MPRI-JPAS | INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE
VOL. 10 NO.9 DEC-2019 ISSN: 1660-5332

IMPROVED INTEGRATED ROUTING PROTOCOL FOR OPPORTUNISTIC NETWORK USING A HYBRID CONGESTION CONTROL MECHANISM.

B. YAHAYA, Z. M. ABUBAKAR, M. O. MOMOH, Y. IBRAHIM
Department of Computer Engineering, Ahmadu Bello University Zaria, Nigeria.

Abstract

In an opportunistic network, information about the context in which users communicate is not available, as there is no dedicated complete path from a source to a destination. This make the design of an efficient routing protocol for an opportunistic network difficult. This research is aimed at the development of an improved integrated routing protocol for the opportunistic network by managing congestion. A hybrid congestion control strategy was developed which combines the various buffer management strategies (use acknowledgment, buffer size advisement, data centric method and duplication avoidance) in the integrated routing protocol. Simulation was carried out using the opportunistic network environment (ONE) simulator. The hybrid congestion control strategy was seen to have outperformed the use of acknowledgment, buffer size advisement, data centric method and duplication avoidance by 58%, 61%, 58%, 52% respectively in terms or delivery probability. In terms of packet loss, the hybrid congestion control strategy outperformed the use acknowledgment, buffer size advisement, data centric method and duplication avoidance by 61%, 11%, 13%, 11% respectively These results showed that proper management of congestion can significantly improve the performance of opportunistic network.

KEYWORDS:
Opportunistic network, buffer management, congestion control, integrated routing protocol.

Introduction

Traditionally, communication between two or more devices in a network use either wired or wireless technology. The wired network could be difficult to expand due to cost, environment, etc. the wireless network needed a centralized administration, constant power supply to serve its base station, and it is difficult to maintain. Both the wired and wireless technology are capitally intensive to build and scale up (Dinakar *et al.*, 2013).

The quest to address some of these issues brought the need for a decentralised autonomous system. The opportunistic network is an autonomous network that allows messages to be forwarded even if a direct link between the source and the destination does not exist. It operate in a delay tolerant manner with or without network infrastructure. It is self organising and easy to deploy. It has a flexible network topology and it has no fixed communation range (Kaur & Kaur, 2009; Verma & Srivastava, 2012; Yogi & Chinthala, 2014; Asgari *et al.*, 2013). Due to is aformmention characteristics, opportunistic network has gained ground in a number of applications (adhoc network for emargency services, coverage extension, tactical networks, etc.). The opportunistic network has been used to complement the wired and wireless network where the wired and wireless network are difficult to deploy. One of the major issue in opportunistic network has to do with routing . It is difficult to design an efficient routing protocol due its characteristics (flexible topology, lack of context information, heterogeity, storage constraint due to the nature of nodes used) (Kaur & Kaur, 2009; Verma & Srivastava, 2012; Huang *et al*., 2008; Shikfa *et al.*, 2010; Ristonovac, 2012). A number of work has been done in Literature to address routing issues in opportunistic network. Vahdat & Becker (2000) developed the epidemic routing protocol which is a context oblivious routing protocol. The epidemic routing protocol floods all messages over the network without using any routing information. This guarantees faster message delivery but generates network overhead which eventually congests the network due to storage constraints of nodes. Lindgren *et al.,* (2003) developed the Probablistic Routing Protocol using History of Encounter and Transitivity (PRoPHET) which learns automatically from previous communication history determined

by users' mobility pattern. PRoPHET uses these information (context information) to route messages in the future. PRoPHET was able to provide better congestion control, acceptable Quality of Service with lower overhead. Howerver, in the absence of context information, it provides higher over head which causes congestion and message delay (Pelusi *et al.,* 2006; Verma & Srivastava 2012). This still leaving congestion as a problem in opportunistic routing. The integrated routing protocol was developed to sum up the merits of the PRoPHET and the epidemic routing protocols. It is a hybrid routing protocol that uses the prophet when context information is available, and the epidemic roting protocol when context information is not available. It significantly outperformed both routing protocols in terms of higher message delivery and lower delay. It did not consider any congestion control strategy which would have improved its performance.

Silva, *et al.,* (2015) surveyed the processes of delay tolerant networks congestion control and organized a taxonomy that helped in mapping and comparing the existing DTN congestion control mechanism. They deduced that "there is no universal congestion control mechanism that will be applicable to all DTN scenarios and applications". In the work of Pan *et al.,* (2013), an integrated buffer management strategy was developed with a view to reducing congestion, but a lower higher overhead and delivery ratio was recorded as compared to the spray-and-wait model. Ip *et al.,* (2007) presented a buffer management strategy to avoid head-of-line blocking in the first-in-first-out case and showed that the proposed strategy reduced the degradation of average delivery delay performance.

In our work (Yahaya *et al*., 2015), some congestion control strategies were applied to the opportunistic network, where a comparative study of congestion control strategies was carried out. It was shown that better performance in terms of delivery probability and lower packet loss was obtained. These congestion control strategies reduced congestion better. This paper is an extended version of the previous publication (Yahaya *et al*., 2015), with the aim of developing a better congestion strategy in the integrated routing protocol by combining the various congestion control strategies as one hybrid congestion control strategy.

The rest of the paper is organized as: Section 2 presents an overview of the integrated routing protocol and congestion in opportunistic network. Section 3 describes the system architecture for the hybrid congestion control mechanism. Implementation details are presented in Section 4, while the results and performance are evaluated in section 5. Section 6 concludes the paper.

CONCEPT OVERVIEW

Integrated Routing Protocol

Routing protocols decide which node to forward data to based-on specific network characteristic they observe. Routing performance improves when more knowledge about the expected topology is used. However, this knowledge is not readily available in opportunistic networks such that trade-off must be made between performance and knowledge requirement (Kaur & Kaur, 2009; Pelusi, *et al.*, 2006; Verma & Srivastava, 2012).The two main routing techniques for opportunistic networks as presented in literatures (Kaur & Kaur, 2009; Orozco, *et al.*2003; Verma & Srivastava, 2012) are:

i. The 'Epidemic' (context-oblivious) routing.
ii. The 'Prophet' (context-aware) routing

The epidemic routing protocol provides a final delivery of messages to random destinations with minimal assumption of topology and connectivity of the network (Pelusi *et al.*, 2006). The heuristic behind this policy is that, the message should be broadcasted all over the network (flooding) expecting that it will eventually reach its final destination. This technique works well in a highly mobile network where the contact opportunities needed for data diffusion are common. They limit message delay but consume resources (Pelusi *et al.*, 2006; Verma & Srivastava, 2012; Journi & Jorg, 2008).

Prophet maintains a delivery predictability metric at every node. (The delivery predictability metric refers to message delivery probability between two nodes) (Pelusi *et al.*, 2006). Hence, it is able to learn the past communication opportunities determined by users' mobility pattern and uses them efficiently in future to determine whether to forward a message to nodes it encounter or not. Whenever two nodes

come into communication range, the sending node compare it delivery predictability metric with the encountered node. If the encountered node has a higher delivery probability metric to the destination, the message is forwarded to it, otherwise the sending node keep the message to itself. The prophet provides congestion control, acceptable QoS with lower overhead. However, in the absence of context information, it provides high overheads and message delay (Pelusi *et al.*, 2006; Verma & Srivastava, 2012).

In some cases, it is not guaranteed that a node with a higher delivery probability will be discovered in reasonable time. Also, some nodes may be new in the network, implying that their context information is not spread in the network. As a result of these, the Integrated routing protocol was made to combine the features of the prophet and the epidemic routing protocol. It uses delivery predictability information when it is available and then uses dissemination-based routing when context information is not available.

Nodes need to know the contact probabilities to all other nodes in the network, every node maintains a probability metric. A node then updates its metric with that of other nodes if the other node has a more recent update time attribute so that the two nodes will have identical contact probability matrices after communication.

The metric is updated whenever a node meets with other nodes, so that nodes that often meet have a high message delivery probability. When node x meets node y, the delivery probability of node x for y is updated by (Verma & Srivastava, 2012):

$$P'_{xy} = P_{xy} + (1+P_{xy})\,P_0 \quad (1)$$

Where P_0 is an initial probability (P_0 ranges between 0 and 1), P'_{xy} is the current delivery probability of node x for y and P_{xy} is former delivery probability of node x for y.

When node x does not meet with node y for some predefined time, the delivery probability decreases by (Verma & Srivastava, 2012):

$$P'_{xy} = \gamma^k P_{xy} \quad (2)$$

Where γ is the aging factor ($\gamma < 1$), and k is the number of time units since the last update. When node x receives node y's delivery probabilities, node x may compute the transitive delivery probability through y to z by (Verma & Srivastava, 2012):

$$P'_{XZ} = P_{XZ} + (1 + P_{XZ})P_{xy}\,P_{YZ}\,\beta \quad (3)$$

Where β is a design parameter for the impact of transitivity. According to Verma & Srivastava (2012) $\beta \in [0,1]$.

The integrated routing protocol was observed to outperformed both the prophet and the epidemic routing schemes with respect to opportunistic networks, but it did not consider and congestion control in it (Verma & Srivastava, 2012).

Congestion in Opportunistic Network

Nodes in opportunistic networks have limited resources, but they are still willing to altruistically forward messages for other nodes in the network. Congestion occurs when nodes buffer becomes saturated.

In opportunistic networks, no end-to-end connection is established and therefore congestion cannot be detected and controlled by a feedback loop (Bjurefors, 2014).The challenge is how to avoid congestion without the feedback loop, using just local information at nodes. Avoiding congestion can be done by pre-emptive eviction of data items from the buffers of the nodes. Congestion algorithms have the potential to improve delivery ratio and decrease average delay. With an uncontrolled eviction policy there is a potential risk that all replicated copies of the data may be evicted before all destinations have been reached, hence decreasing the delivery ratio (Bjurefors, 2014; Oliveira *et al.,* 2014).

Since congestion in an opportunistic networks occurs when a node's buffer is overwhelmed with messages that may not have been forwarded to another node, a node has to evict messages from its buffer in order to keep the number of items in the buffer small. Also, nodes in an opportunistic network cannot rely on acknowledgements since a contemporaneous end-to-end connection may never exist. The nodes that created messages do not know that a node in the network is congested. The congested node itself has to reduce or solve the problem, basing its decision on what to drop from the buffer using local information available at the nodes. Information can be collected from other nodes (Bjurefors, 2014).

Several strategies have been developed on how to deal with congestion in opportunistic networks, which ranges from buffer advertisement beacon to algorithm to off load data. These strategies are described as follows (Bjurefors, 2014):

i. **Buffer eviction using acknowledgement**

The use of acknowledgement in opportunistic network differs from that of legacy network. In the Internet, TCP acknowledgements are used to show that the message has

INTERNATIONAL JOURNAL – PAS
VOL. 4 NO.1 MAR-2018 ISSN: 1660-5332

reached its destination hence, retransmission of the message is avoided and nodes discard the message from their buffer. In opportunistic networks, there is no end-to-end connectivity, so this is not possible. To use acknowledgement in an opportunistic network, time-to-live message must be attached the message to avoid the packets from lingering in the network. The advantage with acknowledgement is that nodes are sure that the message has been delivered to the destination before the message is evicted from the buffer. The disadvantage is that it takes time for an acknowledgement to disseminate in the network. (Bjurefors, 2014).

ii. **Buffer size advertisement**

The type of congestion that is caused by aggregated undelivered packet by replication can be avoided by nodes sharing their buffer utilization size with neighboring nodes. Using these statistics, a node can tell the congestion level at neighboring nodes. By advertising their free buffers, the neighboring nodes can take decision on what to forward and how much to transfer, making it possible to avoid overloading the node. Message can also be prioritized in order to use the buffer space as efficiently as possible (Bjurefors, 2014).

iii. **Duplication Avoidance:**

A node receives a message when it comes into communication range with other nodes. Prior to receiving a message, a node checks if it has the same message in its buffer, if it has the message, it refuses to collect the message in order not to duplicate it buffer. This method avoids unnecessary wastage of buffer space by ensuring that no same copies of messages are kept in the buffer.

iv. **Data-centric node congestion avoidance:**

Messages are forwarded based on the interest in the data. In this principle, there is an assumption that a node is more likely to create buffer space for data items that are of interest to the node itself. It is also assumed that forwarding nodes keep data that they are interested in, which makes the interested forwarding node to become the new source (Bjurefors, 2014). Nodes usually evict data that is of little interest to the nodes in the network, because few nodes will ask for that data. Data of high interest can also be evicted by some nodes using the assumption that other nodes will keep the data, since it will be frequently requested for and shared. The disadvantage of this

strategy is that there is an increase in storage of data items that will never be forwarded or have already reached all nodes interested in the data. Either they are data items that no node is interested in, or data items that have been replicated many times. These data item become stale and consume buffer space, which could have been used to forward other data item (Bjurefors, 2014).

These four congestion control strategies were used individually in (Yahaya *et al.,* 2015) to improve the performance of the integrated routing protocol, this was done in order to know the one that performed better in opportunistic network.

THE HYBRID CONGESTION CONTROL STRATEGY

In order to reduce congestion, there must be a way to select and eliminate messages. These strategies (pre-emptive eviction of messages) presented earlier have been shown to be more ideal in mitigating congestion in opportunistic network (Yahaya et al., 2015; Bjurefors, 2014). It is worth noting that each strategy has its advantages and disadvantages. Combining the congestion control strategies in a manner that reduces the effect of their disadvantages is of special interest. A properly designed hybrid congestion control will improve routing performance in opportunistic network better. The architecture of the hybrid congestion control is presented as;

Nodes move around the network and forward messages to other nodes when they come into communication range. When two nodes meet (say node A and node B), and node A intends to transfer message X intended for node D to node B, a decision has to be made;

- All nodes advertise their buffer size, when they meet,
- Node B check if it has message X in its buffer space,
- If yes, it ignores message X from node A
- If no, is its buffer utilization greater than or equal to75%?
- If yes, collect only messages of interest to node B.
- If no, node B collects the message from node A, and stores it in it buffer, and forwards it to other nodes it encounters in the network.
- Same is repeated whenever nodes come into communication range until message X reaches its final destination, node D.
- Node D then acknowledges the message and sends the acknowledgement to every node it comes across in the network.

- Nodes delete the copy of the message from their buffer as soon as they receive the acknowledgement from other nodes.

By so doing, all four congestion control strategies have been employed and better buffer management is obtained. It is assumed that the buffer space does not reach 100%, since a node receives only selected messages once it buffer utilization has reached 75%.

IMPLEMENTATION DETAILS

The hybrid congestion control strategy was implemented in the opportunistic Network Environment (ONE) simulator which is java based. It was implemented in the integrated routing protocol using P_0, γ and β as 0.75, 0.98 and 0.25 respectively. A message TTL of 300 seconds was used. In order to create basis for comparison, same simulation settings of Yahaya *et al*., (2015) and Verma & Srivastava, (2012) were used.

The simulation used a part of the Helsinki area (4500 * 3400m). Communication was assumed to be between modern mobile phones and similar devices having up to 20MB of free RAM for buffering messages. Nodes are basically users holding these devices and travelling in cars, on foot, or in trams. 100 nodes were used which have different speeds and pause times. The speed and pause time are specified as;

Pedestrians move at random speeds of 0.5-1.5m/s, pause time between 0-120s.

Trams move at a speed of 7-10m/s, pausing for 10-30s at each configured stop.

Cars are moving at a speed of 10-50km/h, with a pause time of 0-120s

The normal Bluetooth transmission range of 10m range, 2Mbits and a low power use of 802.11bWLAN (30m range, 4.5Mbits) were used. Mobile users generate messages on an average of once per hour per node. The message size ranges between 100kb (text message) and 2MB (digital photo).

RESULTS AND PERFORMANCE EVATUATION

In this section, the performance of the hybrid congestion control strategy was evaluated. First we define the performance metrics as;

Sim_time refers to the total time used for the simulation.

Delivery probability refers to total probability of the messages delivery which is ratio of packets created to packets delivered to their destination.

Packet loss refers to the total number of messages that were aborted during the simulation time.
Delay is average time taken for each successfully delivered packets.
The results obtained for the simulation is presented in Table 1.

Table 1: Simulation Results of Hybrid Congestion Control Strategy

Sim_Time (s)	Packet loss	Delivery probability	Delay (s)
0	0	0	0
1000	0	0	543
2000	0	0.099	717
3000	2	0.099	953
4000	2	0.099	1290
5000	3	0.102	1575
6000	3	0.104	1899
8000	4	0.103	2003
10000	6	0.106	2307
12000	12	0.109	2657
14000	20	0.119	2865
16000	32	0.125	3103
18000	41	0.130	3499
20000	64	0.129	3861
22000	80	0.131	4190
24000	96	0.133	4588
26000	111	0.139	4893
28000	121	0.143	5314
30000	158	0.148	5534
32000	167	0.150	5718
34000	187	0.151	5979
36000	190	0.155	6132
38000	215	0.162	6280
40000	235	0.161	6490
42000	240	0.166	6621
43200	252	0.166	6850

Table 1 shows the result of simulating the hybrid congestion control strategy in the ONE simulator using the default simulation time of 43200s. Result from Table 1 was compared with results obtained in Yahaya *et al.,* 2015 which is shown in Figures 1 and 2. At the end of the simulation time, the packet loss, delivery probability and delay obtained are 252, 0.166 and 6850s respectively.

INTERNATIONAL JOURNAL – PAS
VOL. 4 NO.1 MAR-2018 ISSN: 1660-5332

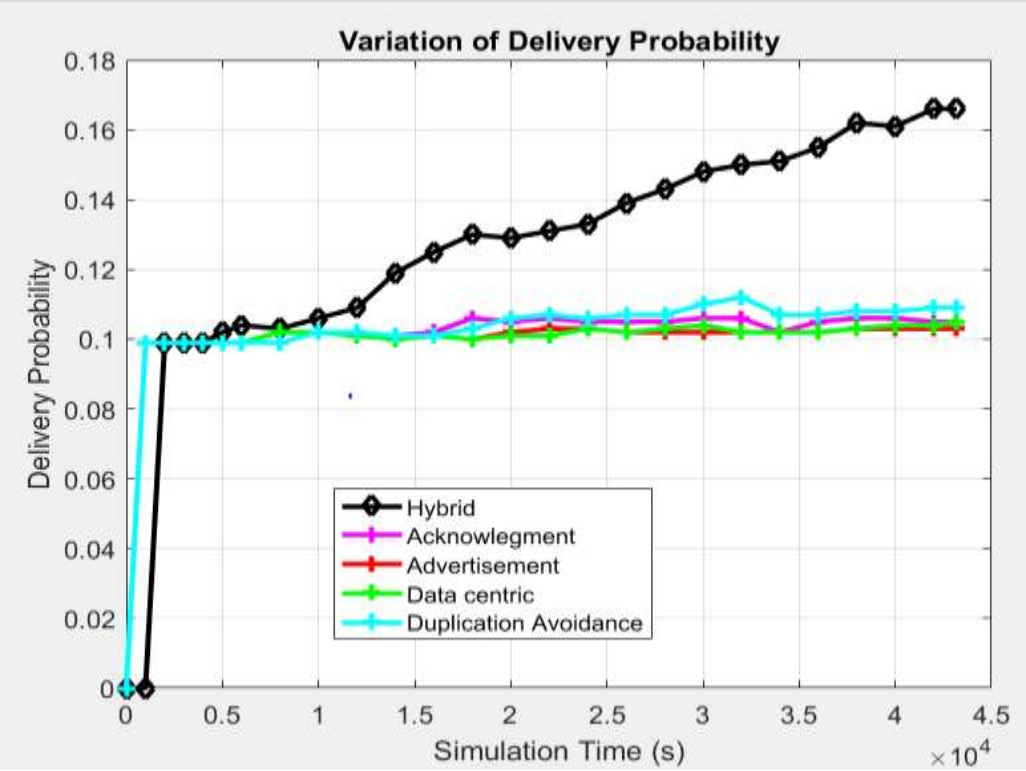

Figure 1: Variation of Delivery Probability with Time

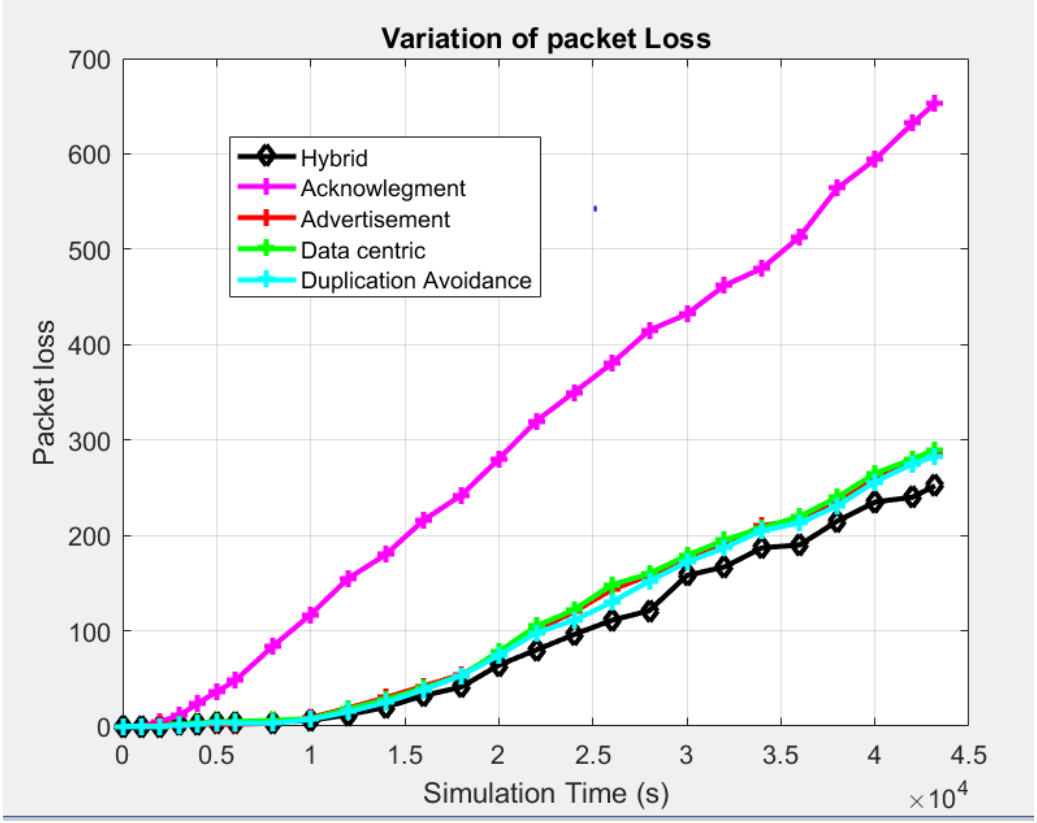

Figure 2: Variation of Packet loss with time

From Figure1, it can be seen the hybrid congestion control strategy outperformed other congestion control strategy with respect to delivery probability. A significantly higher delivery probability of 0.166 was obtained as compared to use acknowledgment, buffer size advisement, data centric method and duplication avoidance with values 0.105, 0.103, 0.105, and 0.109 respectively at the end of the simulation time. The reason for the significant increase in performance being that the hybrid congestion control was able to add up the merits of individual congestion control strategies in itself. This includes prioritizing of messages in order to use the buffer space efficiently, measures to avoid replication of messages in buffer space, timely evacuation of messages from network nodes as soon as the message reaches its final destination, as well as, setting of threshold on when to receive messages in order to prevent congesting nodes. The hybrid congestion control strategy was also able to shed off some limitation of other strategies, for example, losing the message completely before it gets delivered to the destination. This resulted to a better performance which is evident in Figure 2. From Figure 2, it can be seen that at the end of the simulation time, a lower packet loss of 252 was obtained in the hybrid congestion control mechanism as compared to use acknowledgment, buffer size advisement, data centric method and duplication avoidance with values 653, 286, 290 and 283 respectively. This showed that the hybrid congestion control mechanism was able to manage packets relay in the network better without losing the packets.

Another reason for a better performance (increase in delivery probability and reduction in packet loss) is due to the fact that with a good congestion control strategy, congestion is reduced which makes forwarding of messages continue throughout out the simulation time. Without a congestion control method, (or a good congestion control method) or eviction policy, nodes get saturated with messages. Some of these message are unwanted messages or messages that have since been delivered to their final destination. Once the nodes are saturated with message, further relay of messages become difficult which will decrease the delivery rate of messages in the network.

CONCLUSION

Congestion is a major concern in opportunistic network routing. When it is properly managed, a better routing performance is obtained. A hybrid congestion control strategy was introduced into the integrated routing protocol which yielded a better routing performance when compared

with other congestion control strategies. However, it was observed that the hybrid congestion control strategy incurred more delay in message delivery. This is due to the fact that hybrid congestion control strategy took longer time in its execution. Results obtained in this paper are simulated result. Practical real life experiment should be carried out to see if similar result will be obtained as that of the simulated results.

References

Asgari, C., Zareie, A., and Torkashvand, R. R. 2013. Intelligent Routing for Opportunistic Networks Based on Distributed Learning Automata. Journal of Basic and Applied Science Research, 3(7) 117-126. [

Bjurefors, F. 2014. Opportunistic networking: Congestion, Transfer Ordering and Resilience. http://uu.divaportal.org/smash/get/diva2:713179/FULLTEXT01.pdf

Dinakar, S., R.M.Bhavadharini, & S.Karthik. (2013). study of opportunistic network and MANET. *International journal of software & Hardware Reasearch in Engineering, 1*(4).

http://infoscience.epfl.ch/record/180634/files/EPFL_TH5448.pdf

Huang, C.-M., Lan, K.-c., and Tsai, C.-Z. 2008. A survey of opportunistic networks. Paper presented at the Advanced Information Networking and ApplicationsWorkshops, 2008. AINAW 2008. 22nd International Conference on.

IP, Y .K.., Lau, W .C. and Yue, O. C. 2007. "Forwarding and replication strategies for DTN with resource constraints," In Proceedings of IEEE Vehicular Technology Conference, vol. 1, pp. 1260–1264

Journi, K. and Jorg, O. 2008. Time scales and delaytolerant routing protocols. Proceedings of CHANTS"08, San Francisco, California, USA, pp. 13-19. [

Kaur, E. U., and Kaur, E. H. 2009. Routing techniques for opportunistic networks and Security Issues. National Conference on Computing, communication and control.

Lindgren, A., Doria, A., and Schelen, O. 2003. Epidemic Routing for Partially Connected Adhoc Networks. ACM Mobile Computing and Communications Review, 7, 1920.

Oliveira, A. B., del, D. A, V., da Hora, D. N., and Macedo, D. F. 2014. Evaluating contacts in opportunistic networks over more realistic

simulation models. Journal of Applied Computing Research, 3(1), 54-63.

Orozco, J., Santos, R., Ochoa, S. F., & Meseguer, R. (2013) Stochastic Performance Evaluation of Routing Strategies in Opportunistic Networks. *www.dcc.uchile.cl/TR/2013/TR_DCC-20131029-009.PDF.*

Pan, D., Ruan, Z., Zhou, N., Liu, X and Song, Z. 2013. A Comprehensive-integrated buffer management strategy for opportunistic Network. EURASIP Journal on Wireless Communication and Networking. 2013: 103

Pelusi, L., Passarella, A., & Conti, M. (2006). Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. *Communications Magazine, IEEE, 44*(11), 134-141.

Ristanovic, N. (2012). Modeling and Measuring Performance of Data Dissemination in Opportunistic Networks, PhD *Thèse École Polytechnique Fédérale De Lausanne.* 5448.

Shikfa, A., Onen M., & Molva R. (2010). Security Issues in Opportunistic Networks. *MobiOpp '10 Proceeding of the Second International Workshop on Mobile Opportunistic Networking.* 215-216.

Silva, Aloizio P, Burleigh, Scott, Hirata, Celso M, and Obraczka, Katia. 2015. A survey on congestion control for delay and disruption tolerant networks. Ad Hoc Networks, Elsevier 25, 480-494.

Vahdat, A., and Becker, D. 2000. Epidemic Routing for Partially Connected Ad Hoc Networks. Technical Report CS-2000-06, Computer Science Department. Duke University. [

Verma, A., and Srivastava, D. 2012. Integrated routing protocol for opportunistic networks. arXiv preprint arXiv :1204.1658.

Yahaya B., Mu'azu, M.B., Garba, S. (2015) "Congestion Control Strategies On Integrated Routing Protocol for the Opportunistic Network: A Comparative Study and Performance Analysis" International Journal of Computer Applications. 117:1-9.

Yogi, M. K., and Chinthala, V. 2014. A Study of Opportunistic Networks for Efficient Ubiquitous Computing. International Journal of Advanced Research in Computing and Communication Engineering .3(1), 5187-5191