Efficient, Cooperative and Network attributes-Enhanced PRoPHET+ Protocol (EPP) over IoT-enabled OpportunisticNetwork

Sagar Bose[1], Riya Samanta[2], Indrajit Banerjee[3]

Abstract Opportunistic networks are fault-tolerant networks that encounter frequent link failures and a highly intermittent nature. Due to the considerable round trip time, Opportunistic routing protocols typically follow a store-carry-forward routine. As a result, the mobile nodes must keep their message bundles until they meet appropriate forwarders that can further carry these bundles to the desired node. Opportunistic Network is considered one of the major components for the Internet of Things (IoT)-based intelligent systems where end-to-end connections between IoT-enabled nodes are not reliable. The primary motivation of this proposed protocol (EPP) is to consider different physical attributes of participating IoT-enabled mobile nodes and their positional attributes with a current message time-to-live value and decide on routing hops. The primary aim is to increase message delivery rate while keeping an optimal balance between routing overhead, hop count, and cooperation among IoT-enabled nodes. EPP works on delivery rates to find the routing path for message bundles. This predictability value is manipulated using a weighted function of parameters like nodes buffer, bandwidth, power, popularity, and deliverable probability. Besides, EPP also considers statistics on nodes transmission range, the ratio of forwarders distance from the destination to that from the sender, nodes' success ratio, Message TTL, and finally, Enhancement factor, which regulates the contact probability of sender and candidate node. The proposed routing protocol is designed to keep its deployment perspective in handling post-disaster rescue operations. The algorithm is even applied to other movement models, such as the random waypoint mobility model and the shortest map-based mobility model. The simulation shows that EPP maintains high delivery probability while efficiently balancing average latency, average hop count, and overhead ratio.

Keywords Opportunistic routing · Delay-tolerant Networking · Emergency Rescue operation · cooperation

---

[1] Sagar Bose
Indian Institute of Engineering Science and Technology, Shibpur, India
E-mail: sagar.rs2017@it.iiests.ac.in
[2] Riya Samanta
Indian Institute of Technology Kharagpur, IndiaE-
mail: study.riya1792@gmail.com
[3] Indrajit Banerjee
Indian Institute of Engineering Science and Technology, Shibpur, India
E-mail: ibanerjee@it.iiests.ac.in

[1, 2, 3] These authors contributed equally to this work.

Table 1: NOTATION

$Prob(M, N)$	$DeliverableProbabilitybetweenMandN$
B	$BufferOccupancy$
P	$Power$
A	$Bandwidth$
O	$Popularity$
R	$Predictability$
T	$MessageTime - To - Live$
S	$SuccessRatio$
D	$Distance$
K	$TransmissionRange$
W_x	$weightsoftheparameters$
α	$EnhancementFactor$
V_D	$DecisionFactor$
CN	$CandidateNode$

1 Introduction

Building a coordination channel between emergency response teams is a must for managing post-disaster rescue operations. Infrastructure-based connectivity is usually crippled in the event of a significant catastrophe. In this situation, infrastructure-based communication systems like wired or cellular communication are out of scope. On the other hand, Adhoc mobile devices may seem a standard option for continuing relief operations and other emergency coordination activities. In this case, even end-to-end compatibility cannot be assumed, and disconnections are pretty standard. There are already established routing protocols that use opportunistic routing to route message packets effectively. The primary premise of opportunistic routing is that device mobility is an opportunity for communication rather than a hindrance.

Our proposed routing scheme considers real-world parameters like *participation history of IoT-enabled nodes, success ratio, message TTL, and distance between IoT-enabled nodes* for forwarding data packets which are not taken care of by most of the popular probabilistic routing protocols like PRoPHET, PRoPHET+, etc. The work also highlights the applicability of different mobility models. Further, we used a context of a wireless mobile network of intermittently linked IoT-based nodes with minimal power storage and buffer size capacities. Motivated by the above phenomenon, we propose an *Enhanced PRoPHET+ protocol* (EPP). The significant contributions of this paper can be summarized as follows:

1. EPP aims to keep the optimal balance between Routing Overhead, Hop count, and Message Delivery rate while minimizing resource overuse.
2. It incorporates the participation history of IoT-enabled nodes, success ratio, message TTL, and distance between IoT-enabled nodes for making decisions on message forwarding.
3. The concept of Enhancement Factor is introduced which externally regulates the degree of encounters among any pairs of IoT-enabled nodes.
4. Extensive simulations are performed to establish the efficacy of EPP over other popular protocols.

2 Related Work

It is known that delay-tolerant routing is divided into two broad fields, Forwarding based and Flooding based [Saha et al.(2011)Saha, Sheldekar, Mukherjee, Nandi et al.]. The routing where only a lone copy of a message is used, is called Forwarding based. In Flooding, multiple copies of the message are used. Flooding is further of two types that are unlimited and limited, depending on the number of copies generated. In general, each of the flooding techniques uses some kind of heuristic to make routing decisions. The use of heuristic is justified in routing design because finding a routing schedule with full knowledge of the network topology is an NP-hard [Misra et al.(2016)Misra, Saha, and Pal]. Some of the popular flooding-based techniques discussed here are Spray and Wait routing, PRoPHET routing, Epidemic routing, and PRoPHET+ routing.

Epidemic routing [Mitchener and Vadhat(2000)] delivers data to all encountered nodes at the toll of high resource consumption. Spray and Wait [Spyropoulos et al.(2005)Spyropoulos, Psounis, and Raghavendra] is a modification of Epidemic routing and direct delivery, a hybrid between multi-copy and single routing protocols. It imposes an upper bound on the count of possible replicas of a message. The Spray and Wait routing protocol is resource-friendly and fast, its constrained mobility brings limitations to the protocol. PRoPHET [Lindgren et al.(2004)Lindgren, Doria, and Schelen] is a Probabilistic Routing Protocol using History of Encounters and Transitivity for Intermittently Connected Network which increases the message delivery rate by keeping buffer usage and message communication overhead at a low level while assuming that nodes move in predictable behavior. The working principle of PRoPHET is as follows.

β is a scaling constant with β in the range [0, 1]. It regulates the limit to which transitivity should impact the delivery predictability. Suppose that node M meets node N very often and node N comes across node Q more often. Another node X, having a message to communicate to Q, may as well forward the message to M. Although node M may not have repetitive meetings with Q, the transitivity property allows the messages to be sent from M to Q through N. P_{init} is an Initialization constant which defines the initial probability of all nodes. $P_{init} \in [0, 1]$. $\gamma \in [0, 1]$ is the aging factor. The delivery probabilities are rotted with time when a pair does not contact for long. t reflects the number of time units expired since the last update of this probability. Aging helps to exclude non-fresh information maintained by the nodes. Here, the delivery probability Prob(M, N) plays a heuristic. The proposed values are: $\gamma = 0.98$; $P_{init} = 0.75$; $\beta = 0.25$. In [Basu et al.(2018)Basu, Biswas, Roy, and DasBit],a trust-based Watchdog technique is harmoniously amalgamated with PRoPHET so that messages are delivered fortuitously, even in the existence of malevolent and selfish nodes. The Watchdog scans its adjacent nodes resulting in a local perception about their forwarding action. This information is then circulated in the network to create a global knowledge of forwarding performance for finding selfish nodes. But it is shown in [Dhurandher et al.(2017)Dhurandher, Kumar, and Obaidat] that the trust-based protocols do not solve the problem of segregating, avoiding, and identifying the harmful nodes with the amenities of security services such as message integrity, confidentiality, and authentication with cryptographic means. In recent days, more stress is on optimizing energy utilization during delay-tolerant routing mechanism. [Tanwar et al.(2018)Tanwar, Tyagi, Kumar, and Obaidat] talks about a systematic procedure required to be planned for energy prevention during communication among different mobile nodes. More recent work is [Bansal et al.(2019)Bansal, Gupta, Sharma, and Gambhir]. It uses Mendel's Law of Inheritance to solve the problem of routing in an opportunistic network. In the first stage, the protocol predicts the path that the message may follow. The second stage decides whether to transfer the message or not, based on the fitness evaluation of the predicted path. Machine learning as a tool in making various decision adjustments in Opportunistic networking, even in unsupervised form is discussed in [Sharma et al.(2016)Sharma, Dhurandher, Woungang, Srivastava, Mohananey, and Rodrigues]. [Sharma et al.(2019)Sharma, Dhurandher, Agarwal, and Arora] describes a method kROp, which is able to combine the benefits of both context-oblivious and context-aware routing protocols to increase the delivery probability in addition to reducing mean hop count dropped message count, and network overheads but failed to optimize message latency metric. kROp does not cover the security and energy consumption aspect.

Synthesis: We synthesize that there exists a research lacuna in efficient and cooperative data transmission mechanism in an intermittently connected networking environment. Therefore, though different schemes are proposed for modeling DTN and thereby determining the best possible path for data delivery with better network performance, none of the mechanisms are satisfying in terms of cooperative and practicable approach and thereby need an enhancement of PRoPHET+ protocol, which is proposed in this paper.

The remaining contents of this paper are organized as follows. Section 3 describes the working of the proposed scheme. The performance is evaluated in Section 4. Section 5 concludes the paper with future scope.

3 Formulation of EPP

In this section, a detailed formulation of our EPP routing protocol is presented. There are three main assumptions applicable in protocol design.

1. The round-trip time (RTT) value of any message bundle is very high and can be infinite.
2. Post-disaster rescue operation is modeled as an instance of a delay-tolerant network.
3. This protocol also uses heuristics in determining the forwarding process of messages. Moreover, at any instant time, a mobile device can be within the transmission range of another mobile device of the same type.

Definition 1 We introduced *Enhancement Factor*, denoted as α. It is taken as small as possible. The purpose of this factor is to regulate the contact probability Prob (M, N) between the IoT-enabled nodes M and N, whenever needed to be manipulated externally. If this probability increases, nodes M and N have a better possibility to meet each other. Here, $\alpha \epsilon (0, 1)$.

Definition 2 *Deliverable Probability* is a probabilistic metric that indicates the predicted possibility of a IoT-enabled node sending a message to that destination. It is specified at each IoT-based node. As a result, $Prob(M, N)$ is the IoT-enabled node M's deliverable likelihood for IoT-enabled node N. Since they are commonly encountered, the higher the value of $Prob(M, N)$, the greater the probability that M would pass a message to N.

$$Prob(M, N) = (1 - Prob^{\alpha}(M, N)_{old}) * P_{init} + Prob^{\alpha}(M, N)_{old} \quad (1)$$

where α is the Enhancement Factor of the pair (M,N) and $P_{init} \in [0, 1]$ is an initialization constant which ensures that IoT-enabled nodes that are frequently encountered have a high deliverable probability.

Definition 3 *Transitivity* is a property of deliverable probability. If IoT-based node M frequently encounters IoT-based node N and node N frequently encounters node Q, node Q is most likely a suitable node to forward messages to. The equation below depicts how transitivity influences delivery predictability, where $\beta \in [0, 1]$ is a scaling constant that determines the magnitude of the transitivity's effect on deliverable probability.

$$Prob(M, Q) = (1 - Prob^{\alpha}(M, Q)_{old}) * Prob(M, N) * P(N, Q) * \beta + Prob^{\alpha}(M, Q)_{old} \quad (2)$$

Definition 4 *Aging* is also a property of deliverable probability. If a pair of IoT-enabled nodes do not interact with each other for a long time, they are less likely to be effective message forwarders to each other, causing the delivery predictability values to age. The aging equation is seen below, where $\gamma \in (0, 1]$ is the aging constant and ρ is defined as the number of time units t, that have passed after the last time the metric was aged divided by enhancement factor α.

$$Prob(M, N) = \gamma^{\rho} * Prob(M, N)_{old} \tag{3}$$

where, *rho* = t/α

Decision Factor is dependant on nine parameters related to real-world physical attributes. The parameters and their descriptions are as follows:

- *Buffer occupancy*, B is given by $[(B_{left} messageSize)/B_{upperlimit}]$. $B_{upperlimit}$ is calculated as $(B_{total} - B_{this})$, where B_{total} is the overall buffer size and B_{this} is the sum of memory the IoT-enabled node needs to hold self-generated data in terms of logs, traffic details, packet headers, etc
- *Power*, P is crucial to predict the lifetime of the IoT-enabled node. It may happen that a IoT-based node with sufficient buffer space and other criteria to carry forward an intended message does not have enough power to live long in the process. It would die soon, even before meeting the next possible IoT-based node in the process. That is why, if it is handed any message to carry forward, it is obvious that the delivery probability would be very low. Power is computed as $(P_{left} - P_{receive} - P_{send} - P_{upperlimit})/P_{total}$. P_{left} is the remaining power of the IoT-enabled candidate node. P_{send} is the power needed by the candidate to forward a packet to the next hop. $P_{receive}$ is the power utilized by the candidate while receiving a packet from the sender. $P_{upperlimit}$ is (count of packets in the buffer of IoT-enabled candidate node)$*P_{send}$. P_{total} is the initial power capacity of the candidate.
- *Bandwidth*, A plays an important role in regulating of loss of message. Due to the mobility of the IoT-enabled nodes and non-uniform speed distribution among the IoT-enabled nodes in the network, the chance of short-duration contact is huge, so higher bandwidth is preferable to increase deliverable probability.
- *Popularity*, O is calculated as (number of successful transmissions)/(number of maximum transmissions that can be made up to that time). Though the Single point of failure is partially reduced with the buffer and power parameters, but not completely eliminated. Suppose, if many packets are transmitted to a single IoT-enabled node having ample buffer capacity then when this particular IoT-based node fails, all data delivered to this node would disappear. To prevent this, the notion of popularity is added.
- *Predictability*, R is the deliverable probability (defined in Equation-1) used for finding immediate hop. It depicts the current relationship of the IoT-enabled candidate node to the desired IoT-enabled destination node in the long run either directly or through transitive means
- *Message Time-To-Live*, T of the IoT-enabled candidate node is also taken into consideration. Less remaining Message TTL hastens the transfer to an immediate encountered IoT-enabled node. TTL is defined as the amount of time from the generation of the message to the present time. TTL dependant message priority speeds up the chance of message delivery by upholding messages having the closest deadline [Saha et al.(2011)Saha, Sheldekar, Mukherjee, Nandi et al.].
- *Success Ratio*, S
- *Transmission Range*, K
- *Distance*, D

$$V_D = W_1 B + W_2 P + W_3 A + W_4 O + W_5 R + W_6 T + W_7 S + W_8 K + W_9 D \tag{4}$$

Working of EPP: There is a IoT-enabled sender node N_0 having a message bundle. It needs to deliver the bundle to a IoT-enabled destination node N_4. There are three IoT-enabled nodes in between them, N_1, N_2, N_3 . Node N_1 and N_2 fall within the transmission range of N_O but not within the range of N_4. On the other hand, N_3 and N_4 fall within the transmission range of each other. To transfer a message bundle, say, M from N_0 to N_4, the store-carry-forwarding technique is followed. For each known destination, a probabilistic metric called Deliverable Probability is defined at each node, indicating the expected likelihood of that IoT-enabled node transmitting a message to that destination. Thus, N_0 should first select a proper eligible IoT-enabled forwarder node among the candidates, which may be either N_1 and N_2 or both. While doing so, N_0 exchanges deliverable probabilities with all its IoT-enabled candidate nodes. Along with this, physical attributes namely, buffer occupancy, remaining power storage, bandwidth, popularity, cooperation history in terms of success ratio, the relative distance of the IoT-enabled node from the ultimate destination, and transmission range are also exchanged. These attributes including message TTL are used by EPP to determine the next-hop IoT-enabled node among the candidates.

3.1 Parameters and Formulae

P_{init}, β, γ, K: Same meaning as that from Prophet routing algorithm.
Buffer occupancy is given by $[(B_{left} - messageSize)/B_{upperlimit}]$.$B_{upperlimit}$ is calculated as B_{total} - B_{this} , where B_{total} is the overall buffer size and B_{this} is the sum of memory the IoT-enabled node needs to hold self-generated data in terms of logs, traffic details, packet headers, etc.

Power is very crucial to predict the lifetime of the IoT-enabled node. It may happen that a IoT-based node with sufficient buffer space and other criteria to carry forward an intended message does not have enough power to live long in the process. It would die soon, even before meeting the next possible IoT-enabled node in the run. That is why, if it is handed any message to carry forward, it is obvious that the delivery probability would be very low.Power is computed as $(P_{left} - P_{receive} - P_{send} - P_{upperlimit})/P_{total}$. P_{left} is the remaining power of the IoT-enabled candidate node.P_{send} is the power needed by the candidate to forward a packet to next hop.$P_{receive}$ is the power utilized by the candidate while receiving a packet from the sender.$P_{upperlimit}$ is (count of packets in the buffer of IoT-enabled candidate node)*P_{send}.P_{total} is the initial power capacity of the candidate.

Another vital parameter would be *bandwidth*.Due to the mobility of the IoT-enabled nodes and non-uniform speed distribution among the IoT-enabled nodes in the network, chances of short duration contact is huge, so higher bandwidth is preferable to increase deliverable probability. It is clear that there is no scope to know the transmission status of message delivery, so bandwidth may play an important role in regulating of loss of message.

Single point of failure is partially reduced with the buffer and power parameters but not completely eliminated. Suppose, if many packets are transmitted to a single IoT-based node having ample buffer capacity and follow other properties, then when this particular IoT-based node fails, all data delivered to this node is gone.To prevent this, the notion of *popularity* is added. Popularity is manipulated as (number of successful transmissions)/(number of maximum transmission that can be made up to that time).

Predictability is the old probability used for finding immediate hop in traditional PRoPHET rout-

Algorithm 1 EPP Routing

```
Input: Simulation Settings and Mobility Model
Output: Message Statistic Report
    Initialization: Initialize $P_{init}$,$\alpha$,$\gamma$ and $\beta$
 1: $n \leftarrow$ (No. of IoT-enabled Candidate nodes within the proximity of Sender N0)
 2: while (Simulation time is not finished) do
 3:     if $n \geq 1$ then
 4:         Select a IoT-enabled candidate node CN in random order
 5:         if CN     busy then
 6:             for all (Messages M in buffer of N0) do
 7:                 Select a message M from the queue
 8:                 if (CN contains M) then
 9:                     GoTo 8
10:                 else
11:                     if (TTL of M) $\leq 0$ then
12:                         Remove M from S buffer and GoTo step 8
13:                     else
14:                         if (Power of CN is insufficient) OR (Buffer of CN is not enough) then
15:                             GoTo step 5
16:                         else
17:                             if (size of M > current buffer size of CN) then
18:                                 Try to make room for M by dropping some old messages
19:                                 if fail then
20:                                     GoTo Step 8
21:                                 end if
22:                                 if CN is destination then
23:                                     Forward M to CN
24:                                     M from the buffer of N0
25:                                     GoTo Step 32
26:                                 else
27:                                     Exchange deliverable probability vectors between N0 and all CN
28:                                     Update the aging factor using equation ??
29:                                     Exchange physical attributes of IoT-enabled nodes status
30:                                     Normalize the values
31:                                     Calculate and update deliverable probabilities using equations ??,??,?? and ??
32:                                     Order the candidate preference queue in decreasing order of renewed deliverable probabilistic
33:                                     Forward M
34:                                     if (router has energy model) then
35:                                         Update energy values
36:                                     end if
37:                                 end if
38:                             end if
39:                         end if
40:                     end if
41:                 end if
42:             end for
43:         end if
44:     end if
45: end while
46: Generate Message Statistic Report
```

ing. It depicts the current relationship of the IoT-enabled candidate node to the desired IoT-enabled destination node in the long run either directly or through transitive means.

Message Time-to-Live of the IoT-enabled candidate node is also taken into consideration.Less remaining Message TTL hastens the transfer to immediate IoT-enabled encountered node. TTL is defined as the amount of time from the generation of the message to the present time. TTL dependant message priority speeds up the chance of message delivery by upholding messages having the closest deadline [Prodhan et al.(2011)Prodhan, Das, Kabir, and Shoja].

Success Ratio is the ratio of successfully transmitted message to the total count of transfers initiated between a pair interacting [Sharma et al.(2016)Sharma, Dhurandher, Woungang, Srivastava, Mohananey, and Rodrigues].Success ratio intuitively ensures cooperation and participation history of nodes are taken into account for further message transferring. It may happen that during any emergency rescue operation any lost victim who was earlier considered an important point of interest or next-hop station to reach, by the rescuer node is so scared and traumatized that it switches off his cell phone or stop conveying messages. If a node denies to receive and accelerate messages, not only it is unsuccessful to get messages that were meant for itself, but also give adverse impacts on the message delivery of other nodes. This result may not be noticeable if only one node behaves similarly, but could be devastating if multiple nodes act likewise [Misra et al.(2016)Misra, Saha, and Pal].In warfare scenario, voluntary or involuntary non-cooperation takes an expensive toll on message delivery rate. However, in EPP, success ratio helps to eliminate those non-cooperating nodes from the network slowly.

Transmission range is the greatest distance between any pair of IoT-enabled nodes for which the signal radiating from one IoT-enabled node could directly outstretch to the other IoT-enabled node with sufficient strength to rightly derive the coded information.In wireless sensor technology, mobile devices can be equipped with WiFi, Bluetooth, Zigbee, and other transmission means. In this work, Bluetooth is considered because it is cost-effective and in general, all wireless devices ranging from cell phones, PDA, smartwatches have inbuilt Bluetooth system. However, if the cost is not an issue, one can switch to WiFi or other higher range based protocols.

From the work of [Dhurandher et al.(2016)Dhurandher, Borah, Woungang, Sharma, Arora, and Agarwal],it is proved how distance of the candidate node from the destination, can effect opportunistic routing.Thus, of the available candidates,the one which is closer to the destination than others or even than the senders should be given priority.Distance of the candidate from the final destination is also taken into account as one of the deciding factors.This form of distance value may be the Euclidean distance [Dhurandher et al.(2016)Dhurandher, Borah, Woungang, Sharma, Arora, and Agarwal] or Receive signal strength or any other range based techniques [Samanta et al.(2018)Samanta, Kumari, Deb, Bose, Cortesi, and Chaki].

The final parameter proposed is *Enhancement factor*, denoted as α. It is taken as small as possible. The purpose of this factor is to regulate the contact probability Prob (M, N) between the IoT-enabled nodes M and n,whenever needed to be manipulated externally. If this probability increases, IoT-enabled nodes M and N have a better possibility to meet each other. Here, $\alpha \epsilon (0, 1)$ [Boudguig and Abdali(2013)].

4 Performance Evaluation

4.1 Experiment Setup

To verify the performance of the proposed protocol, the ONE Simulator [Keränen et al.(2009)Keränen, Ott, and Kärkkäinen] environment is used.ONE is java based, modular fashioned and simple to use. This simulator is an extensible simulation framework itself, providing message forwarding,mobility, generation of event, various inbuilt-routing protocols and other applications protocols like energy models. It even supports analysis and visualization of results,interfaces for exporting and importing movement traces, events so on. For implementation purpose, the ONE simulator has been customized to add new classes and functionalities. The main new classes included are EPP Router class and E-Active Router Class.The class diagram of which are shown in figure **??**. This is done to enable visibility of certain used parameters and physical attributes of the IoT-enabled nodes like buffer occupancy, power traces, location coordinates, message TTL, speed and transmission range, etc.The IoT-based node is the prime component which is termed as host in the simulator platform. Hosts can be either mobile or static or both, depending on the desired criteria of used mobility model. They are also assumed to have been equipped with necessary hardware. These hosts may be grouped or may move independently.

In this analysis, three mobility models have been considered, namely *Random Way Point Mobility Model, Shortest Map Based Mobility Model and Cluster Based Mobility Model* [Lin et al.(2015), Ekman et al.(2008)Ekman, Keränen, Karvo, and Ott]. The Random Way Point Mobility Model demands nodes to progress randomly. Only a region of the size of the entire world is taken and the nodes move only within that region of an area 450 x 340 square meters. All the hosts are thought to be equipped with an inbuilt energy model. They are all having initial energy of 100 Joule. Energy is assumed to be dissipated at the rate of x Joule per byte. This is a modification of the inbuilt Shortest Path Map Based Mobility of ONE Simulator. In the random Way Point model nodes proceed freely, but to make it more human-like some pattern need to be introduced. To amalgamate geographic restraints into mobility model, a predefined map is needed,and nodes are constrained to move along the pathways.One supports Helsinki town's map, which is presented in the Well Known Text formats. A node randomly chooses one of the directly connected map points to move to. The desired destination must be a location pointed on the map. On top of that, the mobile nodes move along the shortest pathway to the destination following Dijkstra's algorithm [Misra et al.(2016)Misra, Saha, and Pal]. There are 6 groups. Each node is assumed to be equipped with a router of the same type and is fitted with an energy model. The simulation ran for 43200 seconds. A transmission range and transmission speed of 50 meters of 250 kbps are set respectively. Interface is Bluetooth. The world size is set with the default dimension 4500 x 3400 square meters. The prime Post Disaster Rescue Operation is an instance of cluster-based mobility model. It is shown theoretically that cluster mobility model performs better than rest of the models in the field of mapping the human mobility in mission critical condition, where human moves in a team [Saha et al.(2011)Saha, Sheldekar, Mukherjee, Nandi et al.]. The area of the entire locality including all the four clusters is 4500 x 3400 square meters. Here, 4 groups are created. Each represents the following namely,Hospital(H),Rehabilitation centre(F), Rescue Camp(R) and the Disaster zone(D). Within each cluster, nodes are assumed to be pedestrians moving in speed of (0.5, 1.5) meters/second. They are all carrying mobile cell phones with chargeable battery in order to enable opportunistic communication among each other using Bluetooth interface.Carriers are incorporated to do to and fro movement between the groups. Their speed is varied and the outcome is observed accordingly. These vehicles are responsible for maintain-

Table 2: Common Simulation Setting

Simulator	*OneSimulator*
ParametersInitialization	$\alpha = 0.01; P_{init} = 0.75; \beta = 0.25; \gamma = 0.98$
No.ofinterfaces	1(*Bluetooth*)
UpdateInterval	0.1*sec*
Transmissionspeed	250*k*
TransmissionRange	50*m*
InitialEnergy	100*Joule*
TransmitEnergy	0.24*Jouleperbyte*
ScanEnergy	0.1*Jouleperbyte*
ScanResponseEnergy	0.1*Jouleperbyte*
EventGeneratorclass	*MessageEventGenerator*

Table 3: Simulation Setting using Random Way Point Model

No.of IoT − enablednodes	20
World's size	450*x*340*sq.m.*
MessageGenerationRate	7, 12
MessageSize	0.001*k*, 0.005*k*
EventSource/Destination	0, 4
BufferSize MessageTTL	5*M*
Simulationtime	10*min*
	10000*sec*, 20000*sec*

Table 4: Simulation Setting using Shortest Map Based Mobility Model

Noof HostGroups	6
No.of IoT − enablednodespergroup	100, 50, 100, 2, 2, 2
World's size	4500*x*3400*sq.m.*
MessageSize	(0.001 — 0.005)*k*, (0.005 - 0.010)*k*, (0.010 - 0.015)*k*
EventSource/Destination	0, 200
BufferSize	5*M*, 50*M*
MessageTTL	(10, 20, 30, 100, 150, 200)*min*
Simulationtime	43200*sec*

ing inter-cluster communication. They are also equipped with wireless cell-phones with Bluetooth ability.

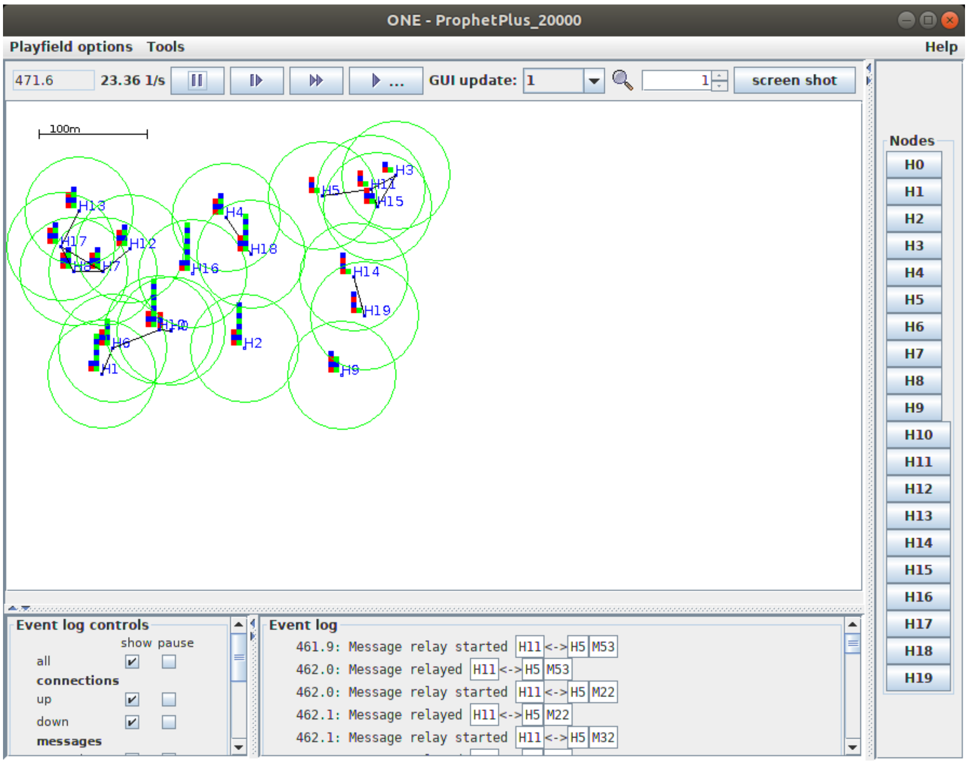
The screenshots of all three mobility models are shown in Figures **??**,**??** and **??** respectively.

4.2 Performance Metrics

The performance metrics which are considered to evaluate the protocols are: *Delivery Probability:* Number of delivered messages / Number of generated messages.
Overhead ratio: (Number of relayed messages-Number of delivered messages) / Number of delivered messages.
*Average Latency:*The mean of the time it takes for messages to reach their respective destinations.
Hop Count Average: The mean of the hops or steps taken by messages to reach their respective destinations.

Table 5: Simulation Setting using Cluster Based Mobility Model

NoofHostGroups	5(4staticgroupsand1carrier)
TransmissionRange	(10, 20, 30, 40, 50)m
No.ofIoT − enablednodesineachstaticgroup	25
No.ofIoT − enablednodesincarriers	10
SpeedofIoT − enablednodesinstaticgroup	(0.5, 1.5)m/s
SpeedofIoT − enabledcarriernodes	(0— 15, 15− 30, 30− 45, 45− 60, 60− 75)m/s
World'ssize	4500x3400*sq.m.*
MessageGenerationRate	(25, 120)*sec*
MessageSize	50*k*, 1*M*
EventSource/Destination	0, 100
BufferSize	(50, 100, 150, 200)*M*
MessageTTL	240*min*
Simulationtime	21600*sec*



```
461.9: Message relay started H11<->H5 M53
462.0: Message relayed H11<->H5 M53
462.0: Message relay started H11<->H5 M22
462.1: Message relayed H11<->H5 M22
462.1: Message relay started H11<->H5 M32
```

Fig. 1: Screenshot of Random Way Point mobility Model

4.3 Results and Discussion

4.3.1 Performance Evaluation based on Random Way Point Mobility Model

From Table-6, it is observed that when the simulation time is varied from 10000 seconds to 20000 seconds and with the above simulation parameters of Table-2 and Table-3, the delivery probability for all the protocols fall. However, in both cases, EPP always has an upper hand over PRoPHET

Table 6: Performance of the three routing applying Random Way Point Mobility Model

SimulationTime	*RoutingProtocol*	*DeliveryProb*	*OverheadRatio*	*LatencyAvg*	*HopCountAvg*
10000	*EPP*	0.0818	16.6813	181.5527	3.5604
	Prophet+	0.0746	11.2892	211.8157	3.012
	Prophet	0.0674	12.5333	193.0293	2.3467
20000	*EPP*	0.041	16.6813	181.5527	3.5604
	Prophet+	0.0374	11.2892	211.8157	3.012
	Prophet	0.0338	12.5333	193.0293	2.3467

and PRoPHET+ whenever delivery probability and latency average are considered. This means in relatively shorter time duration time and with higher chances, messages are being delivered by EPP.When overhead ratio and hop count average values are taken, it is visible that they are slightly higher in EPP with respect to the other two in both the scenarios.There is no visible change in the parameters except delivery probabilities because the energy dissipation rates are fixed in such a way that the IoT-enabled nodes are becoming powerless after 1000 seconds. So intuitively, if one increases the simulation end time limit, the delivery probabilities for all routing protocols would fall, while the other parameters would remain almost constant.

4.3.2 Performance Evaluation based on Shortest Map Mobility Model

1.Varying Message Size:
The simulation settings of Table-2 and Table-4 is used. From Table-7, it is observed that overhead ratio and delivery probability of EPP and PRoPHET+ fall drastically when message size exceeds 0.005 bytes, at fixed buffer space. On the hand, the delivery probability of PRoPHET remains almost constant throughout but it is also very less with respect the other two. The cause of the fall of EPP and PRoPHET+ is their dependencies on available buffer space. Each time before any routing decision is made, buffer occupancy of the next forwarder is checked, but this is not a concern of PRoPHET at all.Similarly, hop count average of EPP and PRoPHET+ converges to one. When no buffer is left, each IoT-based node directly tries to travel to the destination to deliver messages.Due to the same reason, the number of relay messages also decreases so as the delivered ones and hence consecutively the overhead ratio of EPP and PRoPHET+.It is concluded that almost due to the same reason the latency average of EPP and PRoPHET+ falls greatly. As number of relayed messages decreases considerably along with number of delivered ones, not much decision time is wasted for eligibility checking purpose of candidates. From this point on wards sender directly delivers the message to the destination and relatively quicker.

2.Varying Message TTL:
From Table-8, it is clear that since message Time-to-Live threshold is kept low and big message size range (5k-10k) is given. In spite of a large number of message creation, every time number of messages delivered is very less in case of both PRoPHET+ and EPP and is slightly better in PRoPHET. In real life scenario, if the simulation is run for 12 hours, message size might be as large as here but message TTL is not this small. For example, in the custom default setting itself, message TTL is fixed at 300 minutes.It is observed here(from the hop count average column) that EPP and PRoPHET+ behave like direct delivery routing algorithm. Overhead is also zero. Whatever messages are relayed are surely delivered. Random Way Point mobility model does not follow any probabilistic pattern.It does not depict vehicular movement or human-like mobility and predictability oriented

Table 7: Performance of the three routing applying Shortest Map Based Mobility Model: Varying Message Size

MessageSize	*RoutingProtocol*	*DeliveryProb*	*OverheadRatio*	*LatencyAvg*	*HopCountAvg*
0.001,0.005	*EPP*	0.0096	207.5435	314.7978	4.5
	PRoPHET+	0.0079	168.8684	308.1605	3.9737
	PRoPHET	0.0035	52.8941	264.9235	2.3529
0.005,0.010	*EPP*	0.0092	212.5227	309.2205	4.3864
	PRoPHET+	0.0079	160.0263	308.1737	4.0263
	PRoPHET	0.0035	52.2941	264.9353	2.3529
0.010,0.015	*EPP*	0.0092	206.9773	309.3159	4.4091
	PRoPHET+	0.0077	154.5135	304.2514	4.0541
	PRoPHET	0.0035	52.2941	264.9353	2.3529

Table 8: Performance of the three routing applying Shortest Map Based Mobility Model: Varying Message TTL

MessageTTL	*RoutingProtocol*	*DeliveryProb*	*OverheadRatio*	*LatencyAvg*	*HopCountAvg*
10	*EPP*	0.0013	0	217.65	1
	PRoPHET+	0.0013	0	217.65	1
	PRoPHET	0.0033	47.5	299.0813	2.5625
20	*EPP*	0.0013	0	217.65	1
	PRoPHET+	0.0013	0	217.65	1
	PRoPHET	0.004	49.6316	396.6316	2.9474
30	*EPP*	0.0013	0	217.65	1
	PRoPHET+	0.0013	0	217.65	1
	PRoPHET	0.004	49.6316	396.6316	2.9474
100	*EPP*	0.0013	0	217.75	1
	PRoPHET+	0.0013	0	217.75	1
	PRoPHET	0.004	49.6316	396.6316	2.9474
150	*EPP*	0.0013	0	217.65	1
	PRoPHET+	0.0013	0	217.65	1
	PRoPHET	0.0013	0	217.65	1
200	*EPP*	0.0013	0	217.65	1
	PRoPHET+	0.0013	0	217.65	1
	PRoPHET	0.004	49.6316	396.6316	2.9474

routing algorithms are designed keeping group-based and/or pattern-based movement notion. Even a map-based movement might not give expected results for example, in the above given scenario. Simulation results are highly influenced by simulator parameters and how much these attributes and their values are relevant to practical essence. The actual applicability of the any designed routing algorithm should be specified first during design and requirements elicitation process.

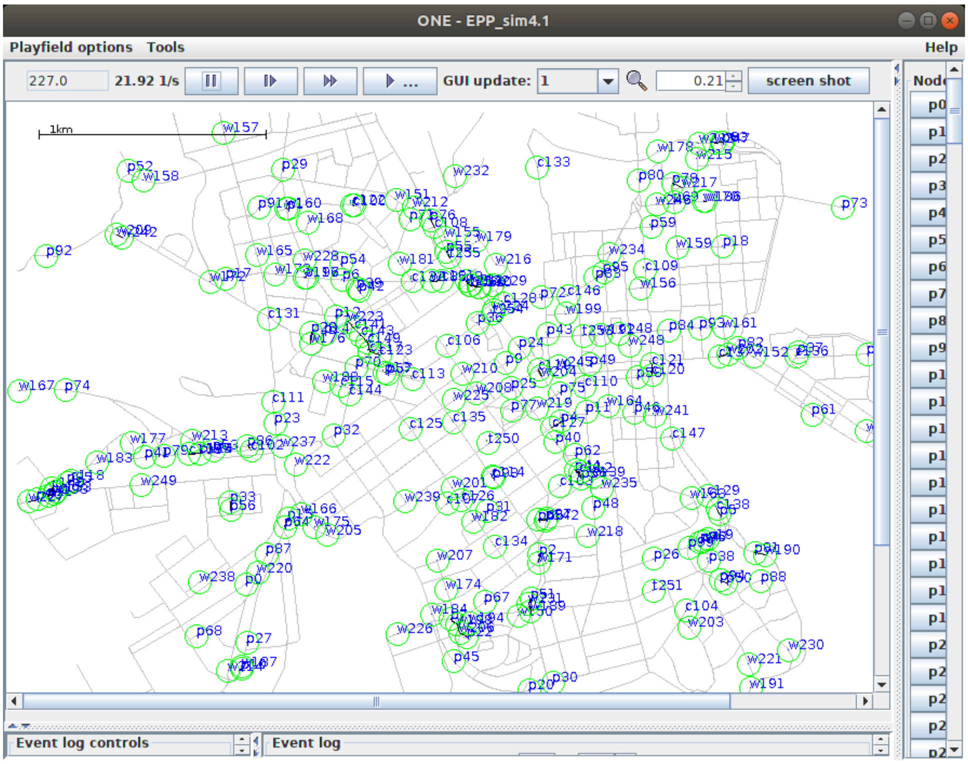


Fig. 2: Screenshot of Shortest Map based Mobility Model

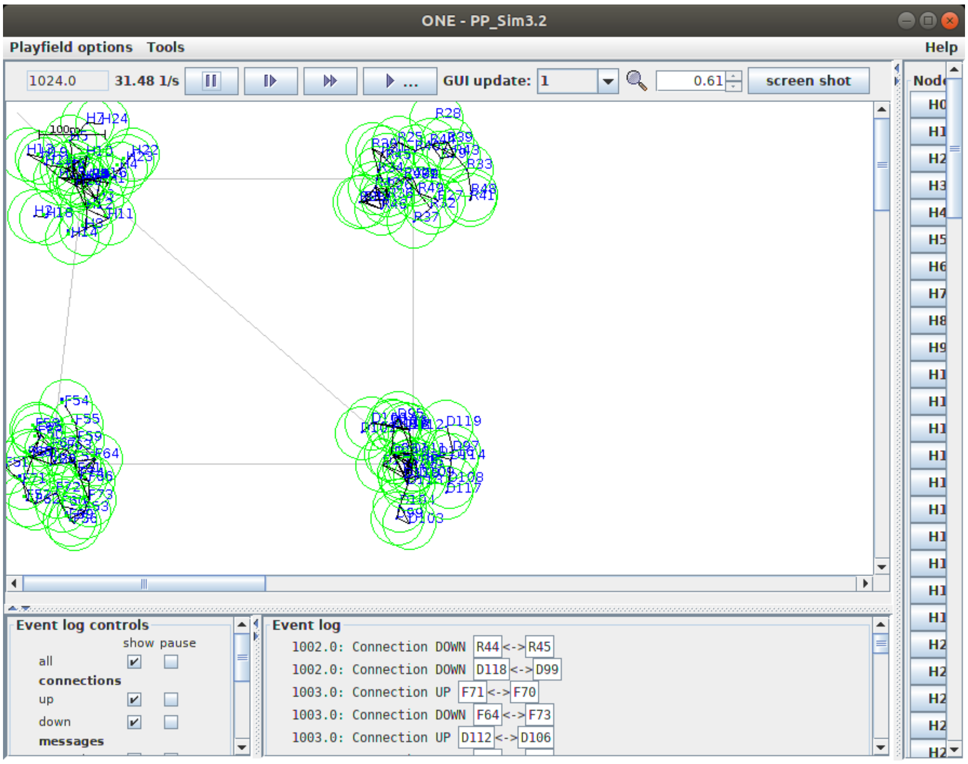
4.3.3 Performance Evaluation based on Cluster Mobility Model: a use case of Post Disaster Rescue Operation

1. Varying the Buffer Size:

Transmission range and Buffer capacity were chosen to determine the relationship of the routing algorithms on the attributes that are device dependent [Saha et al.(2011)Saha, Sheldekar, Mukherjee, Nandi et al.]. Particularly in a post-disaster rescue operation, message format could be assumed to be fixed hence of the same size and should be preferably short, simple and precise. The number of generation of such messages could be enormous, so buffer space should be sufficiently “store” these bundles to “carry forward”.From Fig-4 a and b, it is observed that the Delivery Probability and Hop count average follow almost the same trend as the buffer size of all IoT-enabled nodes increases uniformly from 50M to 200M. The 50M to 100M range of buffer size is standard for battery-driven wireless mobile devices. Within this range, EPP outperforms the other two in terms of maintaining an optimal balance between Delivery Probability and Hop count Average value. By Fig-4c, it is observed that the latency average of EPP is higher than that of PRoPHET+ and PRoPHET individually but is an inherent property of any intermittently connected network following store-carry-and-forward mechanism.

2. Varying the Transmission Range:

In all the simulation Bluetooth interfacing is used. WiFi could have been another alternative, but we chose the former pressing on the notion that almost all devices whether PDA, cell phones, messaging



```
1002.0: Connection DOWN R44<->R45
1002.0: Connection DOWN D118<->D99
1003.0: Connection UP F71<->F70
1003.0: Connection DOWN F64<->F73
1003.0: Connection UP D112<->D106
```

Fig. 3: Screenshot of Cluster Based Mobility Model:Post Disaster Rescue Operation

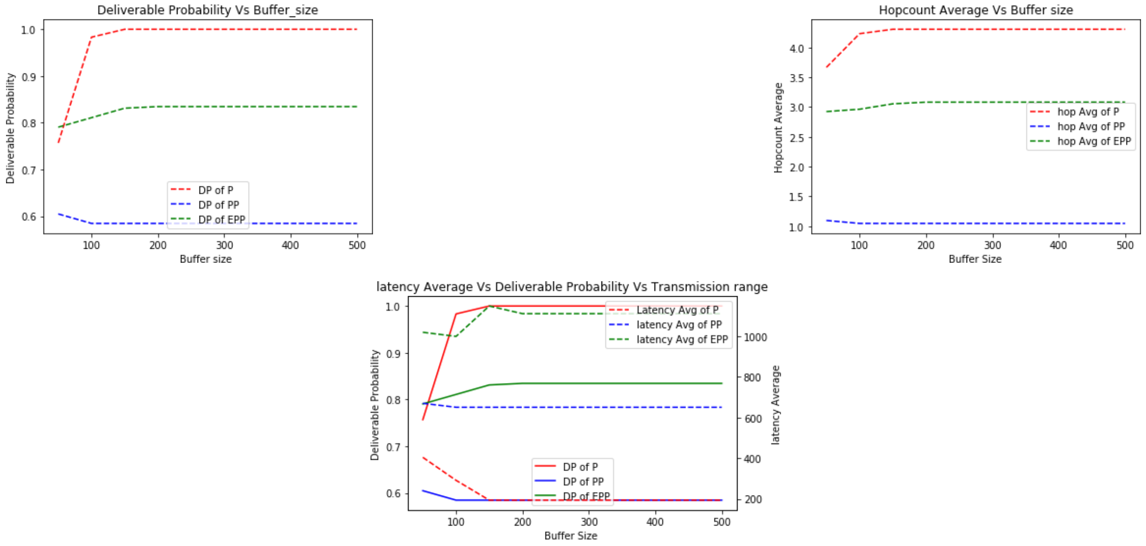


Fig. 4: Buffer Size Vs Performance metrics.

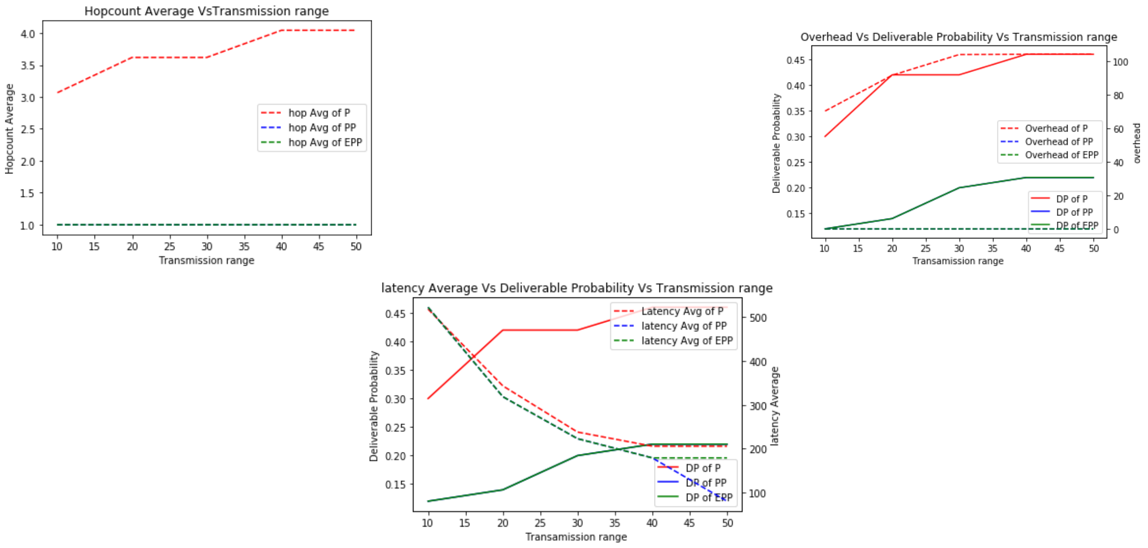


Fig. 5: Transmission Range Vs Performance metrics.

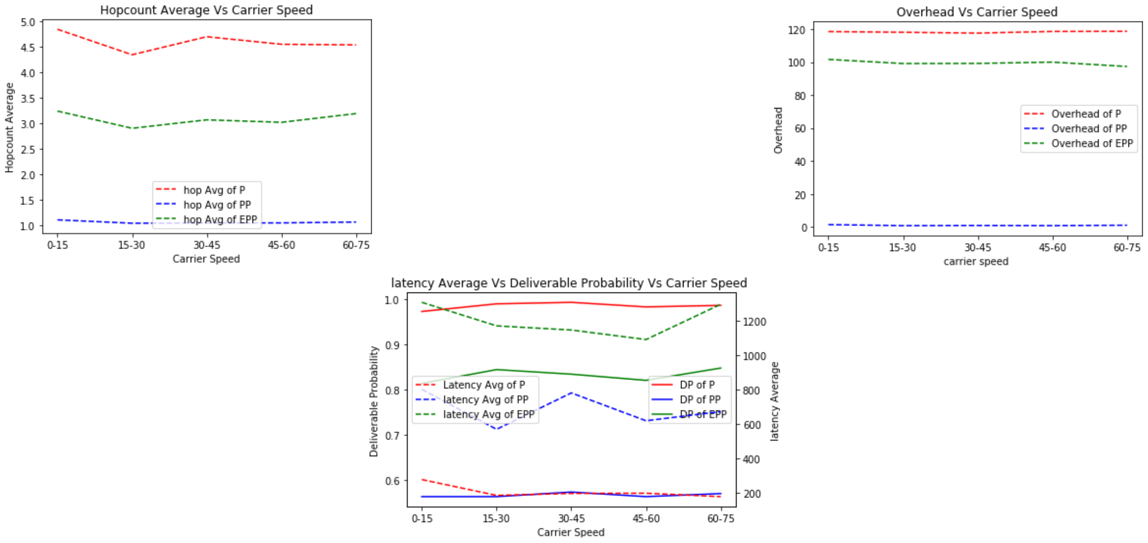


Fig. 6: Carrier Speed Vs Performance metrics.

devices, etc. might not be WiFi-enabled but are always Bluetooth enabled. In general, transmission range of Bluetooth can be as high as 100 meters (for Class I) and as low as below 10 meters (for Class III). Most of the devices have a range of around 10 meters (Class II).The transmission range is varied from 10 meters to 50 meters, assuming including most of the Bluetooth devices. From Fig-6a and b, it is clear that although the Delivery Probability of PRoPHET is higher but takes an inevitable toll on the Overhead Ratio and Hop count Average. Delivery Probabilities of all three protocols gradually improve with the increase in transmission range. Due to the high energy consumption rate, the

IoT-enabled nodes become powerless just after 2100 seconds, hence to adhere with the practicality of the phenomenon, simulation end time is set to 3600 seconds. It is clear that Overhead Ratio of both EPP and PRoPHET+ is zero because whatever messages could be relayed are all delivered. The IoT-enabled nodes could sense this even while started relaying as EPP and PRoPHET both are designed to do so. This means the power requirements and sufficiency are verified along with contact opportunity before forwarding the message to any selected candidate. This was not in the scope of PRoPHET at all. From Fig-6a, it is noted that Latency Average of the routing algorithms was also high initially, which reduces as the transmission range increases. Since most of the IoT-based nodes whether internal or carriers are mobile within a predefined region, low transmission range and speed mean fewer chances to complete full relaying of any message bundle. Thus, while keeping the transmission speed constant and increasing the transmission range overall improves the performance. In terms of Latency Average too, EPP and PRoPHET+ outperform ProPHET. The reason behind this is very less number of messages are actually relayed and delivered and fewer hop counts. As a result of which even including the computation cost for routing decision, EPP and PRoPHET+ have less latency.It becomes obvious that if transmission range further increases or set to the standard value of 100 meters then EPP would perform very well. This would not come free of cost, as a higher transmission range means more energy consumption rate.

3. *Varying the carrier velocity:*

Mobility of nodes is used in Delay Tolerant Network for transmitting the message from source to destination. Node velocity is a very important factor during Post Disaster Management. Here, varying the Carrier node velocities and realistic human walking of 1-5 Km/hr is considered [Saha et al.(2011)Saha, Sheldekar, Mukherjee, Nandi et al.].From Fig-**??**, it is observed that the Overhead Ratio and Latency Average deteriorates as the velocity of the carriers are increased owing to quicker delivery of messages. Specifically, EPP outperforms ProPHET+ and PRoPHET when all these metrics are taken together into account. After reaching an optimal value, the Delivery Probability happens to fall because as the nodes gain speed, messages are transmitted to the adjacent clusters in short span of time.After all this analysis, it can be concluded that EPP outperforms PRoPHET+ in most of the scenarios in context of Delivery Probability. Delivery Probability of PRoPHET might seem better than EPP but it performs worst in terms of Overhead Ratio and Hop count Average.The PRoPHET does not look into the state of various physical attributes of the mobile hosts and the messages which are very well taken into consideration by both EPP and PRoPHET+. PRoPHET+ also skips certain important determining factors which are mostly covered by EPP and this also comes with a cost on Overhead Ratio and Latency Average.Hence, it can be proved that EPP maintains high Delivery Probability while optimally balancing Overhead Ratio, Hop count Average and Latency Average.

5 Conclusion

In this paper, we propose predictability based Enhanced PRoPHET+ protocol (EPP) for fault-tolerant routing in intermittently connected networking scenario. EPP considers participation history of IoT-enabled nodes, success ratio, message TTL, and distance between IoT-based nodes for forwarding message. Post disaster rescue operation is considered as a use case for simulation. Experimentation results show that EPP outperforms the baselines. This is because EPP incorporates all real-world decision parameters and does not rely only on history based encounters. We plan to extend this work in future and apply EPP protocol to Intrusion Detection and Response System. We also plan to incorporate real sensors and implement the real-time hardware model of EPP.

Conflict of interest

The authors declare that they have no conflict of interest.

Acknowledgments

This work is supported by DST Inspire (IF170577), Government of India.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

[Bansal et al.(2019)Bansal, Gupta, Sharma, and Gambhir] Bansal A, Gupta A, Sharma DK, Gambhir V (2019) Iicar-inheritance inspired context aware routing protocol for opportunistic networks. Journal of Ambient Intelligence and Humanized Computing 10(6):2235–2253

[Basu et al.(2018)Basu, Biswas, Roy, and DasBit] Basu S, Biswas A, Roy S, DasBit S (2018) Wise-prophet: a watch-dog supervised prophet for reliable dissemination of post disaster situational information over smartphone based dtn. Journal of Network and Computer Applications 109:11–23

[Boudguig and Abdali(2013)] Boudguig M, Abdali A (2013) New dtn routing algorithm. International Journal of Computer Science Issues (IJCSI) 10(2):82

[Dhurandher et al.(2016)Dhurandher, Borah, Woungang, Sharma, Arora, and Agarwal] Dhurandher SK, Borah S, Woungang I, Sharma DK, Arora K, Agarwal D (2016) Edr: An encounter and distance based routing protocol for opportunistic networks. In: 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), IEEE, pp 297–302

[Dhurandher et al.(2017)Dhurandher, Kumar, and Obaidat] Dhurandher SK, Kumar A, Obaidat MS (2017) Cryptography-based misbehavior detection and trust control mechanism for opportunistic network systems. IEEE Systems Journal 12(4):3191–3202

[Ekman et al.(2008)Ekman, Keränen, Karvo, and Ott] Ekman F, Keränen A, Karvo J, Ott J (2008) Working day movement model. In: Proceedings of the 1st ACM SIGMOBILE workshop on Mobility models, ACM, pp 33–40

[Keränen et al.(2009)Keränen, Ott, and Kärkkäinen] Keränen A, Ott J, Kärkkäinen T (2009) The one simulator for dtn protocol evaluation. In: Proceedings of the 2nd international conference on simulation tools and techniques, ICST (Institute for Computer Sciences, Social-Informatics and . . . , p 55

[Lin et al.(2015)] Lin Z, et al. (2015) Augmenting mobility simulation by public transport: A case study for the one simulator. PhD thesis, Alto University

[Lindgren et al.(2004)Lindgren, Doria, and Schelen] Lindgren A, Doria A, Schelen O (2004) Probabilistic routing in intermittently connected networks. In: International Workshop on Service Assurance with Partial and Intermittent Resources, Springer, pp 239–254

[Misra et al.(2016)Misra, Saha, and Pal] Misra S, Saha BK, Pal S (2016) Opportunistic Mobile Networks: Advances and Applications. Springer

[Mitchener and Vadhat(2000)] Mitchener W, Vadhat A (2000) Epidemic routing for partially connected ad hoc networks. Tech. rep., Technical Report CS-2000-06, Duke Univ

[Prodhan et al.(2011)Prodhan, Das, Kabir, and Shoja] Prodhan A, Das R, Kabir H, Shoja G (2011) Ttl based routing in opportunistic networks. J Network and Computer Applications 34:1660–1670, DOI 10.1016/j.jnca.2011.05.005

[Saha et al.(2011)Saha, Sheldekar, Mukherjee, Nandi et al.] Saha S, Sheldekar A, Mukherjee A, Nandi S, et al. (2011) Post disaster management using delay tolerant network. In: Recent Trends in Wireless and Mobile Networks, Springer, pp 170–184

[Samanta et al.(2018)Samanta, Kumari, Deb, Bose, Cortesi, and Chaki] Samanta R, Kumari C, Deb N, Bose S, Cortesi A, Chaki N (2018) Node localization for indoor tracking using artificial neural network. In: 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), IEEE, pp 229–233

[Sharma et al.(2016)Sharma, Dhurandher, Woungang, Srivastava, Mohananey, and Rodrigues] Sharma DK, Dhurandher SK, Woungang I, Srivastava RK, Mohananey A, Rodrigues JJ (2016) A machine learning-based protocol for efficient routing in opportunistic networks. IEEE Systems Journal 12(3):2207–2213

[Sharma et al.(2019)Sharma, Dhurandher, Agarwal, and Arora] Sharma DK, Dhurandher SK, Agarwal D, Arora K (2019) kROp: k-Means clustering based routing protocol for opportunistic networks. Journal of Ambient Intelligence and Humanized Computing 10(4):1289–1306, DOI 10.1007/s12652-018-0697-3, URL http://dx.doi.org/10.1007/s12652-018-0697-3

[Spyropoulos et al.(2005)Spyropoulos, Psounis, and Raghavendra] Spyropoulos T, Psounis K, Raghavendra CS (2005) Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In: Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking, ACM, pp 252–259

[Tanwar et al.(2018)Tanwar, Tyagi, Kumar, and Obaidat] Tanwar S, Tyagi S, Kumar N, Obaidat MS (2018) La-mhr: Learning automata based multilevel heterogeneous routing for opportunistic shared spectrum access to enhance lifetime of wsn. IEEE Systems Journal 13(1):313–323