# Designing an Efficient Routing Protocol for Opportunistic Network

[1]Nikhil Khichariya,[2]Neha Choubey

[1]M.Tech.Scholar, Computer Technology (CSE), RCET, BHILAI, C.G., India,
[2]Asst.Professor, CSE Department, RCET, BHILAI, C.G., India,
[1]nikhilkhichariya@gmail.com
[2]nehachb5@gmail.com

Abstract - Opportunistic networks are one of the mainly attractive developments of MANETs. In These networks, movable nodes are enabled to correspond with each other even if a route linking them not at all exists. In addition, nodes are not invented to hold or obtain any information about the network topology, which (instead) is essential in traditional MANET routing protocols. Routes are built enthusiastically, while communication are route among the dispatcher and the target(s), and any promising node can opportunistically be use as subsequently hop, provide it is probable to take the communication quicker to the final objective.

These necessities formulate opportunistic networks a difficult and hopeful research field. In this Paper, a new steering protocol for transportation less is predictable that is an enhancement of the obtainable contagion routing protocol.

Keywords—Mobile ad hoc network (MANET), Opportunistic networks (Oppnets), Sensor Networks (sensornets).

## I. INTRODUCTION

A new technology of timeserving networks or Oppnets permits integration of the varied communication, computation, sensing, storage and different resources that surround us additional and additional. We have a tendency to not solely realize ourselves in their thick however depend upon them more and more as requirements instead of luxuries. Few would deny that communications and computing area unit additional and additional pervasive. The goal for Oppnets is to leverage the wealth of pervasive resources and capabilities that area unit inside our reach. Usually this can be often a treasure that continues to be useless owing to "linguistic" barriers. Completely different devices and systems area unit either unable speak to every different, or don't even attempt to communicate. They continue to be on completely different wavelengths-typically virtually, perpetually a minimum of metaphorically. this happens despite devices and systems gaining ground in autonomous behaviour, organization talents, ability to ever-changing environments, or perhaps self-healing once round-faced with part failures or malicious attacks. it's look somewhat ironic to an individual unaware of ability challenges that such ever additional powerful and intelligent entities don't seem to be creating equally nice strides in rebuke one another. With Oppnets, we have a tendency to chart a brand new direction inside the world of laptop networks.

## II. BASICS OF OPPNETS

### A. SEED OPPNET AND ITS GROWTH

Each opportunistic network grows from a seed that's a group of nodes used along at the time of the initial oppnet preparation. The seed is pre-designed (and will thus be viewed as a network in its own right. Within the extreme it will incorporates one node. The seed grows into a bigger network by extending invites to affix the oppnet to foreign devices, node clusters, networks, or different systems that it's able to contact. Any new node that becomes a full-fledged oppnet member, that's a helper, is also allowed to ask external nodes.

### B. OPPNET HELPERS

**1)** Potential Oppnets Helpers:

The set of helpers includes even entities not typically thought of as network nodes, wired and wireless, free-standing and embedded. Even nodes with no sensing capabilities, like networked mainframes from LANs or wireless-equipped processors embedded in cars, will considerably contribute to process or communication capabilities of associate oppnet. After all, any networked computer or embedded processor has some helpful sensing, processing, or communication capabilities.

2) Helper Functionalities:

It ought to be noted that, in general, operating within the "disaster mode" doesn't need any new functionalities from the helpers. for instance, just in case of fireside observation tasks, the weather sensor net that became a helper is merely told to prevent collection precipitation knowledge, and use the discharged resources to extend the sampling rates for temperature and wind direction. It's potential that additional powerful helpers might be reprogrammed on the fly.

C. CRITICAL MASS FOR AN OPPNET AND GROWTH LIMITATIONS

1) Critical Mass:

Oppnets is extremely effective if they're able to build up their size (by invitatory different nodes) enough to achieve a definite "critical mass" in terms of size, node locations, and node capabilities. Once this threshold is passed, they're able to communicate, calculate, associated live aspects of entities and physical surroundings in their interior in an new detail. Sensornets or not will gather data-legitimately or not-on general public, employees, or different monitored people.

2) Growth Limitations:

The network stops inviting additional nodes once it obtains enough helpers providing enough sensing, processing, and communication capabilities (cost/benefit analysis of inviting additional nodes can be performed). It ought to avoid recruiting superfluous nodes that wouldn't facilitate and may scale back performance by victimization resources simply to "gawk." This doesn't mean that network configuration becomes frozen.

D. APPLICATIONS FOR OPPNETS

1) Emergency Applications:

We see vital applications for opportunistic networks altogether varieties of emergency things, for instance in cyclone disaster recovery and Homeland Security emergencies. We have a tendency to believe that they need the potential to considerably improve potency and effectiveness of relief and recovery operations.

2) Benevolent and Malevolent Oppnet Applications:

As most technologies, opportunistic networks will be accustomed either profit or damage humans, their artifacts, and technical infrastructure they depend upon. Invited nodes may be "kept within the dark" regarding the goals of their host oppnets. Specifically, "good guys" may be cheated by a malevolent oppnet and believe that they'll be accustomed profit users.

3) Counteracting Malevolent Oppnet Applications:

To counteract malevolent oppnets threats, predator networks that go after all types of malevolent networks - including malevolent oppnets- will be created. They sight malevolent nets, plant spies in them, and use the spies to find true goals of suspicious networks some of the suspicious networks may really be benevolent ones, victims of false positives.

## III. EVOLUTION

The design of economical routing ways for opportunistic networks is mostly a sophisticated task thanks to the absence of data regarding the topological evolution of the network. Routing performance improves once a lot of information regarding the expected topology of the network is exploited. Sadly, this sort of data isn't simply on the market, and a trade-off should be met between performance and information demand.

A first classification is between algorithms designed for utterly flat accidental networks (without infrastructure), and algorithms during which the accidental networks exploit some type of infrastructure to opportunistically forward messages (with infrastructure). Within the former case, approaches is any divided in dissemination primarily based and context based. Dissemination-based algorithms square measure basically styles of controlled flooding, and differentiate themselves for the policy accustomed limit flooding. Context-based approaches sometimes don't adopt flooding schemes, however use information of the context that nodes square measure operative in to spot the simplest next hop at every forwarding step. Algorithms that exploit some type of infrastructure is divided (depending on the kind of infrastructure they trust on) in mounted infrastructure and mobile infrastructure. In each cases the infrastructure consists by special nodes that square measure a lot of powerful with relation to the opposite nodes normally gift within the accidental network. They need high storage capability and thus they will collect messages from several nodes passing by, even for a protracted time. They even have high energy. Nodes of a set infrastructure square measure settled at specific geographical points whereas nodes of a mobile infrastructure move around within the network following either pre-determined familiar ways or utterly random ways.

A. ROUTING WITHOUT INFRASTRUCTURE

1) Dissemination-based Routing

The design of economical routing ways for opportunistic networks is mostly a sophisticated task thanks to the absence of data regarding the topological evolution of the network. Routing performance improves once a lot of information regarding the expected topology of the network is exploited. Sadly, this sort of data isn't simply on the market, and a trade-off should be met between performance and information demand.

A first classification is between algorithms designed for utterly flat accidental networks (without infrastructure), and algorithms during which the accidental networks exploit some type of infrastructure to opportunistically forward messages (with infrastructure). Within the former case, approaches is any divided in dissemination primarily based and context based. Dissemination-based algorithms square measure basically styles of controlled flooding, and differentiate themselves for the policy accustomed limit flooding. Context-based approaches sometimes don't adopt flooding schemes, however use information of the context that nodes square measure operative in to spot the simplest next hop at every forwarding step. Algorithms that exploit some type of infrastructure is divided (depending on the kind of infrastructure they trust on) in mounted infrastructure and mobile infrastructure. In each cases

 

the infrastructure consists by special nodes that square measure a lot of powerful with relation to the opposite nodes normally gift within the accidental network. They need high storage capability and thus they will collect messages from several nodes passing by, even for a protracted time. They even have high energy. Nodes of a set infrastructure square measure settled at specific geographical points whereas nodes of a mobile infrastructure move around within the network following either pre-determined familiar ways or utterly random ways.

2) Context-based Routing

Most of the dissemination-based techniques limit messages flooding by exploiting information concerning direct contacts with destination nodes. Context-based routing exploits additional info concerning the context that nodes are operative in to spot appropriate next hops towards the ultimate destinations e.g., the house address of a user could be a valuable piece of context info to choose following hop. The utility of a number as next hop for a message is here after remarked as utility of that host. Context-based routing techniques are usually able to considerably cut back the messages duplication with relation to dissemination-based techniques. On the opposite hand, context-based techniques tend to extend the delay that every message experiences throughout delivery.

B. ROUTING WITH INFRASTRUCTURE

1) Routing based on fixed infrastructure

In infrastructure-based routing, a supply node wish to deliver a message usually keeps it till it comes handy of a base station happiness to the infrastructure, then forwards the message to that. Base stations are usually gateways towards less challenged networks, e.g., they'll offer net access or they'll be connected to a computer network. Hence, the goal of an time serving routing formula is to deliver messages to the gateways, that are purported to be able to realize the ultimate destination additional simply. Two variations of the protocol are attainable .The primary one works specifically as delineated on top of, and solely node-to-base-station communications are allowed. As a result, messages expertise fairly high delays. The classic example of this approach is that the Infostation model.

2) Routing based on mobile infrastructure (carrier-based routing)

In carrier-based routing, nodes of the infrastructure square measure mobile information collectors. They move around within the network space, following either pre-determined or capricious routes, and gather messages from the nodes they move. These special nodes square measure mentioned as carriers, supports, forwarders, MULEs, or perhaps ferries. They will be the sole entities liable for messages delivery, once solely node-to-carrier communications square measure allowed, or they will merely facilitate increasing property in distributed networks and guaranteeing that additionally isolated nodes are often reached. Within the latter case, delivery of messages is accomplished each by carriers and normal nodes, and each node-to-node and node-to-carrier communication varieties square measure allowed.

C. EPIDEMIC ROUTING

Mobile ad hoc routing protocols enable nodes with wireless adaptors to speak with each other with none pre-existing network infrastructure. Existing ad hoc routing protocols, whereas study to speedily ever-changing constellation, assume the presence of a connected path from supply to destination. Given power limitations, the arrival of short-range wireless networks, and therefore the wide physical conditions over that unplanned networks should be deployed, in some eventualities it's doubtless that this assumption is invalid. Epidemic Routing wherever random pair-wise exchanges of messages among mobile hosts guarantee ultimate message delivery, appears to be the best answer up to now

1) Goals

The goals of Epidemic Routing square measure to:

i) Efficiently distribute messages through partly connected unplanned networks in an exceedingly probabilistic fashion.

ii) Minimize the number of resources consumed in delivering any single message

iii) Maximize the share of messages that square measure eventually delivered to their destination.

2) Epidemic Routing Protocol

Epidemic Routing supports the ultimate delivery of messages to discretionary destinations with negligible assumptions relating to the underlying topology and property of the underlying network. In fact, solely periodic pair-wise property is needed to make sure ultimate message delivery. The Epidemic Routing protocol works as follows. The protocol depends upon the transitive distribution of messages through unexpected networks, with messages eventually reaching their destination. Every host maintains a buffer consisting of messages that it's originated further as messages that it's buffering on behalf of different hosts. For potency, a hash table indexes this list of messages, keyed by a novel symbol related to every message. Every host stores a trifle vector referred to as the outline vector that indicates that entries in their native hash tables square measure set. Whereas not explored here, a "Bloom filter" would well scale back the area overhead related to the outline vector.

## IV. METHODOLOGY

The Limited Flooding Epidemic (LiFE) Protocol :

Limited Flooding Epidemic (LiFE) Protocol is described in detail. For the design of LiFE protocol, the following three improvement factors namely Random_neighbor_selection factor, Stability factor, and Delivery_probability factor, have been added in the existing Epidemic protocol to reduce the amount of message flooding in the network. These improvements will reduce the number of message copies relayed in the network by selecting a proper next hop node instead of flooding the message copy to every node in the network.

### A. RANDOM_NEIGHBOR_SELECTION FACTOR

This factor is used to limit the number of potential neighboring nodes selected as next hop of a sender or an intermediate node. Each node before forwarding the message to its neighbors first calculates a random number say x. If the number of neighboring nodes is greater than x, then the message is forwarded to the x neighbors only. If x is greater than the number of neighbors of a node, then the message is forwarded to all the neighbors. In this way it limits the number of message copies spread in the network.

### B. STABILITY FACTOR

In order to predict the stability of node's movement denoted by S, a table called the Speed Table is used. As the node moves, it records its coordinates as well as the time. Thus, a node can utilize this information to calculate its own average speed over two different positions. We have a list of such average speeds which is stored in the Speed Table. Using this list, it can be analyzed whether the change in average speeds is very large or nominal. A large change signifies an unstable movement whereas a nominal change accounts for a stable node. Initially all the nodes are given a stability value equal to zero. For every two consecutive speeds if the change is greater than 10 units per second, the stability is decreased using the formulae:

$$Snew = Sold - (1-Sold)*Sint \quad \text{..... (1)}$$

Otherwise it is increased using the formula

$$Snew = Sold + (1-Sold)*Sint \quad \text{..... (2)}$$

Here Sint is an initialization constant whose value can be taken in between 0 and 1. In this work, it is taken to be 0.5 which can be modified accordingly as per the need.

### C. DELIVERY PROBABILITY FACTOR

LiFE uses this factor to calculate the delivery probability of a node to another node in the network. It utilizes the history of encounters and transitivity as done in PRoPHET to deliver the message assuming that nodes move in a predictable fashion and not randomly. The delivery predictability P(a,b) is the probability with which node A is likely to meet node B in the future. If the neighbor has more probability of meeting the destination node, the carrier node transfers the message to the neighbor. In order to find the delivery probability of a node, the LiFE protocol uses the same equations as defined in PRoPHET protocol.

The aforementioned Stability factor and Delivery probability factor parameters are used to calculate the Utility Metric denoted by U(i) of the ith node with the formula:

$$U(i) = W(j)*Vi(j) \quad \text{.....(3)}$$

where W(j) is the weight of the jth parameter and Vi(j) is the value of the jth parameter for ith node i.e. Vi(1) is the Stability factor value, Vi(2) is the Delivery_probability factor value for node i. U(i) is thus calculated for node i and a threshold T can be used to decide its selection as the next hop for the message. The message is then forwarded to those neighboring nodes that have a U(i) value greater than T. Thus, T is further used to control the amount of flooding in the network.

## V. RESULT

In this work a new routing protocol named LiFE has been designed and flooding has been limited as well as minimized which results a more efficient routing protocol then Epidemic Routing protocol in terms of Messages Delivered, Dead Nodes, Latency average, Over head Ratio, Average Residual Energy, Message Relayed and various other parameters.

## VI. CONCLUSION & FUTURE SCOPE

Opportunistic networking is a very promising technology for realizing the ubiquitous vision. Based on the increasing pervasiveness of our world, and on releasing end-to-end connectivity constraint, it can better exploit social characteristics via context awareness. We presented here a new routing protocol for Oppnets which is a hybrid of Message Ferrying and Infostation based routing protocols. This protocol tries to reduce the average delays and to improve message delivery rate.

## REFERENCES


[1] "Opportunistic Networking:Data Forwarding in Disconnected Mobile Ad Hoc Networks" Luciana Pelusi, Andrea Passarella, and Marco Conti, IIT-CNR.

[2] "Controlling the Mobility of Multiple Data Transport Ferries in a Delay-Tolerant Network" Wenrui Zhao, Mostafa Ammar and Ellen Zegura.

[3] "Opportunistic Networks:The Concept and Research Challenges in Privacy and Security", Leszek Lilien, Zille Huma Kamal, Vijay Bhuse, and Ajay Gupta.

[4] "Routing in Opportunistic Networks", Hoang Anh Nguyen, Silvia Giordano.

[5] "Prioritized Epidemic Routing for Opportunistic Networks" Ram Ramanathan, Richard Hansen, Prithwish Basu, MobiOpp'07, June 11, 2007.

[6] "Epidemic Routing for Partially-Connected Ad Hoc Networks", Amin Vahdat and David Becker "MobiHoc Poster: Probabilistic Routing in Intermittently Connected Networks".

[7] Anders Lindgren Avri Doria Olov Schel´en, Mobile Computing and Communications Review, Volume 7, Number 3.

[8] Electronics and Telecommunications Research Institute (ETRI), 161 Gajeong-don, Yuseong-gu, Daejeon 305-350, Korea,"Probabilistic Routing in Intermittently Connected Networks", Anders Lindgreny Avri Doria Olov Schel´eny.

[9] "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks", Thrasyvoulos Spyropoulos, Konstantinos Psounis, Cauligi S. Raghavendra,SIGCOMM'05 Workshops, August 22–26, 2005, Philadelphia, PA, USA.Copyright 2005 ACM 1-59593-026-4/05/0008.

[10] "Spray and Focus: Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility" Thrasyvoulos Spyropoulos, Konstantinos Psounis and Cauligi S. Raghavendra, Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops(PerComW'07) 0-7695-2788-4/07.

[11] "INFOSTATIONS : A New System Model for Data and Messaging Services",0-7803-3659-3/9$71 0.00 0 19 97 IEEE, David J. Goodman, Joan Borr&s, Narayan B. Mandayam arid Roy D. Yates.

[12] "Message Ferrying: Proactive Routing in Highly-partitioned Wireless Ad Hoc Networks".

[13] "Ferry Replacement Protocols in Sparse MANET Message Ferrying Systems", Jeonghwa Yang, Yang Chen, Mostafa Ammar, and Chungkee Lee.

[14] "Exploiting Mobility for Energy Efficient Data Collection in Wireless Sensor Networks"Mobile Networks and Applications 11, 327–339, 2006, SUSHANT JAIN, RAHUL C. SHAH, WAYLON BRUNETTE and GAETANO BORRIELLO, SUMIT ROY.

[15] "The Shared Wireless Infostation Model - A New Ad Hoc Networking Paradigm (or Where there is a Whale, there is a Way)", MobiHoc'03, June 1–3, 2003 ,Tara Small, Zygmunt J. Haas.


 