Nigerian Journal of Engineering,Vol. 30, No. , December 2023, ISSN (print): 0794 – 4756, ISSN(online):2705-3954.

Nigerian Journal of Engineering,
Faculty of Engineering, Ahmadu Bello University, Zaria, Nigeria
journal homepage: www.njeabu.com.ng

Congestion Control on the Epidemic Routing Protocol for Opportunistic Networks

B. Yahaya*[1], M. O. Momoh[2], Y. Ibrahim[3], K. O. Shobowale[4], Z. M. Abubakar[5]

[1,3,5]Department of Computer Engineering, Ahmadu Bello University Zaria
[2,4]Department of Mechatronics Engineering Air Force Institute of Technology, Kaduna
*basiraee@gmail.com

Research Article

Abstract

Designing a good routing protocol for an opportunistic network is difficult because of its inherent characteristics (Lack of context information, heterogeneity, storage constraints, unstable connectivity, etc.).Due to the aforementioned constraints, most nodes flood messages in the network. This is done with the assumption that the message will eventually reach its final destination than continuously keeping it in the nodes' buffer. As such,flooding-based schemes are used. These flooding based schemes have the disadvantage of causing network congestion, overutilization of system resources, as well as causing network overhead. If these schemes are not properly managed, packets would be lost and drop in network performance would be recorded. This research is aimed at improving the performance of the epidemic routing (a flooding-base routing protocol) by managing congestion. Buffer size advertisement congestion control strategy was used. Simulation was carried out using the opportunistic network environment (ONE) simulator which the codes are written in java. The buffer size advertisement congestion control strategy was developed and incorporated on the epidemic routing protocol on the Helsinki benchmark simulation area. Results were obtained and compared with the epidemic routing protocol. The epidemic routing protocol with buffer size advertisement congestion control strategy was seen to have outperformed the epidemic routing protocol without congestion control strategy by 25% in terms of delivery probability. In terms of packet loss, the buffer size advertisement congestion control strategy outperformed the epidemic routing protocol by 44%. These results showed that proper management of congestion can greatly improve the performance of opportunistic network.

doi: 10.5455/nje.2023.30.03.14

Keywords
Opportunistic network, congestion, flooding-based routing, buffer management

Article History
Received: – February, 2023
Reviewed: – October, 2023
Accepted: – November, 2023
Published: –December, 2023

1. Introduction

The opportunistic network is an autonomous, delay tolerant network (DTN)that forwards messages even if a direct link between the destination and the source does not exist. It operate with or without network infrastructure. It is self organising and easy to deploy. It has a flexible network topology and it has no fixed communication range (Kaur & Kaur, 2009; Verma & Srivastava, 2012; Yogi &Chinthala, 2014; Asgari *et al.,* 2013). An opportunistic network is derived from the delay-tolerant network there are no specific links between nodes in opportunistic networks, and messages are propagated in a "store-carry-forward" manner (Yu*et al.,* 2022; Abouarork& Ahmad, 2021). These aforementioned characteristics have made opportunistic network widely used in a number of applications (adhoc network for emergency 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. Routing, congestion and security are the major issue in an opportunistic network due its inherent characteristics (heterogeneity, flexible topology, storage constraint, lack of context information) (Dinakar *et al.*, 2013; Mishra & Gupta 2022; Qiu *et al*., 2020). As such, it is difficult to design an efficient routing protocol for the opportunistic network (Kaur & Kaur, 2009; Verma & Srivastava, 2012; Huang *et al*., 2008; Shikfa*et al.,* 2010; Ristonovac, 2012; Orozco*, et al.*2003). There exist numerous routing protocol in an opportunistic network (Ali *et al*., 2019)

Some of the routing protocols in an opportunistic network include :

i. Epidemic (Vahdat & Becker 2000)
ii. Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) (Lindgren *et al*., 2003).
iii. Spray-and-Wait (Spyropoulos, *et al.,*2005)
iv. Integrated Routing Protocol (IRP)(Verma & Srivastava, 2012)
v. Coding in Opportunistic Routing (CodeOR) (Lin *et al*., 2008)
vi. History Based Routing Protocol for Opportunistic Networks (HIBOp)
vii. Practical Opportunistic Routing (POR) Hu *et al.,* (2013)

viii. Probabilistic Routing Protocol for Intermittently Connected Mobile Ad-hoc Network (PRoPICMAN)(Nguyen *et al*., 2007).

There are many schemes (Epidemic, IRP, Spray-and-Wait, etc) use flooding approach in one way or the other in order to improve delivery rate due to the absence of context information in the opportunistic network.(Vahdat & Becker 2000; Lindgren et al., 2003; Keranen & Ott, 2009; Verma & Srivastava, 2012; Lin et al., 2008; Islam & Waldvogel 2011; Asgari et al., 2013; Hu et al., 2013; Lohachab&Jangra, 2019; Ali *et al.,* 2022).However, these flooding- based schemes generates network overhead which eventually congests the network due to storage constraints of nodes.(Vahdat & Becker, 2000). Congestion greatly affect the network performance in a negative manner (Zhang et al., 2021) such as lose of data, significant reduction in quality of service, and the network becomes prone to security threat.Therefore, reducing congestion in flooding-schemes is important.

In the attempt to make the epidemic routing protocol(a flooding-based scheme) better, Verma & Srivastava, 2012 hybridized the epidemic routing protocol with the PRoPHET routing protocol to form integrated routing protocol. The integrated routing protocol significantly performed better with a higher message delivery since it did not flood messages at all times. However, a better performance would have been achieved when he considers security and congestion in the routing protocol.

Silva, *et al.,*(2015) surveyed the processes of DTN congestion control. They concluded 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 in order to reducing congestion, but a higher overhead ratio was obtained as compared to the spray-and-wait model.

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 were seen to reduced congestion greatly. This paper is an extended version of the previous publication (Yahaya *et al*., 2015), with the aim of applying best congestion control technique (buffer size advertisement) to the epidemic routing protocol.

The remainder of the paper is organized as: Section 2 presents an overview of the epidemic routing protocol and congestion in opportunistic network. Section 3 explain the congestion control technique. Implementation details are presented in Section 4, while the results and performance are evaluated in section 5. Section 6 concludes the paper.

2. Concept Overview

2.1 Epidemic Routing Protocol

Routing protocols decide which device forwards data to based-on specific network characteristic they observe. The more the knowledge of the network topology known and used, the better routing performance obtained. In opportunistic networks this knowledge is not readily available, such that tradeoff must be made between performance and knowledge requirement (Kaur & Kaur, 2009; Pelusi, *et al.*, 2006; Verma & Srivastava, 2012). This tradeoff is seen in the high network delay incurred in opportunistic routing.

In order to reduce network delay, the epidemic routing protocol floods packet all over the network without using any network metric or context information. Epidemic provides a final delivery of messages to the destinations using minimal assumption of connectivity and topology of the network (Pelusi *et al.*, 2006). The heuristic behind this policy is that, the message should be broadcast all over the network (flooding) expecting that it will reach its final destination. This technique works well in a highly mobile network where the contact opportunities needed for data diffusion are common.

The epidemic protocol simply forwards all data to nodes in the network with minimal information of network connection or organization. In the epidemic routing protocol, each message is recognized by it globally unique message ID, a source and a destination address. Each node maintains two buffers, one for storing the message it initiated and the other for messages it is storing for other host. Each node stores a summary vector which contains a summary of the messages stored in its buffer. When two nodes meet, they exchange their summary vector, then each node check which message is missing and then request for the missing message. By so doing, the messages get flooded in the network, and eventually, the message reaches its destination (Vahdat & Becker, 2000).

The epidemic routing protocol is the only solution when routing information about the user is absent. Higher delivery probability is guaranteed even though it saturates the network with many copies of the same data, generate high overhead, it consumes network resources, suffer from network contention and may potentially lead to network congestion(Jones & Ward, 2006; Pelusi *et al.*, 2006; Verma & Srivastava, 2012; Journi & Jorg, 2008).

2.2 Congestion in Opportunistic Network

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

The absence of an end-to-end connection in opportunistic network makes it difficult to detect and control congestion using a feedback loop (Bjurefors, 2014). Hence, how to avoid a feedback loop, using only local information at nodes should be used. Avoiding congestion can be done using pre-emptive eviction of data from the nodesbuffers.

Good congestion algorithms can improve delivery ratio and decrease average delay. With an uncontrolled eviction policy, there is a risk that all duplicated copies of 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 the buffers' of nodes are overwhelmed with messages that may not have been sent to another node, a node has to evict messages from its buffer in order to keep the number of messages in the buffer few. Also, nodes in an opportunistic network cannot depend on acknowledgements since a continuous end-to-end connection may not exist. The nodes that created messages do not know when a node in the network is congested. The congested node has to solve the problem by deciding on what to drop from the buffer using just the local information at the nodes. Information can be collected from other nodes (Bjurefors, 2014).

Several strategies have been developed on how to reduce 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

There is a difference in the use of acknowledgement in opportunistic network as compared to that of legacy network. For example, TCP acknowledgements are used when messages have reached their destination hence, retransmission of the message is avoided and nodes dispose the message from their buffer. In opportunistic networks, the absence of an end-to-end connection makes it impossible. Lingering of messages can be avoided by assigning time-to-live messages in order to use acknowledgment.The merit of acknowledgement is that messages would be delivered to the final destination before the message is removed from the buffer. The demerit is that it takes long for an acknowledgement to be sent in the network. (Bjurefors, 2014).

ii. Buffer size advertisement

The type of congestioncaused by accumulated undelivered packet by replication can be prevented by nodes giving their buffer utilization sizewith neighboring nodes. Using these information, a node knows the level of congestion of neighboring nodes. By advertising their available space, the neighboring nodes easily decide on what to forward. As a result, overloading of node is avoided. Message can also be prioritizedso as to make buffer space usage as efficient as possible (Bjurefors, 2014; Ip *et al.,*2007).

iii. Duplication Avoidance:

Nodes exchange messageswhen theycome into communication range with other nodes. Before a node receives a message, it checks whether it has the same message in its buffer, if it has that same message, it refuses to collect the message in order not to duplicate it buffer. By so doing, unnecessary wastage of buffer space is avoided by ensuring that same copies of messages are not restored in the buffer.

iv. Data-centric node congestion avoidance:

A messages is sent based on the interest in its content. There is the assumption that a node is more likely to make space in its buffer for data items it is interested in. Also, it is assumed that forwarding nodes keep data that they are interested in. This makes the forwarding node to become a new source (Bjurefors, 2014). Nodes usually delete data which are of little interest to the nodes in the network, because the data will be requested by few nodes. Data of high interest can also be evicted by some nodes using the assumption that other nodes will keep such data, since the data will be frequently asked for and shared. The drawback of this method is that there is a rise in the storage of data items that may never be forwarded or data that has already reached all nodes interested in it. They could either be data items that no node is interested in, or over replicated data items. Such data become stale and waste buffer space, which would have been useful in forwarding other data items (Bjurefors, 2014).

3.0 Congestion Control Strategy

In order to reduce congestion, there has to be a way of selecting and eliminating 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.

Buffer size advertisement was used as the congestion control strategy. This is because the epidemic routing protocol has a way of preventing duplication of messages on its own. That is, by exchanging the summary vector when two nodes meet, then each node check which message is missing and then request for the missing message only. Also, the use of acknowledgement was found not to very effective in opportunistic network due to the absence of a complete end-to-end connection at all times. In order to avoid consumption of buffer space by stale data which may never be used in the network, data-centric node congestion avoidance was not used.

In the buffer size advertisement method, 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. The decision is depicted in the algorithm presented hereunder. The Flowchart of the congestion control strategy is depicted in Figure 1.

All nodes advertise their buffer size when they meet
Node B check for message X in its buffer space when it meets node A
If *node B has message X*
Then
ignores message X from node A
Else if *its buffer utilization greater >= 95%?*
Then
ignores message X from node A, delete messages forwarded >2
Else *collects the message X from node A, stores in buffer, and forwards it to other nodes when encountered in the network.*
End if

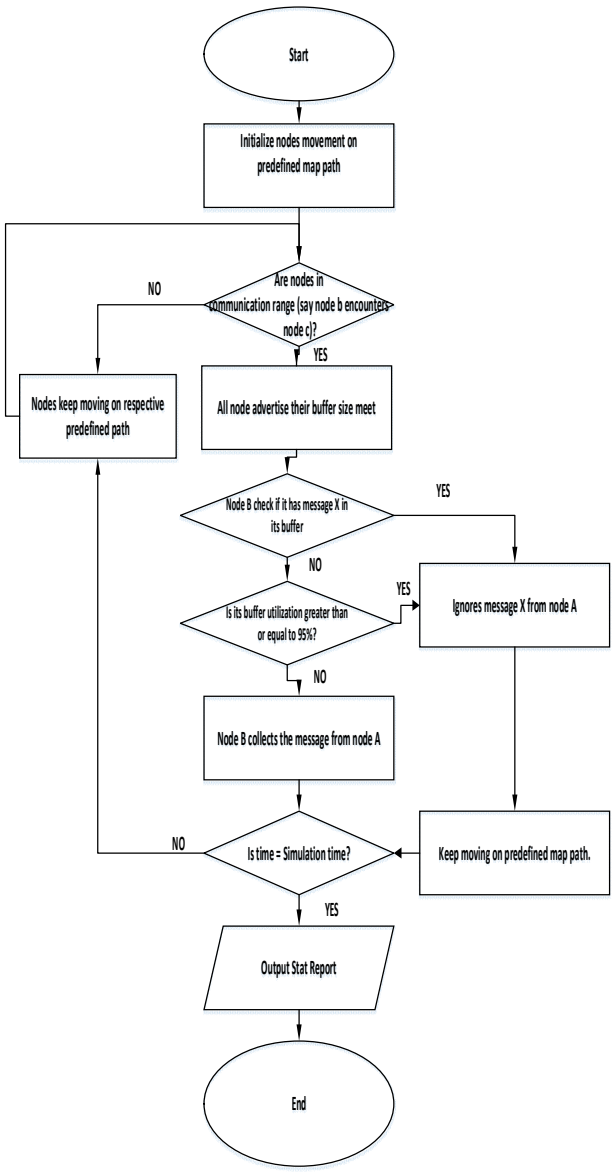

Figure 1: Flowchart of the Congestion Control Strategy

Using this method, message spread like epidemic of some disease through the network as long as the buffer space is available. Buffer size advertisement congestion control strategy was used to prevent the buffer space from being completely full, so as to prevent unwanted message dropping and packet loss. Also, nodes were made to drop messages which has been delivered to their destination. A message is dropped if the message had been shared with a number of nodes so as create space for new messages.

3.1 Implementatıon Detaıls

Simulations were carried out in the opportunistic Network Environment (ONE) simulator which is Java-based. It was implemented in the epidemic routing protocol. In order to create basis for comparison, similar simulation settings of Vahdat and Becker, 2000 were used.
The simulation area has a dimension of 1500* 3000m. Communication was assumed to be between smart mobile phones and similar smart devices having up to 20MB of RAM for buffering messages. Nodes are basically users holding these devices and travellingin cars,on foot, or in trams. 50 nodes were used which have different speeds and pause times. Nodes were moving in to a random way-point mobility model with speed ranging from 0-20m/s (Camp *et al*., 2002; Vahdat & Becker 2000).
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).

4.0 Results and Performance Evaluation

This section presents the performance of the congestion control strategy.
The performance metrics are defined 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.
The results obtained for the simulation is presented in Table 1.

Table 1: Simulation Results of Epidemic Routing Protocol with and without Congestion Control Strategy

Sim_time (s)	Delivery prob.	Delivery prob. with CC	Packet loss	Packet loss with CC
0	0	0	0	0
2000	0	0	0	0
4000	0.088	0.081	31	2
6000	0.091	0.089	72	8
8000	0.103	0.104	91	15
10000	0.105	0.106	119	24
12000	0.109	0.113	145	38
14000	0.128	0.131	174	58
16000	0.117	0.133	193	75
18000	0.125	0.138	219	81
20000	0.135	0.142	236	103
22000	0.139	0.161	258	109
24000	0.143	0.173	277	117
26000	0.141	0.174	282	122
28000	0.155	0.181	306	128
30000	0.159	0.195	311	135
32000	0.168	0.201	318	147
34000	0.170	0.219	320	159
36000	0.180	0.243	331	170
38000	0.222	0.261	337	186
40000	0.248	0.281	348	197
42000	0.250	0.311	352	203
432000	0.247	0.309	366	205

Table 1 shows the result of simulating the epidemic routing with and without congestion control strategy in the ONE simulator using the default simulation time of 43200s. CC was used to denote congestion control in the Table. At the end of the simulation time, thedelivery probabilityfor the epidemic routing protocol with and without congestion control were 0.309 and 0.247 respectively, the packet loss was205 and 366 respectively. Result from Table 1 were used to generate Figures 2 and 3.

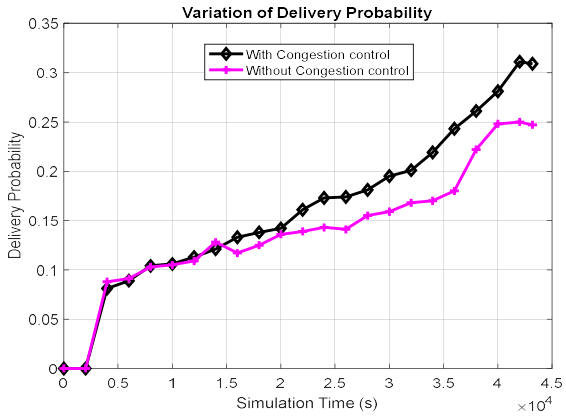

Figure 2: Variation of Delivery Probability with Time

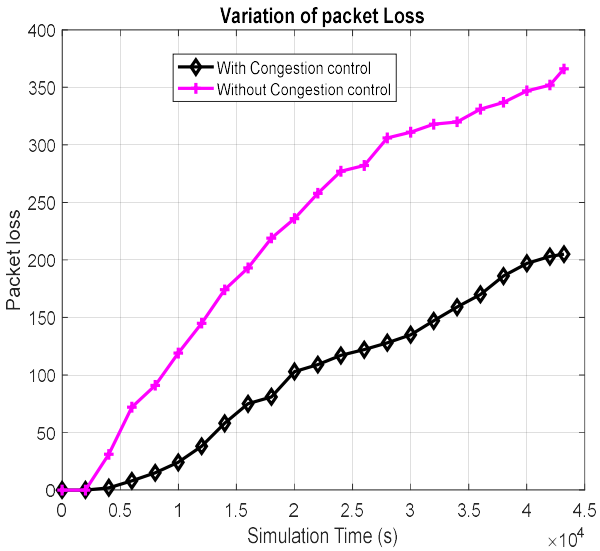

Figure 3: Variation of Packet loss with time

The congestion control strategy improved the routing performance of the epidemic routing protocol with respect to delivery probability as seenin Figure 2. A significantly higher delivery probability of was obtained (0.309) as compared to that without congestion control (0.247) at the end of the simulation time. The reason for the significant increase in performance includes 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 congestion control strategy was able reduce the loss of messages before it gets delivered to the destination. This resulted to a better performance which is evident in Figure 3. From Figure 3, it can be seen that at the end of the simulation time, a lower packet loss of 205 was obtained with the congestion control mechanism as compared to that of the epidemic routing protocol without congestion control (366). This showed that the 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 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 messages, further relay of messages become difficult which will decrease the delivery rate of messages in the network.

5.0 Contribution to Knowledge

This work presented a modified buffer size advertisement mechanism as a congestion control strategy. The congestion

control strategy significantly improved the performance of epidemic routing protocol, this is evident in higher delivery probability (25%)and lower packet loss (44%). This showed that proper management and control of congestion can greatly improve the performance of opportunistic network.

6.0 Conclusion

Congestion is a major concern in opportunistic network routing. When it is properly managed, a better routing performance is obtained. Buffer size advertisement congestion control strategy was introduced into the epidemic routing protocol which yielded a better routing performance when compared with the epidemic routing without the congestion control strategy in it. The epidemic routing protocol with buffer size advertisement was seen to increase the delivery probability from 0.247 to 0.309 (25%), and reduce the packet loss from 366 to 205 (44%). These results showed that with proper management of congestion, better packet relay is obtained which greatly improve the performance of the opportunistic network.

References

Abouarork& Ahmad, (2021) Authentication in opportunistic networks: State and art, Journal of Discrete Mathematical Sciences and Cryptography, 24:6, 1689-1700, DOI: 10.1080/09720529.2021.1873254

Ali, H. K., Lenando, H., Alrfaay, M., Chaoui, S., Chikha, H. B., &Ajouli, A. (2019). Performance Analysis of Routing Protocols in Resource-Constrained Opportunistic Networks. Advances in Science, Technology and Engineering Systems Journal, 4(6), 402413. doi:10.25046/aj040651

Ali, H. K., Lenando, H., Chaoui, S., Alrfaay, M., & Tawfeek, M. (2022). A Dynamic Resource-Aware Routing Protocol in Resource-Constrained Opportunistic Networks. Computers, Materials & Continua, 70(2), 41474167. doi:10.32604/cmc.2022.020659

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

Camp, T., Boleng, J., & Davies, V. (2002). A Survey of mobility models for ad hoc network research. Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile ad hoc Networking: Research, Trends and Application, vol. 2, no. 5, pp483-502.

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

Hu, W., Xie, J., & Zhang, Z. (2013). Practical Opportunistic Routing in High-Speed Multi-Rate Wireless Mesh Networks.Proceedings of the 14th ACM International Symposium on Mobile Ad-hoc Networking and Computing (MobiHoc'13). 127-136. Bangalore, India — July 29 - August 01, 2013. doi>10.1145/2491288.2491310

Huang, C.-M., Lan, K.-c., and Tsai, C.-Z. 2008. A survey of opportunistic networks. Paper presented at the Advanced Information Networking and Applications Workshops, 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

Islam, M. A., & Waldvogel, M. (2011). Questioning flooding as a routing benchmark in Opportunistic Networks. *Paper presented at the Internet Communications (BCFIC Riga), 2011 Baltic Congress on Future*. 128-133.

Jones, E. P., & Ward, P. A. (2006). Routing strategies for delay-tolerant networks. *Submitted to ACM Computer Communication Review (CCR)*.

Journi, K. and Jorg, O. 2008. Time scales and delay-tolerant 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.

Keranen, A., & Ott, J. (2009). The ONE Simulator for DTN Protocol Evaluation. *Special report, Helsinki University of Technology, Networking Laboratory.*

Lin, Y., Li, B., & Liang, B. (2008). *CodeOR:* Opportunistic routing in wireless mesh networks with segmented network coding.*Paper presented at the Network Protocols,ICNP 2008. IEEE International Conference on.*

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

Lohachab, A. and Jangra, A. (2019) "Opportunistic Internet of Things (IoT): Demystifying the Effective Possibilities of Opportunistic Networks towards IoT," in Proceedings of the 2019 6th International Conference On Signal Processing And Integrated Networks (SPIN), pp. 1100–1105, Noida, India.

Mishra, S.K., Gupta, R. (2022). Routing Protocols in an Opportunistic Network: A Survey. In: Pandian, A.P., Fernando, X., Haoxiang, W. (eds) Computer Networks, Big Data and IoT. Lecture Notes on Data Engineering and Communications

Technologies, vol 117. Springer, Singapore. https://doi.org/10.1007/978-981-19-0898-9_14

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.

Qiu, S., Wang, D., Xu, G., and Kumari, S. (2020) Practical and provably secure three-factor Authentication protocol based on extended chaotic-maps for mobile lightweight devices. IEEE Transactions on Dependable and Secure Computing, vol. 1.

Ristanovic, N. (2012). Modeling and Measuring Performance of Data Dissemination in Opportunistic Networks, PhD *ThèseÉcole Polytechnique Fédérale De Lausanne.* 5448. *http://infoscience.epfl.ch/record/180634/files/EPFL_TH5448.pdf*

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.

Spyropoulos, T., Psounis, K., Raghavendra, C. S.(2005) Spray and wait: an efficient routing in intermittently connected mobile networks. *Proceeding of ACM SIGCOMM Workshop on Delay Tolerant Networking (WDTN), Philadelphia, USA,* pp. 252-259.

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

Yu, L., Xu, G., Wang, Z., Zhang, N., and Wei F. (2022). A Hybrid Opportunistic IoT Secure Routing Strategy Based on Node Intimacy and Trust Value. Hindawi Security and Communication Networks Volume 2022, Article ID 6343764, 12 pages https://doi.org/10.1155/2022/6343764

Zhang, Q.F., Gui, C., Song, Y., Sun, B. L., and Dai, Z. F. (2021) "Routing algorithm in opportunistic networks based on node mobility," Journal of Software, vol. 32, no. 8, pp. 2597–2612, China.