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 emphasizes on the developing of a path protocol when the minimum possible packet drop occurs in wireless mesh networks. Due to packet dropping 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 portable computers, 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.
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 was inspired by statistical signature-based analysis of observed traffic. Sensors are placed on selected nodes for promiscuous sensing of radio channels. Each sensor has a 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. To establish a trust management scheme among the neighbors, authors have proposed a voting mechanism [12].

Jay dip, 2011 has proposed a mechanism that 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].

Jay dip 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 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 which 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 et 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

\[
\begin{align*}
\text{Max} &= \text{rand}(1,1) \\
\text{Max} &= 10 \\
\text{Max} &= \text{uint8}(\text{Max} \times 100) \\
\text{if} (\text{Max} > 50) \\
\quad \text{Max} &= 50 \\
\text{end} \\
\text{if} (\text{Max} < 10) \\
\quad \text{Max} &= 10 \\
\text{end} \\
\text{disp} '\text{Max}=\text{Max}' \\
\end{align*}
\]

\[
\begin{align*}
\text{Max} &= 945 \\
\text{for} (i = 1:1:\text{Max}) \\
\quad \text{n}(i,:) &= \text{randint}(1,2,[2 \ 100]) \\
\quad \text{end} \\
\text{plot} (\text{n}(i,1), \text{n}(i,2), \text{'--rs', 'LineWidth', 1},...) \\
\quad \text{'MarkerEdgeColor', 'k', ...} \\
\quad \text{'MarkerFaceColor', 'b', ...} \\
\quad \text{'MarkerSize', 10, ...} \\
\quad \text{'Tag', 'hi'}) \\
\text{hold on;} \\
\text{grid on;} \\
\text{hold on;} \\
\% \text{generate RREQ} \\
\text{RREQ.Src}=1 \\
\text{RREQ.Dst}=5 \\
\end{align*}
\]
Path Algorithm

```matlab
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=9999999999999999
small=INF
tmp=0;
errorcount=0;
dataloss=0;
newdataloader=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
```

```matlab
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 = 784
ys = 2601
d = 0 11.1803 54.1202 58.1808

Columns 1 through 4

xs = 36
ys = 961
d = 0 11.1803 54.1202 58.1808

Columns 1 through 4

xlabel('Columns 5 through 6

data = 31.5753

Columns 5 through 6

ys = 1369
d = 1521

Columns 1 through 4

xs = 0 11.1803 54.1202 58.1808

Columns 1 through 4

ys = 31.5753 22.0227

Columns 5 through 7

ys = 53.7587

...%

ys = 53.7587

...%

ys = 53.7587

...%

ys = 53.7587

...%

ys = 53.7587

...%

ys = 53.7587

...%

ys = 53.7587

...%
$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 34.4819 52.0000

$\text{xs} = 2304$
$\text{ys} = 169$

disp 'Reducing path and data loss'
l=1;
disp ' Data loss 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
disp 'Data loss after reduction'
dataloss
newdataloss
pause(5);
Reducing path and data loss
data loss in after optimizing network =
newdataloss = 0.4087
data loss now =
newdataloss = 1.0036
... ...
data loss = 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 minimum possible packet drop occurs in wireless mesh networks. Due to packet dropping 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. Weiβ, 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, kyeong soo kim, juan carlos zuniga “802.11s tutorial overview of the amendment for wireless local area networking” in ieeec802 plenary, dallas , November 2006.

[5]. Akylidiz, 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. Balasubramaniam, C. Ko, R. Limprasitiporn, 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 Intrusion 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. Hariharan, 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; Shrestha,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 (IJCSIM), 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. Giuliani, 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.