protocol that is based on selective altruism and utilitarianism. It is distributed, symmetric reputation model that uses both first-hand and second-hand information for computation of reputation values. It uses dynamic source routing (DSR) protocol for routing and assume that promiscuous mode of operation is possible. The misbehaving nodes are punished by isolating them from accessing the network resources [19].

Sergio Marti at al, 2000 first proposed the idea of watchdog monitoring mechanism to monitor neighbors. The authors have also proposed a scheme named path rater to avoid misbehaving nodes in routing [20].

Sukla Banerjee, 2008 proposed a mechanism to detect and remove the black hole and gray hole attacks. This technique is capable of cooperating malicious nodes which drop a significant fraction of packets in AODV protocol. In this technique, each node can locally maintain its own table of black listed nodes whenever it tries to send data to any destination node and it can also aware the network about the black listed nodes [21].

Sheenu Sharma et al, 2009 described the simulation of black hole attack in mobile ad-hoc networks [22].

T. Repantis et al, 2006 has proposed a decentralized trust management middleware for ad hoc, peer-to-peer networks based on reputation. The reputation information of each peer is stored in its neighborhood and piggybacked on its replies. Tseng et al. have applied techniques based on finite state machines to detect misbehaving nodes in AODV routing protocol. The approach involves monitoring nodes that cooperate with each other and aggregate their observations at different locations in the network [23].

Y.L Sun et al, 2006 have presented trust as a measure of uncertainty. Using theory of entropy, the authors have developed a few techniques to compute trust values from certain observation. In addition, trust models – entropy-based and probability-based are presented to solve the concatenation and multi-path trust propagation problems in a MANET [24].

Yu Cheng et al, 2009 proposed a practical algorithm channel aware detection (CAD) to detect and isolate the selective forwarding attackers in the area of multi hop networks such as WMNs. CAD mainly adopts two strategies for detection: hop-by-hop loss observation by downstream nodes and traffic monitoring by upstream nodes [25].

Results and Analysis

Path protocol is obtained…………………

when received by the destination the time is calculated and thus...

distance is obtained...

After optimization when received by the destination the time is calculated once again and thus...

Path Protocol is obtained..

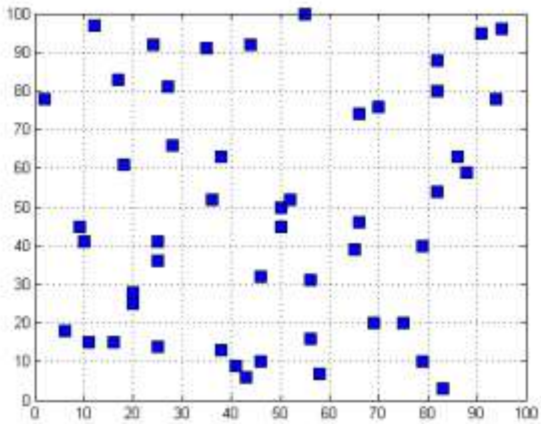
Distance Algorithm

```
clc;
clear all;
Max1=rand(1,1);
Max=10;
Max=uint8(Max1*100);
if(Max>50)
   Max=50;
end
if(Max<10)
   Max=10;
end
disp 'Max='
Max;
for(i=1:1:Max)
n(i,:)=randint(1,2,[2 100])
end
%n(2,:)=randint(1,2,[2 100])
%n(3,:)=randint(1,2,[2 100])
%n(4,:)=randint(1,2,[2 100])
%n(5,:)=randint(1,2,[2 100])
for i=1:1:Max
%stem( n(i,1),n(i,2))
plot( n(i,1), n(i,2),'--rs','LineWidth',1,...
            'MarkerEdgeColor','k',...
            'MarkerFaceColor','b',...
            'MarkerSize',10,...
            'Tag','hi')
hold on;
end
grid on;
hold on;
% generate RREQ
RREQ.Src=1
RREQ.Dst=5
```

```
%%%%%%%% all the nodes generate a hello packet put the start time
```

```
Max=
n =
   18   61
n =
   18   61
   28   66
n =
   18   61
   28   66
   70   76
…
…
…
n =
   18   61
   28   66
   70   76
   46   10
   24   92
   17   83
   55  100
    9   45
   12   97
    2   78
   82   88
   10   41
   27   81
   44   92
   20   28
   16   15
   88   59
   56   16
   86   63
   36   52
   41    9
   25   14
   20   25
   43    6
   91   95
   50   50
   35   91
   38   13
   79   40
   25   41
```

```
    11    15
    95    96
    58     7
    25    36
    83     3
     6    18
    66    74
    66    46
    56    31
    75    20
    69    20
    38    63
    79    10
    94    78
    50    45
    46    32
    52    52
    82    80
    65    39
    82    54
RREQ =
    Src: 1
RREQ =
    Src: 1
    Dst: 5
```



Path Algorithm

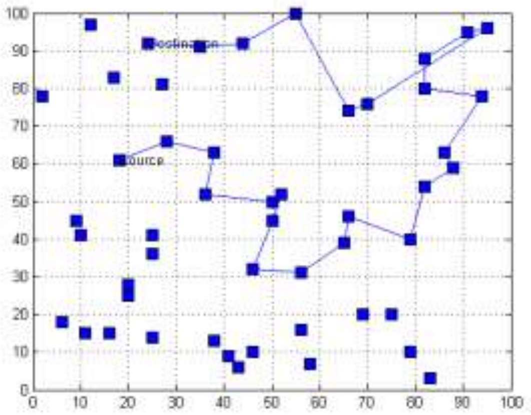
```
xs=0
ys=0
for i=1:1:Max
  for j=1:1:Max
    if(i==j)
    d(i,j)=0
    else
       xs=(n(i,1)-n(j,1))*(n(i,1)-n(j,1))
       ys=(n(i,2)-n(j,2))*(n(i,2)-n(j,2))
       d(i,j)=sqrt(xs+ys)
     end

   end
 end
 %%%%%%%%%%%%%%%%%%%%%%%%%
 path=RREQ.Src;
 current= RREQ.Src;
 INF=999999999999999
 small=INF
 tmp=0;
 errorcount=0;
 dataloss=0;
 newdataloss=0;
 while current~=RREQ.Dst

   for i=1:1:Max
     if current~=i
       if( d(current,i)<small)
        k=ismember(path,i);
        k=find(k);
        if(k)
          disp 'hi'
        else
        small=d(current,i)
        tmp=i;
        end
       end
     end
   end
   current=tmp;
   path=[path current]
   small=INF
   errorcount=errorcount+1
end
 disp 'loop ends'
 path

 sz=size(path)
 sz=sz(:,2)
 x1=n(path(1),1)
 rows=x1
   x2=n(path(1),2)
  col=x2
```

```
for i=2:1:sz
   x1=n(path(i),1)
rows=[rows  ;x1]
   x2=n(path(i),2)
   col=[col;x2]
end
x=[rows col]
hold on
%set(gca,'Visible','off')
str1(1) = {'Destination'};
str2(1) = {'Source'};
text(rows(1),col(1),str2)
text(rows(errorcount+1),col(errorcount+1),str1)
for l=1:1:errorcount
  % plot(X1,Y1,...,Xn,Yn)
   plot([rows(l) rows(l+1)],[col(l) col(l+1)])
   %hold on
   pause(0.5)
     dataloss=dataloss+rand(1,1)
     disp 'dataloss'
     dataloss;
end
 pause(2)
 %plot(x(:,1),x(:,2))%ploting a path between nodes
 %set(gca, 'ColorOrder', 'red');
hold all;
%%%%%%%% Network is connected and data loss is calculated
```

```
xs =
    0
ys =
    0
d =
    0
xs =
  100
ys =
   25
d =
         0   11.1803
xs =
        2704
ys =
  225
d =
         0   11.1803   54.1202
```

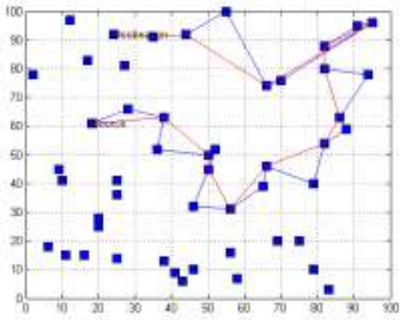
```
xs =
   784
ys =
        2601
d =
         0   11.1803   54.1202   58.1808
xs =
    36
ys =
   961
d =
  Columns 1 through 4
         0   11.1803   54.1202   58.1808
  Column 5
   31.5753
xs =
     1
ys =
   484
d =
  Columns 1 through 4
         0   11.1803   54.1202   58.1808
  Columns 5 through 6
   31.5753   22.0227
xs =
        1369
ys =
        1521
d =
  Columns 1 through 4
         0   11.1803   54.1202   58.1808
  Columns 5 through 7
   31.5753   22.0227   53.7587
…
…
…

xs =

   144

ys =

        1849
```

```
d =

  Columns 1 through 4

        0   11.1803   54.1202   58.1808

  Columns 5 through 8

   31.5753   22.0227   53.7587   18.3576

  Columns 9 through 12

   36.4966   23.3452   69.4622   21.5407

  Columns 13 through 16

   21.9317   40.4599   33.0606   46.0435

  Columns 17 through 20

   70.0286   58.8982   68.0294   20.1246

  Columns 21 through 24

   56.8595   47.5184   36.0555   60.4152

  Columns 25 through 28

   80.5295   33.8378   34.4819   52.0000

  Columns 29 through 32

   64.5136   21.1896   46.5296   84.5813

  Columns 33 through 36

   67.2012   25.9615   87.1149   44.6430

xs =

        2304

ys =

   169
```



```
disp 'Reducing path and data loss'
 l=1;
 disp ' dataloss in after optimizing network ='
 newdataloss;
 while l<=errorcount
     newdataloss=newdataloss+rand(1,1)
     display 'dataloss now='
     newdataloss;
     pause(0.4)
    if(l<errorcount)
         if(sqrt((((rows(l+2)-rows(l))*(rows(l+2)-rows(l)))+((col(l+2)-col(l))*(col(l+2)-col(l))))<2*sqrt(((rows(l+1)-rows(l))*(rows(l+1)-rows(l)))+((col(l+1)-col(l))*(col(l+1)-col(l)))))
 plot([rows(l) rows(l+2)],[col(l) col(l+2)],'Color','red')
             l=l+2;
         else
             plot([rows(l) rows(l+1)],[col(l) col(l+1)],'Color','red')
           l=l+1;
          end
         else
             plot([rows(l) rows(l+1)],[col(l) col(l+1)],'Color','red')
             l=l+1;
          %hold on
         end
        end
         disp 'Data loss before reduction'
         dataloss
         disp ' Data loss after reduction'
         newdataloss
         pause(5);
```

```
Reducing path and data loss
 dataloss in after optimizing network =
newdataloss =
    0.4087
dataloss now=
newdataloss =
    1.0036
…
…
…
dataloss =
   11.7770
 Data loss after reduction
newdataloss =
    5.6155
```



Conclusion and Future Work

Conclusion Future Work

Client nodes are unable to get services from gateway nodes, hence network gets down. The Paper emphasis on the developing of a path protocol when the minimun possible packet dropp occurs in wireless mesh networks. Due to packet droping occurrences the network performance degrades. In the work, we have evaluated the Performance of WMN under packet dropping on the basis of their throughput and Data packet loss.

In the future directions, this work can be extended by using hundreds of nodes and we need to develop the Intrusion detection System (IDS) that also chooses the monitor by considering battery life parameter. It is important to consider congestion conditions of the nodes using information obtained from other layers before determining the nodes to be malicious. Also, detecting intrusions at different layers increases the information about the malicious nodes thus identifying these nodes more accurately.

References

[1]. X. Wang and A. O. Lim, "IEEE 802.11s wireless mesh networks: Framework and challenges," *Ad Hoc Netw.*, vol. 6, no. 6, pp. 970-984, 2008

[2]. G. R. Hertz, S. Max, E. Weiß, L. Berlemann, D. Denteneer, and S. Mangold, “Mesh Technology enabling Ubiquitous Wireless Networks,” in Proceedings of the 2nd Annual International Wireless Internet Conference (WICON ’06), Boston, MA, USA: ACM, Invited Paper, pp. 11, August, 2006.

[3]. Yan Zhang, Jun Zheng “Book Title:-Security in Wireless Mesh Networks”.

[4]. w.steven,jan kryus, kyeongsoo kim, juan carlos zuniga “802.11s tutorial overview of the amendment for wireless local area networking” in ieee802 plenary, dallas , November ,2006.

[5]. Akyildiz, I.F.; Xudong Wang “A Survey on Wireless Mesh Networks” in Communications Magazine, IEEE Volume 43, Issue 9, pp. S23 - S30, September 2005

[6]. www.meshdynamics.com/mesh-network-technology.html

[7]. A. Pirzada and C. McDonald, “Establishing trust in pure ad hoc networks”, in Proceedings of the 27th Australasian Conference on Computer Science, Vol. 26,pp. 181-199, 2004.

[8]. A. Patwardhan, F. Perich, A. Joshi, T. Finn, and Y.Yesha, “Querying in packs: trustworthy data management in ad hoc networks”, International Journal of Wireless Information Networks, Vol. 13, No. 4, pp. 263 – 274, October 2006.

[9]. C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, “A specification-based intrusion detection system for AODV”, in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 125-134, 2003.

[10]. G. Vigna et al., “An Intrustion Detection Tool for AODV-based Ad hoc Wireless Networks”, Annual Computer Security Applications Conf. (ACSAC 2004), Tucson, 2004, pp. 16–27

[11]. H. Yang, J. Shu, X. Meng, and S. Lu, “SCAN: self-organized network-layer security in mobile ad hoc networks,” IEEE Journal on Selected Areas in Communications, Vol 24, pp. 261-273, 2006.

[12]. J. S. Baras and T. Jiang, “Managing trust in self-organized mobile ad hoc networks”, in Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS ’05), Invited Talk in the Wireless and Mobile Security Workshop, February 2005,San Diego, California, USA.

[13]. J. Sen, M. G. Chandra, P. Balamuralidhar, S.G. Harihara, and H. Reddy, “A distributed protocol for detection of packet dropping attack in mobile ad hoc networks”, in Proceedings of the International Conference on Telecommunications (ICT’07), Paper ID: 74, Track: AdRouting and Protocol, Penang, Malaysia.

[14]. Jaydip Sen “An Efficient Algorithm for Detection of Selfish Packet Dropping Nodes in Wireless Mesh Networks”, International Journal of Computer Information Systems and Industrial Management Applications, ISSN 2150-7988 Volume 3 (2011) pp. 363-37.

[15]. Lee, M.J;Jianliang Zheng; Young-Bae Ko; Shreshtha,D.M” Emerging Standards for Wireless Mesh Technology”IEEE Wireless Communication, Vol 13,No. 2”,2006.

[16]. M. Conti, E. Gregori, and G. Maselli, “Reliable and efficient forwarding in MANETs,” Ad Hoc Networks Journal, Vol 4, No 3, pp. 398-415, 2006.

[17]. N. A. Benjamin and S. Sankaranarayanan,“Performance of wireless body sensor based mesh An Efficient Algorithm for detection of Selfish Packet Dropping Nodes in Wireless Mesh Networks 369 network for health application”, International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM), Vol 2, pp. 20 – 28,2010.

[18]. R. Mahajan, M. Rodrig, D. Wetherall, and John Zahorjan, “Sustaining cooperation in multihop wireless networks,” in Proceedings of the 2nd Conference on Symposium on Networked Systems Design and Implementation (NSDI’05), Vol 2, pp. 231-244, 2005.

[19]. S. Buchegger and J.-Y. L. Boudec, “Performance analysis of the CONFIDANT protocol: cooperation of nodes- fairness in dynamic ad-hoc networks,” in Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc’02), pp. 226-236, Lausanne, Switzerland, 2002.

[20]. S. Marti, T.J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom ’00),pp. 255 – 265, 2000.

[21]. Sukla Banerjee,”Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”,Proceedings of the World Congress on Engineering and Computer Science,WCECS 2008,October 22-24,2008, San Francisco,USA.

[22]. Sheenu Sharma, Roopam Gupta,”Simulation Study of Black hole Attack in Mobile Ad-hoc Networks”,Journal of Engineering Science and Technology,Vol 4 No.2 ,2009, 243-250

[23]. T. Repantis and V. Kalogeraki, “Decentralized trust management for ad hoc peer-to-peer network’s”, in Proceedings of the 4th International Workshop on Middleware for Pervasive and Ad Hoc Computing (MPAC ’06), p. 6, April 2006, Melbourne, Australia.

[24].Y.L. Sun, W. Yu, Z. Han, and K.J.R. Liu, “Information theoretic framework of trust modeling and evaluation for ad hoc networks”, IEEE Journal on Selected Areas in Communications, Vol. 24, pp. 305 – 317, 2006.

[25]. Yu Cheng,Devu Manikantan Shila and Tricha Anjali,”Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks”, Dept. of Electrical and Computer Engineering,Illinois Institute of Technology,Chicago,USA,2009.