www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 7 (July 2013), Page No. 2221-2227

Detection Of Routing Misbehavior In Manet By Enhanced 2ack Scheme Using Dsr Protocol

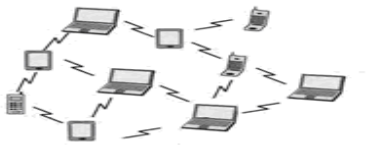
Mrs.K.Gomathy, Mr.P.Dineshkumar
Assistant Professor
Department of Computer Applications Dr.N.G.P Arts and Science College
Coimbatore-641 048
nharinisurya@gmail.com dinesh_july04@yahoo.com

ABSTRACT: *This paper focuses on routing misbehavior in MANET and method for detection of links which causes misbehavior. In MANET all the interested nodes to participate in routing should be fully co operative. But some nodes refuse to share the resources but get benefits for other nodes. Due to the node mobility, open structure and dynamic topology changes performance of network gets affected. The 2ACK scheme is used to detect such behavior by sending acknowledgement through opposite direction of the routing path. The proposed enhanced scheme using DSR protocol reduces the overhead of acknowledgement by 2ACK scheme.*

Keywords*:* Selfish node, Routing, Wireless Networks, DSR

1. INTRODUCTION

Mobile Ad-hoc networks (MANET) are self configuring and self-



Mobile Ad Hoc Networks

Organizing multi hop wireless Networks in MANET nodes (hosts) communicate with each other via wireless links either directly or relying on other nodes as routers. Every mobile device in a network is autonomous. Network nodes in MANET are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably.The mobile devices are free to move haphazardly and organize themselves arbitrarily. The Communication in MANET is take place by using multi-hop paths.

1.1. Classification of MANETS

MANET are two types closed and open. In a closed MANET, all mobile nodes cooperate with each other. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global

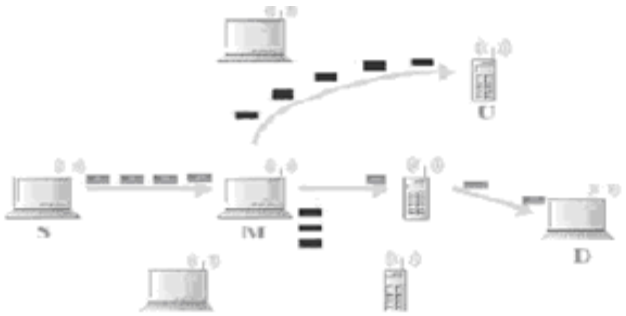
connectivity. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes, and their behavior is termed selfish or misbehavior. One of the major sources of energy consumption in mobile nodes of MANET is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

1.2.Routing schemes in MANETS

The use of conventional routing protocols in a dynamic network is not possible because they place a heavy burden on mobile computers and they present convergence characteristics that do not suit well enough the needs of dynamic networks. The network structure is mostly static in wired networks that are why link failure is not frequent.
Therefore, routes in MANET must be calculated much more frequently in order to have the same response level of wired networks. Various techniques have been proposed to prevent selfishness in MANET. These schemes can be broadly classified into two categories: *credit-based* schemes and *reputation-based* schemes.

2. Misbehavior nodes in MANETS

In MANET, routing misbehavior can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets.



Scenario for Packet Dropping and Misrouting

A node may misbehave due to selfish, overloaded, broken, or malicious an overloaded node lacks the buffer space, CPU cycles or available network bandwidth to forward packets. A selfish node is unwilling to spend CPU cycles, battery life or available network bandwidth to forward packets not directly , even though it expects others to forward packets behalf of its. A malicious node creates a denial of service (DOS) attack by dropping packets. A broken node might have a software problem which prevents it from forwarding packets. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called *selfish* or *misbehaving* nodes, and their behavior is termed *selfishness* or *misbehavior*.

One of the major sources of energy consumption in mobile nodes of MANET is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy. Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANET. Two techniques were introduced, namely *watchdog* and *path rater*, to detect and mitigate the effects of the routing misbehavior, respectively.

Various techniques have been proposed to prevent selfishness in MANET. Some of the related works are as follows. The work given in [6] explains detection of malicious nodes by the destination node, isolation of

malicious nodes by discarding the path and prevention data packets by using dispersion techniques. The work given in [7] describes the performance degradation caused by selfish (misbehaving) nodes in MANET. They have proposed and evaluated a technique, termed 2ACK to detect and mitigate the effect of such routing misbehavior.

3. RELATED WORK

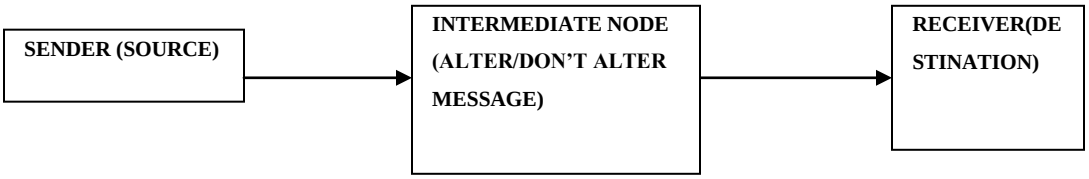
3.1 2ACK system

The system is used to detect the misbehavior routing using 2ACK and also check the confidentiality of the data message in MANET circumstances. Here, we used a scheme called 2ACK scheme, where the destination node of the next hop link will send back a 2 hop acknowledgement called 2ACK to indicate that the data packet has been received successfully. 2ACK do the following things.

If the 2ACK time is less than the wait time and the original message contents are not altered at the intermediate node then, a message is given to sender that the link is working properly.

If the 2ACK time is more than the wait time and the original message contents are not altered at the intermediate node, then a message is given to sender that the link is misbehaving.

At destination, a hash code will be generated and compared with the sender's hash code to check the confidentiality of message. Hence, if the link is misbehaving, sender to transmit messages will not use it in future and loss of packets can be avoided.



SYSTEM MODEL

The various modules in the system model are as follows:

Module 1(Sender Module)

The task of this module is to read the message and then divide the message into number of packets and send them to receiver through intermediate node. After sending the packets pktcnt (is incremented by 1.Wait time and 2ACK are compared. If 2ACK time is less than the wait time pktmiss is incremented by 1. The ratio of pktmiss and pktcnt is compared with (Threshold Ratio) TRmiss. If it is less than TRmiss then routing works properly otherwise misbehaving.

Module 2(Intermediate Module)

The task of this module is receiving and forwarding the packets from sender to receiver and also the acknowledgement packets from receiver to sender.

Module 3 :(Receiver Module)

The task of this module is receiving the packets and performs the decoding. After that sends the acknowledgement packets through the intermediate mode.

3.2 Functioning of the enhanced 2ACK Scheme.

Three nodes have taken (N1, N2, N3) to illustrate the scheme. N1 as Source node, N2 as Intermediate node and N3 as Receiver node.

A. At node N1

while (true) do
• Read the destination address;
• Read the message;
• Find the length of the message.
pktmiss=0, pktcnt=0, WT=20 ms, d=0.2,
2ACK Time=Current Time (Acknowledgement ac-accepted time) – Start Time.
while (length > 48 bytes) do
Take out 48 message packet;
Length = length – 48;
Encode message using hash function;
Send message along with the hash key;
pktcnt;
Receive 2ACK packet;
if (2ACK time > WT) then
pktmiss++;
end
end
if (length < 48 bytes) then
Encode message using hash function;
Send message along with the hash key;
pktcnt++;
Receive 2ACK packet;
if (2ACK time > WT) then
pktmiss++;
end
end
end

B. At node N2

while (true) do
Read message from source N1
if (Alter) then
Add dummy bytes of characters;
Process it and forward to destination N3;
Receive 2ACK from N3 and send it to N1;
else if (Do not Alter) then
Process it and forward to destination N3;
Receive 2ACK from N3 and send it to N1;
end
end

C. At node N3

while (true) do
Read message from N2;
Take out destination name and hash code;
Decode the message;
Send 2ACK packet to N2;
End

D. At N1 and N3 parallel

while (true) do
if ((pktmiss/pktcnt)>d and (hash code of source msg) !
= (hash code of destination msg)) then
Link is misbehaving and the confidentiality
is lost;
end
if ((pktmiss/pktcnt)<d and (hash code of source msg) !
= (hash code of destination msg)) then
Link is working properly and the confidentiality
is lost;
end
if ((pktmiss/pktcnt)>d and (hash code of source msg)
= (hash code of destination msg)) then
Link is misbehaving;
end
if ((pktmiss/pktcnt)<d and (hash code of source msg)
= (hash code of destination msg)) then
Link is working properly;
end
end

4. PROPOSED WORK

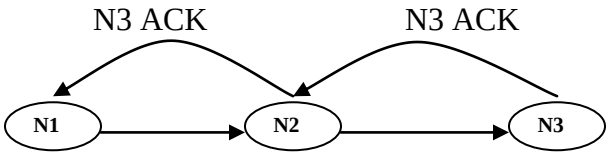
The enhanced 2 ACK scheme uses base of 2ACK scheme. The improved 2ACK scheme is used for detecting misbehaving link or node in triplet. In 2 ACK scheme algorithms, two nodes are needed to keep track of Acknowledge packets. . To reduce number of ACK and detecting which node is exactly misbehaved in triplet, we come towards improved 2 ACK scheme.

4.1 Working of Enhanced 2ACK Scheme.

The enhanced 2 ACK scheme uses base of 2ACK scheme. The improved 2ACK scheme is used for detecting misbehaving link or node in triplet. In 2 ACK scheme algorithms, two nodes are needed to keep track of Acknowledge packets. . To reduce number of ACK and detecting which node is exactly misbehaved in triplet, we come towards improved 2 ACK scheme.

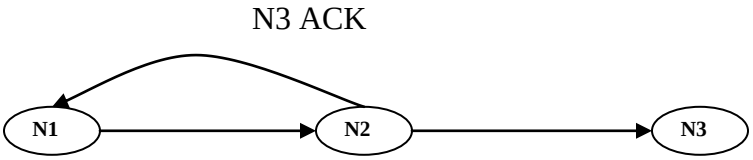
1. Best Case:

In this case, let assume that within the time tm, two consecutive nodes has to receive and send ACK packet. The packet will be sent by N1 to N2 and will be forwarded by N2 to N3. Then N3 will send ACK in reverse path (i.e. N3->N2->N1) Here N2 will not send its own ACK to N1



2. When N3 Misbehaved:

In the this case, if N3 is refusing to send acknowledgment packet N2 will wait for N3's ACK for given time tm and if it is not getting then N2 will send its own ACK to N1 which indicates N1 that N3 is misbehaving as N1 is getting ACK of N2 and not of N3.



3. Worst Case:

If N1 didn't get any acknowledgement after given time, which informs that N2 misbehaves.

4.2. Advantages of Enhanced 2ACK scheme

1. System Line load.

System has low Line Load when compared with 2 ACK scheme and reliability is more in the proposed system.

2. Partial Data forwarding

Enhanced 2ACK scheme not supports partial data forwarding. Hence, it reduces misbehavior of the nodes.

5. CONCLUSION

Mobile Ad Hoc Networks (MANET) has been an area for active research over the past few years. It is highly dependent on the cooperation of all its nodes to perform networking functions. This makes it highly vulnerable to selfish nodes. One such misbehavior is routing. When such misbehaving nodes participate in the

Route Discovery phase but refuse to forward the data packets, performance may be degraded and less reliable to the end user. The proposed system is a study of existing algorithm that detects misbehaving links in Mobile Ad Hoc Networks and suggests some enhancements for the existing system to have better performance and high reliability. The enhanced 2ACK scheme helps to detect misbehavior by a one hop acknowledgement.

5. REFERENCES

[1] L.M. Feeney and M. Nilsson. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment, Proc. IEEE INFOCOM, 2001:Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Volume 3 (2001), Pages. 1548-1557, Year of Publication: 2007

[2] D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) in 10th IEEE International Conference, 27-30 Aug 2002,Year of Publication :2002, ICON 2002.

[3] K. Balakrishnan, J. Deng, and P.K. Varshney. TWOACK:Preventing Selfishness in Mobile Ad Hoc Networks , Proc.IEEE Wireless Comm. and Networking Conf. WCNC '05),Mar. 2005,Volume 4,Pages 2137-2142, IEEE Press 2005,Yearof Publication:2005

[4] Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP '01), 2001.

[5] Elizabeth Royer and C-K Toh: A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. IEEE Personal Communications Magazine, pages 46-55, April 1999.

[6] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing mis-behavior in MANETs", *IEEE Trans. Mob. Comput.*, vol. 6, no. 5, pp. 536–550, 2007.

[7] S. Dhanalakshmi and, M. Rajaram, "A reliable and secure frame-work for detection and isolation of malicious nodes in MANET",*Int. J. Comp. Sci. Netw. Secur.*, vol. 8, no. 10, pp. 184–190,2008