International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Issues of Multi hop relaying in Opportunistic network

[1]Sandeepak Bhandari & [2]Er.Satish Arora
CT Institute of Technology & ResearchGreater Kailash, G.T Road, Maqsudan Jalandhar, www.ctgroup.in

Abstract-
A new network is invented or a class of delay tolerance network in which some device which is carried by the users in their daily life and can pass message when they get opportunity, hence network is called opportunistic network. Opportunistic network use the concept of relay to transmit data between source and destination. By relay means that use of intermediate nodes between source and destination for providing communication between them. As there is no fixed infrastructure or topology is present in this network. So there are various issues in this network namely Routing and Privacy. In this paper we studied the working and performance of opportunistic network with multi hop relaying technique. In muti hop relaying technique the two nodes communicate with the help of intermediate node where the distance between these two nodes greater than the range of these nodes. But there are several issue with these nodes like packet loss, throughput.

Keywords- Introduction; Opportunistic network; Related Work; Research Methodology and Results

I. INTRODUCTION

A new network is invented or a class of delay tolerance network in which some device which is carried by the users in their daily life and can pass message when they get opportunity, hence network is called opportunistic network. It is formed by the nodes having capability to support this network, the nodes are connected wirelessly. The nodes are mobile or stable so no fixed infrastructure is present in this network and this network can work even in disconnected environment. Every node have a finite range in which they can communicate or can forward the message. A node can forward a message only when any other node comes in his range. The nodes have to store the message until another node is not come in his range. All nodes have to work in the store-carry-forward manner in this network. In this network, group of intermediate nodes help to send a message from source to destination. Nodes have no predefine topology of the network, two node might be or never connected, no fix route between two node is use to send message. Network topology may change due to activation and deactivation of the node. If destination node is not in the range of source node then it passes the message to the nearest node in its range and so on node by node closer to the destination. This network is very easy to implement in any situation or any environment like war and disaster prone areas where communication is for short time and needs very quickly. In such environment we have less time to implement the network topology or to make an infrastructure. At such a location or time this network is very useful to facilitate the user to communicate.

Working of Opportunistic Network

In opportunistic network, communication opportunities (contacts) are intermittent, so an end-to-end path between the source and the destination may never exist. One of the possible solutions to resolve the above issues is to exploits node mobility and local forwarding in order to transfer data. Data can be stored and carried by taking advantage of node mobility and then forwarded during opportunistic contacts. The following three steps show working of opportunistic network.

1. Message forwarding to an intermediate node by source

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

2. Message forwarding between intermediate nodes
3. Message forwarding between intermediate and destination

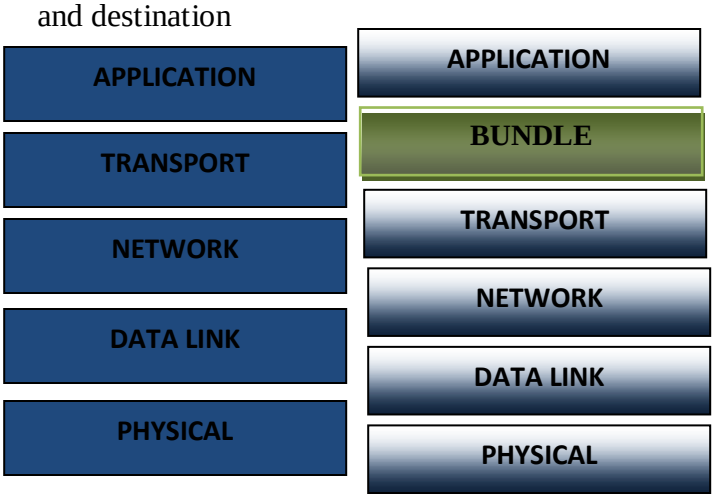

Fig 1: Original five- layer TCP/IP stack
Fig 2:TCP/IP stack with Bundle layer

II.RELATED WORK

Jia Jianbin, et. al(2013) studied that hop count is an important parameter for routing strategies in wirelesss network. Particularly in the opportunistic networks, due to the intermittent connectivity between mobile nodes, it imposes great impact on the delivery performance. In the previous works there are papers either claimed that two-hop is enough, or claimed that more hops increase the delivery delay. All of those conclusions are well justified under their specific assumptions and conditions, but the factors arising towards multi-hop benefit have not be well investigated Chaintreau et.al(2006), studied the transfer opportunities between mobile devices carried by humans by analyzing several user traces. They found that the distribution of the inter-contact time of a pair of devices, i.e., the time gap between two successive contacts, follows approximately a power law distribution. Also present a preliminary analysis of 2 user traces with a focus on statistical properties like node degree distribution and topological properties like cluster occurrences.

Papaj Jan et. al (2012) discussed to find that the opportunistic network as a most challenging evolution of MANETs. Opportunistic network provide possibility to exchange message between nodes even in disconnected mode by forwarding the message packet to the neighbor node by the selection algorithm of opportunistic network, and message is move closer to the destination node. They introduce the basic security issues, described and there are displayed basic security mechanism and algorithms, they find that a strong and robust security solution is needed to transmission of data between source and destination node. In this article they present the security key issues and challenges. They find opportunistic as the promising technology for the next generation mobile network, if in future someone found a robust and secure routing technique in this network. But this is a difficult task due to absence of knowledge about the network topology.

L. Lilien et. al(2006)introduced a new paradigm and a new technology, which we call opportunistic networks. An opportunistic network grows from its seed—the original set of nodes employed together at the time of the initial oppnet deployment. The seed grows into a larger network by extending invitations to join the oppnet to foreign devices, node clusters, or networks that it is able to contact. A new node that becomes a full-fledged member, or helper, may be allowed to invite external nodes. All helpers collaborate on realizing the goals of the oppnet. They can be employed to execute different kinds of tasks, even though in general they were not designed to become elements of the oppnet that invited them. Oppnets, as an epitome of pervasive computing, are subject to significant privacy and security challenges, inherent to all pervasive systems. To the best of our knowledge, we are the first to define and investigate opportunistic networks.

L. Pelusi et.al(2006)discussed an overview of opportunistic message forwarding and routing techniques that is use by a user to communicate with other user of the same network. Opportunistic message forwarding supposes an end to end communication between to or more

communication pattern but without any fixed infrastructure or direct path between the end points. In such situations routing is very difficult, in opportunistic network data forwarding and message forwarding is the same thing. In this article they also demonstrate the routing approaches use in this network.

D. Nain et.al(2006)studied about the Mobile Relay Protocol.MRP has been conceived to integrate pre-existing ad hoc routing protocols andmanage message forwarding when no route towards the destination node of a message is found and the application that has generated the message can tolerate some form of extra delay.

III. RESEARCH METHODOLOGY

In Opportunistic network no fixed infrastructure is present and the message is forward through many intermediate nodes, there may be a selfish node which is not interesting to forward the message to a particular destination, or the user doesn't want to show his identity when want to communicate or send message to a particular destination, then it is risk to the privacy of user or the packet dropped by the selfish node.

Also the content of message is also access by the intermediate nodes, so there is a problem that how to encrypt the message and share a key between source and destination without showing it to intermediate nodes.

1. No Fixed Infrastructure is present.
2. Message is passes through many intermediate nodes.
3. Intermediate nodes may or may not forward the message i.e. risk of loss of packet.
4. Message should be kept secure from intermediate nodes.

IV. SIMULATION ENVIRONMENT

The proposed network and the privacy based methodology are implemented in NS 2.35. NS (network simulator) environment is one such facility which lends a high performance language for technical computing. It uses the standard of network and show like actual outputs.

Parameter	**Value**
Terrain Area	800 m x 800 m
Simulation Time	6 s
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV
Data Payload	1000Bytes/Packet
Number of Nodes	13
Number of Sources	1

Table 1: Simulation Parameters

V. SIMULATION SETUP

We consider some cases to show the problem.

Case 1: Communication is successful like normal scenarios. Every node do his work properly, no intermediate node wishes to stop the communication. Here the only concern is to protect the data confidentiality by using a efficient encryption scheme.

Case 2: In this network the intermediate node have a problem to send or forward a message of a particular destination or the message from a particular sender.

CASE 1:

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

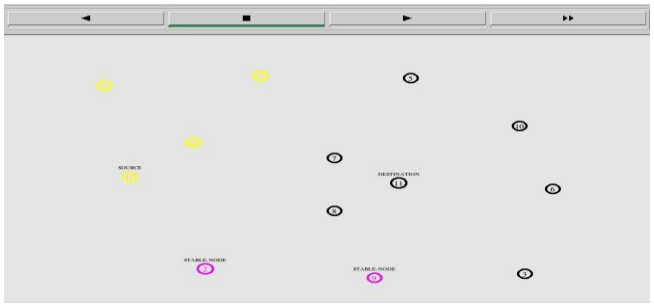

Figure 3: Network design for normal scenario (without any concern).

Network is divided into two clusters (presented by color). Node 2 is the stable node of cluster having yellow color and Node 9 is the stable node of cluster having black color, both stable nodes is presented by pink color.

Node4 (source) from cluster wants to communicate with node 11 (destination) of another cluster.

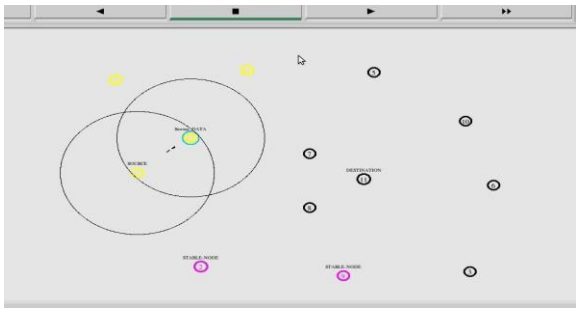

Figure 4: Sharing message with mobile node (intermediate node).

Now source node forward the message to Nodeβ (mobile node in network) when both are in communication range.

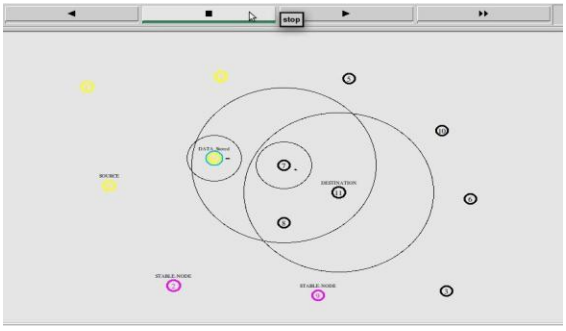

Figure 5: Message forward to the destination.

Nodeβ change its location and come in the communication range of node 7, hence forward the message to node7, and node7 pass to the destination (both are in communication range).

As above figures shows that message is successfully reaches at destination, this is because no intermediate node interested to stop the communication between source and destination. The nodes who want to do this called selfish node. Selfish node drop the packet of a particular destination to whom he don't wishes to forward.

CASE 2:

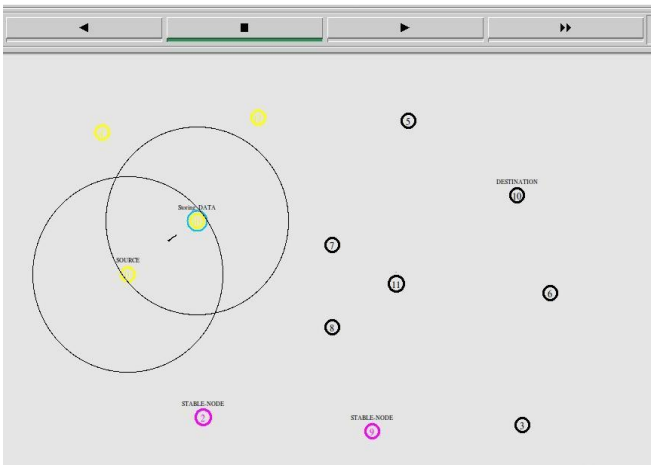

Figure 6: Message forward to a mobile node (intermediate selfish node).

In this network the source is same (node 4) but the destination is change. As like the previous case Node4 forward the message to Nodeβ, as both are in communication range. If user identity is shown to all, then it causes many problems. Some users do not want to explore their identity while using the network. In this network the message is only forward when both nodes are in the communication range, so when a node forward a message packet then it location is also identify such that the Node x and Node y meets at the location at a particular time.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

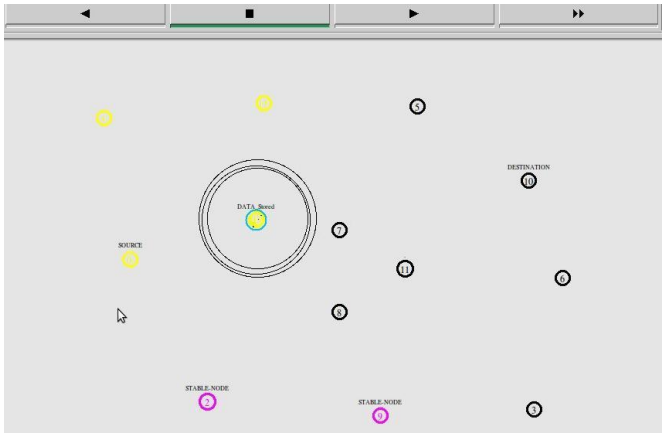

Figure 7: Destination information analyze by selfish node.

Node β drops the packet of the destination Node10 hence communication is not complete between source and destination

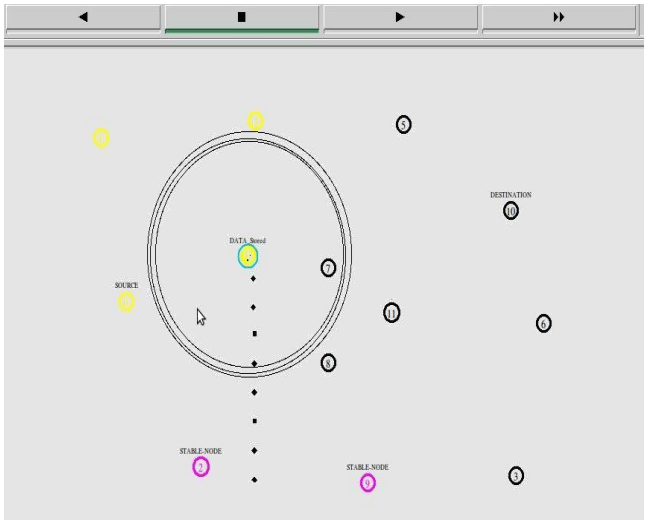

Figure 8: Packet drop by selfish node.

Node β drops the packet of the destination Node10 hence communication is not complete between source and destinati

VI. SIMULATION RESULTS

1.PACKETLOSS

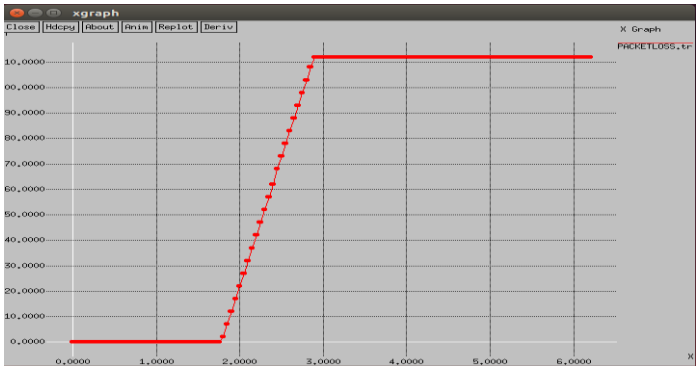

Fig 9 PacketLoss

2.THROUGHPUT

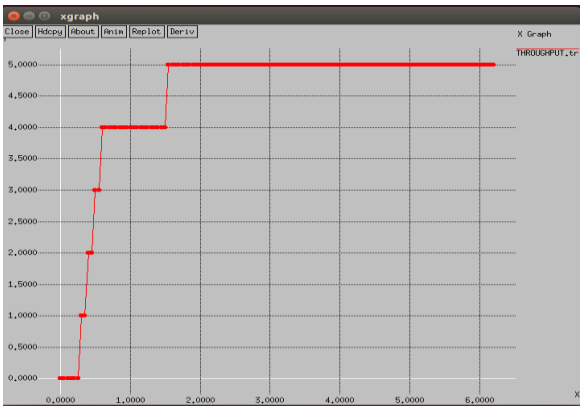

Fig 10 Throughput

4. Delay

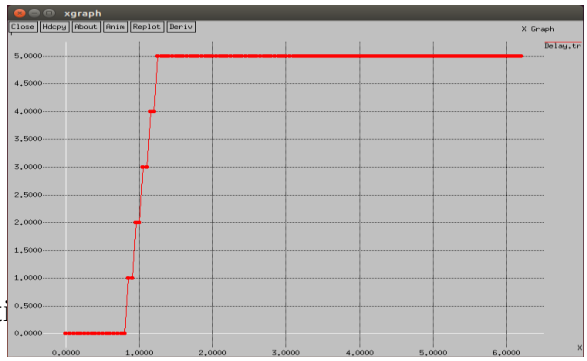

Fig 11 Delay

VII. CONCLUSION

Opportunistic network is suitable for providing communication where end to end path may never exist. Opportunistic network follows the store-carry-forward mechanism i.e a node get the data

from other data which is in the range of that node and store and carry it until ,it find another node to which it can forward it,i.e Opportunistic network is entirely depend upon intermediate node for providing communication between two nodes ,it is known as Realy, but there are several issues related with intermediate node like Packet loss, Integrity of data etc, which should be handled to provide secure communication

VI. REFERENCES

[1] Jia Jianbin, Chen Yingwen, Xu Ming, Xia Geming, and Xiao Xiaoqiang(2013), "Towards the Benefit of Multi-Hop Relaying in Opportunistic Networking",IEEE Infocom on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing.

[2] Chaintreau, Pan Hui, Jon Crowcroft, Christophe Diot, Richard Gass, and James Scott(2006)," Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms",IEEE Infocom.

[3] PapajJan, DobosEubomir and Cumar(2012),"Opportunistic Networks and Security"Journal of Electrical and Electronics Engineering, vol. 5,no.1..

[4] L. Lilien, Z. H. Kamal, V. Bhuse, and A. Gupta(2006),"The Concept of Opportunistic Network and their Research Challenges in Privacy and Security","Mobile and Wireless Network Security and Privacy", Book Chapter, pp. 85-117.

[5] L. Pelusi, A. Passarella, and M. Conti(2006),"Opportunistic Networking: data forwarding in disconnected mobile ad hoc networks", IEEE Communications Magazine, vol. 44, no.11.

[6] D. Nain, N. Petigara, and H. Balakrishnan(2003), "Integrated Routing and Storage for Messaging Applications in Mobile Ad Hoc Networks", in Proceedings of WiOpt, Autiplis, France.

[7] S. Jain, K. Fall and R. Patra(2004),"Routing in a delay tolerant network", Proceedings of the ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp.145–158, New York, NY: ACM.

[8] W. Li and A. Joshi,(2010)," Security Issues in Mobile Ad Hoc Networks- A Survey" Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.

[9] Xingguang Xie, Yong Zhang, Chao Dai, Mei Song(2011),"Social relationship enhance predicable routing in opportunistic network", Seventh International Conference on Mobile Ad-hoc and Sensor Networks.

[10] L. Dora, T. Holczer(2010),"Hide-and-Lie: Enhancing Application-level Privacy in Opportunistic Networks" Proceedings of the Second International Workshop on MobileOpportunistic Networking (MobiOpp). In ACM, pp.135-142.

[11] Fall(2003), "A delay-tolerant network architecture for challenged internets", in the Proceedings of the ACM Conference on Applications, Technologies Architectures, and Protocols for Computer Communications, pp.27–34.