World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 58-62
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Paramjeet Singh
Department of Computer Engineering Guru Kashi University, Talwandi Sabo Bathinda, Punjab, India

Jaspreet Singh
Department of Computer Engineering Guru Kashi University, Talwandi Sabo Bathinda, Punjab, India

Correspondence:
Paramjeet Singh
Department of Computer Engineering Guru Kashi University, Talwandi Sabo Bathinda, Punjab, India

Security management in network based on message priority and cap on hop-count

Paramjeet Singh, Jaspreet Singh

Abstract

MANET is the mobile ad-hoc network. It is infrastructure less network. There is no central controller which can control the network performance and secure the network from various kinds of attacks. There requires the special arrangement in the protocol so that the attacker node can be identified and removed. MANET is the network having higher vulnerability to various kinds of attacks. It is due to the higher vulnerability to various kinds of attacks. These various kinds of attacks will downgrade the performance of the network. To protect the system from these kinds of attacks priority of the packets is one of the better technique. Where those nodes will be given with higher priority who has to send the packets on to such route who has higher number of hop count. So that the network life time for the packet can be reduced. Because less time will reduces the probability of attacks. These types of schemes are highly successful as far as cost reduction is concerned. Performance has been compared on three parameters like End to End delay, Throughput, and Packet Delivery ratio. All the factors has improved to 14%, 75% and 11.19% respectively.

Keywords: MANET, AODV, Hop count, Priority.

Introduction

In an ideal static network, the nodes are immobile and interconnected to each other. Any node that wishes to send a message first determines a path to its destination, and the message is consequently sent through the determined path. But that is not how connections are in real life. The nodes are mobile, the contacts between nodes are occasional, the connections are intermittent, and the power of the nodes may turn off at times. This results in a need for *Delay Tolerant Networks (DTNs)*, where the message is stored in the node's buffer till the time it does not come across the destination node, or an intermediate node that could forward the message near to its destination. The main principal for routing message in Oppnets is *"Store, Carry and Forward"*. A node stores any message generated by it, or any incoming message in its buffer and keep carrying it, until it finds a suitable node to which it can forward the message or deliver it directly to the destination.

Opportunistic networks are considered as the subclass of DTNs and are quite different from MANETs. In MANETs, first a complete end-to-end path from the source to the destination is determined, following which the message is sent in the network. If the path breaks at any point of time during the message transfer, a new path is determined, after which the message transfer continues. On the other hand in an Oppnet, nodes dynamically decide the path/next hop for the message forwarding due to which MANET and Internet routing protocols fail to work in Oppnet scenarios.

Forwarding in mobile opportunistic networks is a hard problem because of two key challenges: the unpredictable mobility of the underlying nodes, and the resource constraints which include limited battery life, short contact durations and small buffers. For a mobile network operating under such constraints, the joint question of which messages to transmit and which messages to drop becomes important. As with a forwarding algorithm, every node should be able to decide which messages are transmitted and which messages are dropped based on the information the node has, all the while balancing the trade-offs that exist between success rate, delay and cost. Hence there is a need to develop and study prioritization schemes for messages such that nodes can forward high priority messages and drop low priority messages.

What is Priority

Message prioritization can be performed independent of the underlying forwarding algorithm. Such schemes include FIFO, LIFO and ttl-based algorithms.

While such schemes are easy to implement, the fact that they do not take into account network information can lead to poor performance and suboptimal use of the scarce resources. For the schemes which do use network information to make informed decisions there is a crucial question: on the one hand, one can assign high priorities to messages which are close to their intended destination. A node following such a scheme, will upon an encounter, drop the message farthest from its destination and transmit the message closest to its destination.

On the other hand, one can decide to assign high priorities to messages which are farthest away from their destination. Following such a scheme, the first message which will get dropped will be the message which is closest to its destination, and the first message which will get transmitted (after delivering the those messages destined to the encountered node) will be the message farthest from the destination. Clearly the notion of 'distance' to a destination is extremely important in such schemes that use network information.

Related Work

Deepak Kumar Sharma (2016) et al: This paper aims at improving the forwarding strategy in the Epidemic routing protocol for Oppnets, which currently makes use of First in First Out (FIFO) strategy to forward the data packets. In this work, Priority Based Forwarding for Epidemic Routing (PBFER) is presented that forwards the packets based on the priority of messages. Through simulations the performance of PBFER is evaluated and

compared with Epidemic routing protocol.

Vijay Erramilli (2013) et al**:** The main objective of this paper is to study different message

prioritization schemes using real measurements. Such schemes can be broadly divided into two categories - schemes which do not use any network information, and schemes which do. Examples of the former set of schemes include FIFO/LIFO etc.

sun-kyum kim (2016) et al: They propose a novel forwarding scheme that considers refined contact probability and betweenness centrality. In the proposed scheme, nodes with higher probabilities of contact with other nodes tend to gather together, while nodes with higher betweenness centralities compensate for intermittent connection disruptions among nodes in the network.

Sonam Kashyap(2012) et al: In case of wireless networks if the nodes are mobile then Manets (mobile ad-hoc networks) can be used for communication. But this is only possible when distance between the nodes is small, if the distance increases then it is not possible to communicate so to remove this limitation opportunistic networks were developed. With this network nodes can communicate irrespective of the distance and the type of node Opportunistic networking tries to remove the assumption of physical end to end connectivity while providing connectivity opportunities to pervasive devices when no direct access to the Internet is available.

Neelam Sharma(2016) et al**:** this paper is concerned with a crucial problem of MANET which is congestion control (CongClt). CongClt can be described as a mechanism used to control congestion (Cong) and keep the traffic below the capacity of the network. Many approaches have been proposed to overcome CongClt in Ethernet as well as in MANET. Controlling the Cong in MANET is quite difficult due to its fundamental characteristics. This discussion is centered on CongClt in MANET. In this work we discussed some of the CongClt techniques along with characteristics and working.

Algorithm

Step1 Layout the nodes in random way into the network of specific size.

Step2 Bind the nodes with Routing protocol.

Step3 Assume one node as source and one node as destination.

Step4 Identify the route from source to the destination.

Step5 Count the Number of Hops from source to the destination on determined route.

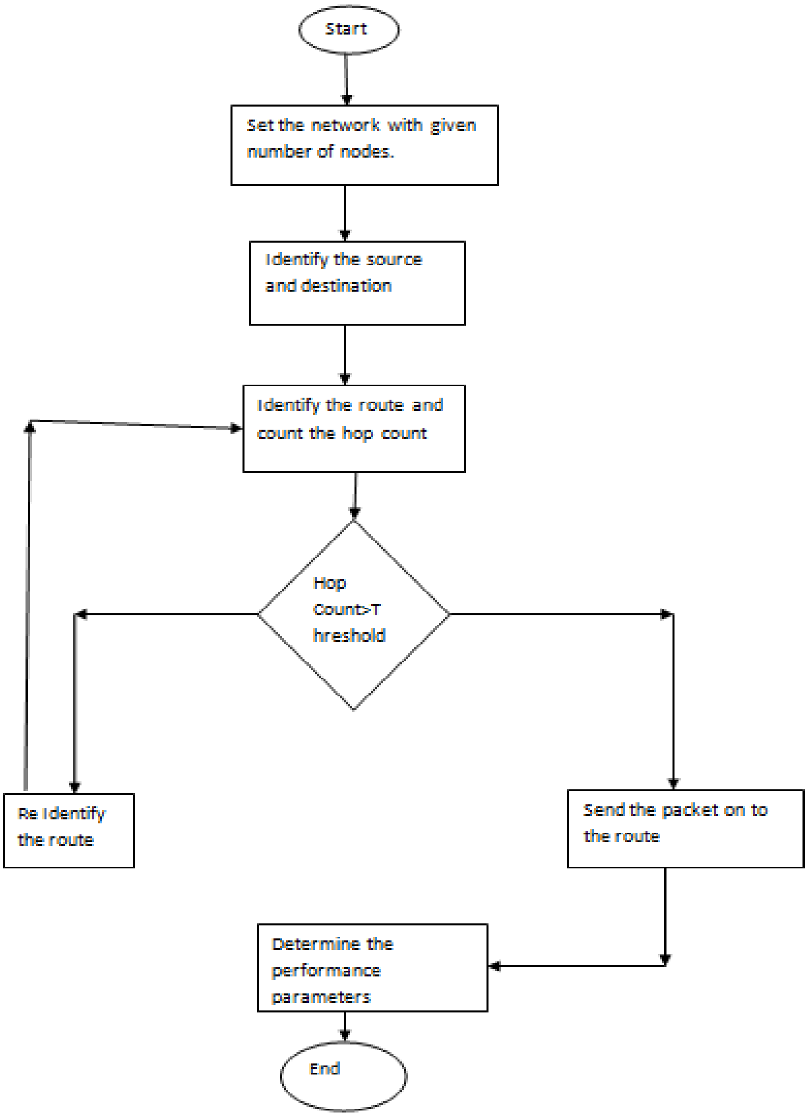
Step6 Check the hop count with threshold limit. If hop count is greater than the threshold goto step5.

Step7 else give the higher priority to the packets to be sent on determined route.

Step8 identify the performance parameter.

Step9 End

Flowchart


Start
Set the network with given number of nodes.
Identify the source and destination
Identify the route and count the hop count
Hop Count>T hreshold
Re Identify the route
Send the packet on to the route
Determine the performance parameters
End

Results and Discussions

Network Configuration

For setting the priority to the packets there requires network to configure. Various basic settings are being configured for showing the performance enhancement.

Parameters	Values
Number of Nodes	50
Protocol	AODV
Application	CBR,FTP
Link Layer Protocol	TCP,UDP
If Queue Length	50
Delay	2 sec.

Table 1.1

These basic settings are set before starts to build the network. These settings are performed to set network to take up that much load which will be applied in real life situation. So that whatever results will come out can be thought of as real life results.

Performance Parameters

There are various performance parameters are used which will be there to check the performance of the network. So that any network performance can be checked in comparison to other. These parameters results will be considered and represented in graphical way.

1. **End to End delay:** It is the total time taken that is start of communication time and end of the communication time. If there is any delay in between then end to end delay will be increased. Else the end to end delay will be reduced.

   End to End Delay=End Time-Start Time
2. **Throughput:** It is the amount of packets sent per unit interval of time successfully.

   Throughput=(sent packet-received packet)/total time
3. **Packet Delivery Ratio:** it is the measure of amount of packets delivered. It is the measure of packets sent, packet Received and how many packets dropped.

   PDR=(Total_Sent- droped)/Total_sent

Nam Simulator Figures

Node Placement

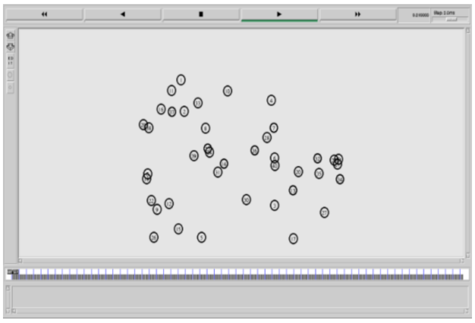


Fig. 2

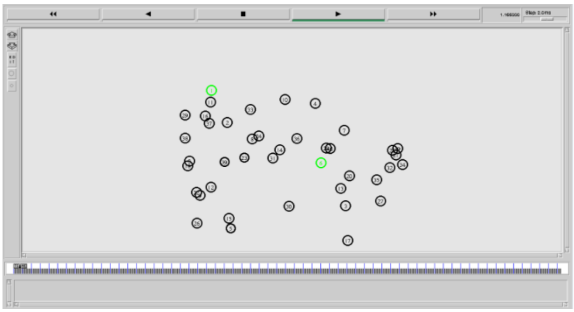
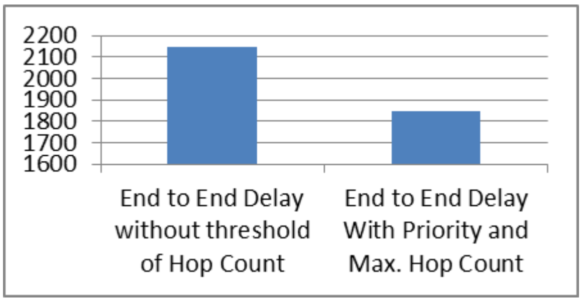


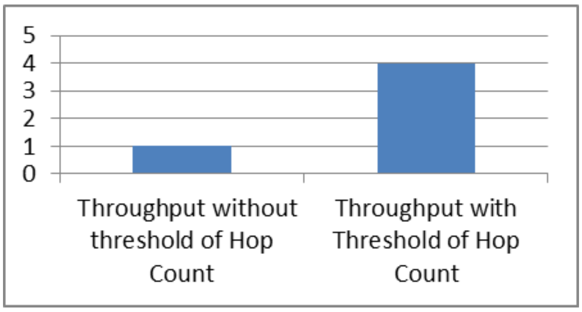
Figure 3

a. End To End Delay



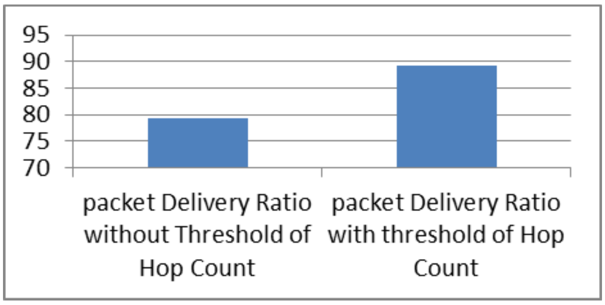
Graph 1

b. Throughput



Graph 2

c. Packet Delivery Ratio



Graph 3

d. Percentage Improvement

End To End Delay	14%
Throughput	75%
Packet Delivery Ratio	11.19%

Table 1.5

From the above table it is clear that the all the factors has improved. That means end to end delay, throughput, and packet Delivery Ratio has improved.

Conclusion and Future Work

MANET is the network having higher vulnerability to various kinds of attacks. It is due to the higher vulnerability to various kinds of attacks. These various kinds of attacks will downgrade the performance of the network. To protect the system from these kinds of attacks priority of the packets is one of the better technique. Where those nodes will be given with higher priority who has to send the packets on to such route who has higher number of hop count. So that the network life time for the packet can be reduced. Because less time will reduces the probability of attacks. These types of schemes are highly successful as far as cost reduction is concerned. Performance has been compared on three parameters like End to End delay, Throughput, and Packet Delivery ratio. All the factors has improved to 14%, 75% and 11.19% respectively. In future this type of scheme can be tested on to other proactive and hybrid protocols. So that this types of technique can be declared global best.

References

1. Deepak Kumar Sharma1, Sanjay K. Dhurandher1, Mohammad S. Obaidat2, Sahil Pruthi and Balqies Sadoun," A Priority Based Message Forwarding Scheme for Opportunistic Networks", 2016 IEEE
2. Vijay Erramilli, Mark Crovella, " Forwarding in Opportunistic Networks with Resource Constraints",2012.
3. SUN-KYUM KIM," Effective Forwarding Scheme for Opportunistic Networks Based on Refined Contact Probability and Betweenness Centrality", JOURNAL OF INFORMATION SCIENCE AND ENGINEERING(2016)
4. Sonam Kashyap1, Jasvir Singh2," Survey on Latest Routing Algorithms in Opportunistic Networks", International Journal of Science and Research (IJSR),2014
5. Yongxuan Lai, Guilin Li," PBQ: A Priority-Based Query Processing Algorithm in Opportunistic Wireless Sensor Network", Journal of Applied Science and Engineering, Vol. 17, No. 2, pp. 203_213 (2014)
6. Andrea Lupia, Floriano De Rango, "Energy Consumption Evaluation of SAODV with Trust Management Scheme under Gray-Hole Attacks", International Journal of Information Technology and Knowledge Management, Vol 2(2), pp. 545-548, 2015.
7. Haroun Benkaouha, "AFDAN: Accurate Failure Detection protocol for MANETs", University of Turku Dep. Information Technology, 2015.
8. Siddlingappagouda Biradar, "Enhancing the quality of service using MAODV protocol in MANET's", Swedish Defence Research Agency Command and Control System Sweden, 2015.
9. Prachatos MitraThe journal of Military Electronic & Computing, "Mobile Ad Hoc Networking Revamps Military Communications".
10. Sunil J. Soni, P.Kanungo "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2Simulator", Procedia Engineering Vol. 23, pp.229–234, 2015.
11. C .Perkins and E. Belding-Royer, "Ad-hoc On-Demand Distance Vector (AOVD) Routing", IETF RFC 3561, 2015.
12. Hongmei Deng, Wei Li, and Dharma P. Agrawal,

"Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzi ne, vol. 40, no. 10, October 2002.

13. Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) routing," Internet Draft, November 2002