IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received December 29, 2016, accepted January 14, 2017, date of publication April 4, 2017, date of current version May 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2690341

Store-Carry-Cooperative Forward Routing With Information Epidemics Control for Data Delivery in Opportunistic Networks

CHERRY YE AUNG[1], (Student Member, IEEE), IVAN WANG-HEI HO[2], (Member, IEEE), AND PETER HAN JOO CHONG[3], (Member, IEEE)

[1]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, 639798
[2]Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Kowloon, Hong Kong
[3]Department of Electrical and Electronic Engineering, Auckland University of Technology, Auckland 1010, New Zealand

Corresponding author: Cherry Ye Aung (cherryaung@ntu.edu.sg)

The work of I. W.-H. Ho was supported by the Early Career Scheme, University Grant Committee of the Hong Kong Special Administrative Region, China, under Project 25200714.

ABSTRACT Data delivery in opportunistic networks requires robustness and resiliency due to the mobility and probabilistic propagation channels caused by fading. Besides the 100% data delivery, delivery with minimum delay, overhead, buffer consumption, and controlling unnecessary transmissions/replications are equally important. In this paper, we propose a data delivery solution for opportunistic networks. The solution comprises two main algorithms: store-carry-cooperative forward routing and information epidemic control. In the data forwarding, nodes proactively monitor and exploit the direct/two-hop cooperative forwarding opportunities and adaptively switch between the cooperative forwarding and reactive store-carry-forward routing. An information epidemics control algorithm, which provides earlier control signal distribution time and faster recovery rate, is also proposed. The susceptible-infected-recovered model is used to study the effectiveness of the proposed mechanism. Extensive network performance evaluation is conducted under a wide range of scenarios, which include fading environments, obstacle-constrained environments, and mobile social network environments. We show that: 1) the information epidemics control mechanism provides higher vaccination rate and recovery rate; 2) proactive replication incurs a number of unnecessary transmissions; 3) monitoring the vicinity and exploiting the opportunity shorten the data delivery delay; and 4) with the integrated solution, a robust data delivery is achieved and a substantial amount of unnecessary transmissions are well deterred.

INDEX TERMS Opportunistic networks, cooperative forwarding, broadcast, store-carry-forward, information epidemics control.

I. INTRODUCTION

Opportunistic networks are a form of mobile ad hoc networks (MANET) where the network topology is composed of opportunistic and unreliable links. Some applications of opportunistic networks include disaster recovery networks, military networks, and mobile social networks. For such networks, end-to-end routing is shown to be inefficient for data delivery due to opportunistic links and dynamic topology. The store-carry-forward (SCF) based approach has become a conventional data forwarding mechanism in such networks [1]–[3].

It has been shown that SCF routing can achieve eventual data delivery for opportunistic networks [2]. In SCF routing, a node with a lower ID proactively sends its summary vector to its contact node and each node in turn gets the copies of messages it has not yet seen from the other. The nodes keep the copies and replicates whenever there is a contact opportunity. Due to the lack of the data delivery information, a node will try to replicate the packet to all the neighboring nodes it encountered [8]. Therefore, massive packet replications are inevitable in SCF routing. Moreover, it is possible that the destination node is in the vicinity of the node holding the copies under some network situation. So, simply replicating with all the neighboring nodes causes unnecessary transmissions and may lead to longer delivery delay.

Several packet discarding strategies have been proposed to control and eradicate the spread of packet copies in networks [23]. The VACCINE recovery scheme is shown to be the most effective recovery scheme in the existing works [23]–[25]. By using VACCINE (anti-packet), susceptible node will become immuned and infected node will become recovered and will not infect other susceptible nodes when it receives the anti-packet.

In addition to mobility, the presence of stationary and mobile scatterers in the environment results in fading in the network, which further incapacitates the contact opportunities [3]. Most routing protocols in MANET and opportunistic networks did not consider the impact of fading caused by stationary and mobile scatterers on the network performance. Instead, most existing protocols evaluate the performance based on the deterministic modelling of the propagation channel.

Cooperative forwarding is shown to be an efficient routing mechanism in static and mobile wireless networks under fading environments [5]–[7]. It takes into account the probabilistic nature of wireless channel. In this forwarding, one or more forwarding nodes are located in between the source and destination nodes that are not in contact. It broadcasts the data packet over the air and the relay nodes forward the packet in a cooperative fashion to the destination node. This is in contrast to generic unicast forwarding used in traditional routing. In mobile environment, this type of forwarding requires nodes position information or complete network topology information prior to the data delivery process. Therefore, this type of forwarding cannot be directly applied in opportunistic networks.

As discussed above, network topology can change dramatically due to mobility and probabilistic propagation channels caused by fading. As a result, it is hard to predetermine the network scenario as the node density could change drastically at any point of time. Hence, adaptive routing which is robust to different network scenarios and provides highest data delivery with minimum delivery delay, overhead, buffer consumption, and packet transmissions is needed.

In this paper, we propose a network layer solution called store-carry-cooperative forward (SCCF) routing with information epidemics control. It aims to solve long delivery delay problem and information epidemic problem for opportunistic networks where the lack of infrastructure, high mobility, unstable link connectivity, fading, and obstacle-constrained environments are the major concerns on the data delivery performance. The major contribution of this paper is summarized as follows.

1) We propose an adaptive data forwarding algorithm where nodes proactively monitor the direct/two-hop cooperative forwarding opportunities and deliver the data packet. The nodes adaptively switch between the cooperative forwarding and SCF forwarding based on the contact opportunity. The SCF forwarding here is reactive in which nodes replicate the packet copies only when the message has never been forwarded by cooperative forwarding.
2) We propose an information epidemics control algorithm where nodes continuously monitor the broadcast-based cooperative transmissions over the air. The nodes then translate the information overheard into packet states and then build the knowledge base for the packet delivery progress. This knowledge is used to deter packet infections and vaccinate others from being infected.
3) We study the effectiveness of the proposed solution based on the susceptible-infected-recovered (SIR) model and show that it provides higher vaccination rate and recovery rate. Due to the flexibility of the proposed scheme, it can also be integrated with any SCF-based routing.
4) We first study the network performance by varying network densities. We then evaluate it in relatively sparse and hostile environments where we study the effect of different fading distributions, varying mean speed, obstacles, and social contact patterns.

The rest of the paper is organized as follows. Section II reviews related work on routing and information epidemics control schemes. The overview of the proposed scheme is provided in Section III. Section IV presents the link awareness approach. The proposed routing scheme with several protocol details are presented in Section V. The proposed vaccinating algorithm and the integration with the data forwarding module is discussed in Section VI. Section VII discusses the susceptible-infected-recovered model for information epidemics in the network. Section VIII evaluates the network performance. The concluding remarks are provided in Section IX.

II. RELATED WORK

A. ROUTING

Extensive research on routing in mobile wireless networks has been carried out. These includes end-to-end routing [4], cooperative forwarding [6], [7], and SCF routing [8]–[22]. The summary of the related works is also given in Table 1.

Cooperative forwarding differs from end-to-end routing in the sense that it takes into account the unreliable nature of wireless channel [3]. It utilizes broadcast wireless nature and combines several weak/unreliable links to make a reliable communication link. It has been shown that it provides a resilient data delivery for networks with adverse wireless links. However, it requires topology information using proactive source routing or position information to locate the destination. CORMAN [6] is one of the first cooperative forwarding protocols proposed for mobile networks. In CORMAN, it was shown that fading can dramatically jeopardize the network performance. Although the efficacy of exploiting cooperative opportunistic forwarding under fading environment was demonstrated, there is a performance drop when the network connectivity becomes intermittent.

In contrast to end-to-end routing and cooperative forwarding, SCF-based routing does not locate the destination node. Instead, it uses available contact opportunities and replicates the copies whenever there is a contact. Exploiting the node's mobility, the relay nodes are expected to have contact with

TABLE 1. Summary of related work.

Protocol	Network type	Routing type	Addressing mode	Information epidemics control approach
CORMAN [6]	MANET	Cooperative forwarding over the pre-determined shortest paths.	broadcast	N.A
POR [7]	MANET	Position-based cooperative forwarding.	broadcast	N.A
ER [8]	Opp Net	SCF forwarding.	unicast	Self-healing
Spray and Wait [9]	Opp Net	SCF. Nodes spread message copies to L distinct relays. Each node carrying a copy performs direct transmissions.	unicast	Self-healing. Limit the no. of copies.
(p,q) ER [10]	Opp Net	Direct, two-hop, probabilistic, and epidemic forwarding based on randomly generated probabilities p and q.	unicast	VACCINE
Multi-spreader [11]	Opp Net	SCF. Limit the max number of spreaders replicating the copies.	unicast	VACCINE
PER [12]	Opp Net	SCF. Replicate the packets to nodes which has lowest-cost route to the destination.	unicast	Self-healing
DTN+MANET [13], [14]	Opp Net	Forward the packets over the end-to-end path if there is or use SCF otherwise.	unicast	VACCINE
DTN+MANET [15]	Opp Net	Send/forward the packets when there is a route or store otherwise.	unicast	N.A
HYMAD [16]	Opp Net	End-to-end routing within group and SCF forwarding between group.	unicast	Self-healing
G-ER [17]	Opp Net	End-to-end routing within group and SCF forwarding between group.	unicast	Self-healing. Keep only one copy in each group.
GAR [18]	Opp Net	Quota-based SCF approach. To minimize the delay, neighbours store and carry the overheard packets if the buffer space is available.	broadcast	Self-healing. Limit the no. of copies.
OOF [19]	Opp Net	Replicate the packet only if the joint delivery probability of two copies is greater than that of single copy.	unicast	Self-healing. Limit the no. of copies.
R3 [20]	Opp Net	Replicate the packets over the pre-determined multi-paths.	unicast	Control the no. of paths.
Vicinity-aware routing [21]	Opp Net	WAIT for multi-hop opportunities and forward the packets when available.	unicast	N.A
TCC-aware routing [22]	Opp Net	Multi-hop communications inside TCC and SCF forwarding outside TCC.	unicast	Self-healing. Replicate to nodes with higher forwarding metric.

the destination at some point and deliver the packet. As it only relies on the contact node information, this type of routing is robust to intermittent network connectivity and can guarantee eventual data delivery.

Epidemic routing [8] is the first SCF routing protocol, which is robust to link losses and network disconnection. However, it has been shown that massive packet replications and unnecessary buffer consumption are inevitable in this scheme. To control the packet replications (also known as the forwarding cost), some protocols limit the number of copies made for a packet or the number of hops a packet traverses [9]–[11], [18].

In (p, q) epidemic routing [10], packets are forwarded blindly in a probabilistic manner. Two randomly generated probabilities p and q are used to decide to forward/replicate a packet by direct, two-hop, probabilistic, and epidemic forwarding approaches. These schemes show that the number of packet copy transmissions can be controlled by limiting the spreaders/forwarders. However, it can be observed that the message delivery delay is higher compared to the epidemic routing in those schemes. In [18], a quota-based approach is proposed to control the forwarding cost, where it limits the number of copies allowed to be made for each packet. IEEE 802.11 broadcast mode is used and therefore, neighbour nodes are also able to receive the copy, which will then store and carry if the buffer space is available so as to minimize the delivery delay. However, in pervasive network, it is unlikely to predetermine the optimal value for quota as the value is very much dependent on network density and connectivity. So, using more quota will approach the forwarding cost of the flooding-based forwarding and less quota will cause longer delivery delay.

Some adaptive routing schemes which are the integration of SCF routing (also called delay tolerant network (DTN) routing) and multi-hop unicast routing (also called end-to-end routing) have been proposed for opportunistic networks. In [13] and [14], nodes find the end-to-end path and forward the data packet. SCF-based forwarding is used when the end-to-end connection breaks. It uses the node density and velocity to decide switching between the multi-hop unicast forwarding and the SCF forwarding. It assumes that all nodes in the network have the same communication range and determines the density based on the number of one-hop neighbours.

Similar to [14], HYMAD [16] is also a hybrid DTN-MANET routing protocol, which uses multi-hop unicast routing to forward messages within cluster/group and uses SCF routing to forward messages between groups. In G-ER [17], it treats a group of connected nodes as an individual node. A packet will be replicated only once to each group no matter how many nodes are within the group to alleviate the buffer occupancy. Both HYMAD and G-ER consider the scenario where groups of nodes are scattered in the network and the connectivity within a group is fairly stable while the inter-group connectivity is intermittent. Another hybrid MANET-DTN approach [15] showed the benefits of integrating the SCF mechanism into a proactive MANET routing protocol. In this protocol, it stores the data packet when there is no end-to-end path or sends the packet if it finds a route. However, this scheme can incur large delay as it lacks a mechanism to push forward data delivery under the cases where no end-to-end path can be found.

Moreover, there exists some other recent adaptive routing schemes for networks with diverse connectivity characteristics. In [19], a message is replicated to a node only if the joint delivery probability of two copies is greater than the delivery probability of a single copy. It assumes known knowledge about long-term intermeeting times between nodes and computes delivery probabilities based on the knowledge. In [20], multiple forwarding paths are selected and data copies are forwarded along the predetermined multiple paths. In [21], it highlights the importance of being aware of nodes' vicinity on the delivery delay. The WAIT forwarding strategy is discussed where nodes wait for the end-to-end transmission opportunities and forward data packets using multi-hop transmissions. Similar to [21], the existence of transient connected components (TCC) in the network is also highlighted in [22]. Packets are replicated to nodes with higher forwarding metric using multi-hop communications.

Data delivery in social delay-tolerant networking has also been discussed in recent works [33], [34]. These works focus on community formation and aggregation in the network. In [34], a replica of the data packet is forwarded to nodes with higher centrality values than the current node. Forwarding nodes are selected based on the node centrality and community labels. Upon delivering the copy to a member of the destination community, the original carrier discards the message from its buffer to prevent it from further dissemination. The member node will replicate other members with higher local centrality until the message is delivered to the destination. Similarly, in [33], nodes which are located between communities, also known as bridge nodes, are first identified and then data copies are forwarded to those bridge nodes. Inter-community multi-copy and intra-community single-copy mechanism is used to minimize the forwarding cost.

Most existing adaptive routing protocols for opportunistic networks combine multi-hop unicast routing and SCF-based routing. In those approaches, nodes wait/discover for the multi-hop opportunities and use SCF if there is no multi-hop route. The route discovery process of multi-hop unicast forwarding involves sending route request message in network-wide manner or to some specific number of hops, sending route reply, building the routing table, maintaining the routes, and discarding the erroneous routes. The advantage of using multi-hop unicast forwarding approach is that if the nodes are connected in the network with reliable links, it provides the delivery in shortest possible time. However, it has been said that the multi-hop unicast routing approaches do not adapt well to the dynamic wireless environment variations and the protocols may suffer from the high cost of multi-hop contacts discovery and the high risk of using outdated information [3]. Hence, for the network with mobility, fading, and obstacle-constrained nature, the data delivery using such approach will be unreliable. Moreover, it is also hard to predetermine the switching point between the two approaches in such dynamic environment.

In contrast to the existing works, the proposed solution proactively monitors the two-hop vicinity and does not require to have multi-hop routes/contacts discovery. It forwards the data packets by broadcast-based cooperative forwarding whenever there is an opportunity in the vicinity. Proactive monitoring of two-hop vicinity gives the node the need to switch between the broadcast-based cooperative forwarding and the SCF forwarding adaptively and instantly. In addition, by limiting to two-hop, the protocol does not incur high overhead cost and has less risk of using outdated information. It is also noted that making use of two-hop vicinity tremendously reduce the waiting time compared to the direct delivery [21]. Nodes reactively replicate the packet copies only when there is no opportunity and the packet has never been forwarded by cooperative forwarding. This replication will in turn cause more nodes become involve in seeking the opportunities in the vicinity, and hence, ensures faster data delivery. Moreover, overhearing the cooperative transmissions over the air provides the node the ability for better information epidemics control. By having the adaptive routing capability and the information epidemics control, the proposed solution works well in highly dynamic MANET and opportunistic networks where the lack of infrastructure, high mobility, unstable link connectivity, fading, and obstacle-constrained environment are the major concerns on the data delivery performance.

B. INFORMATION EPIDEMICS CONTROL

Recovery schemes for controlling the spread of packet replications were proposed in [23]. *IMMUNE (self-healing)* and *VACCINE* are the two most commonly used packet discarding strategies for information epidemics control in opportunistic networks. The VACCINE recovery scheme is shown to be the most effective one in the existing works [23]–[25]. In *VACCINE*, a node maintains information of packets which have been successfully delivered to the destination node in addition to information of packets it has received so far in a list. This list is exchanged between two nodes to avoid sending duplicates and the packet that has been delivered to the destination. In SCF-based routing, a vaccine is generated for a packet when the destination node receives the packet or when a node receives an ACK from the destination node upon delivering the packet.

Analogy to the epidemiology, the SIR model has been widely used for analysis of information dissemination in the network [23]–[25]. In the SIR model, a packet is considered as one infectious disease. A node is said to be susceptible if it does not have a copy of that packet. A node is said to be infected when it receives a packet copy. A node becomes recovered when it successfully delivers the packet to the destination node or receives the anti-packet.

In the existing information epidemics control approaches, a vaccine is generated only when a node successfully delivers a packet to the destination. However, in opportunistic links

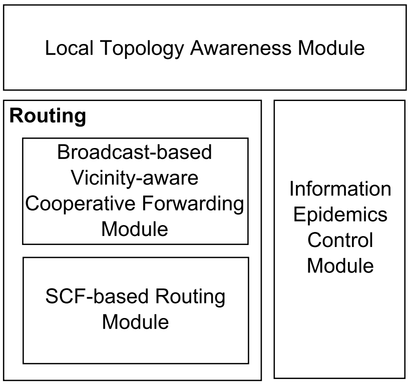


FIGURE 1. Network layer architecture.

and dynamic topology environments, due to the effect of mobility and fading, having a direct contact with the destination is scarce. This results in late information epidemics control and more infections. In this paper, we propose a vaccinating scheme which provides early control signal distribution, and hence leverage the information epidemics control in the network. The proposed vaccinating scheme is integrated with the data forwarding algorithm. Due to the flexibility of the scheme, it can also be integrated with any SCF-based routing.

III. OVERVIEW OF SCCF

In this paper, we propose a data delivery solution for networks where the lack of infrastructure, high mobility, unstable link connectivity, fading, and obstacle-constrained environments are the major concerns on the data delivery performance. The proposed solution does not require any information in advance. The illustration of network layer architecture is shown in Fig. 1. The basic idea is 1) deploying the local topology awareness and vicinity-aware cooperative forwarding on top of the SCF routing; 2) reactively replicate the packet copies only when the message has never been forwarded by cooperative forwarding; and then 3) incorporating the vaccinating module which deters packet infections and vaccinate others from being infected.

In SCCF data forwarding, five different types of data forwarding are defined. They are *direct, two-hop, forwarder, forwarder-by-chance,* and *replicate*. SCCF uses broadcast transmission for the first four forwarding types and unicast for the *replicate* type. A node inserts the respective data forwarding type in the data packet header before it forwards the packet. This information is used to inform the nodes receiving or overhearing the packet so that they can process accordingly. Fig. 2 and Fig. 3 illustrate how respective forwarding types are used in SCCF. Section V details the SCCF data forwarding algorithm.

In SCCF vaccinating, nodes maintain a packet state vector inside which the progress of each data packet is recorded. There are four possible packet states: *No_copy, Have_copy, Local_fwd,* and *Delivered*. The four packet states and the state transition are shown in Fig. 5. Section VI discusses how state

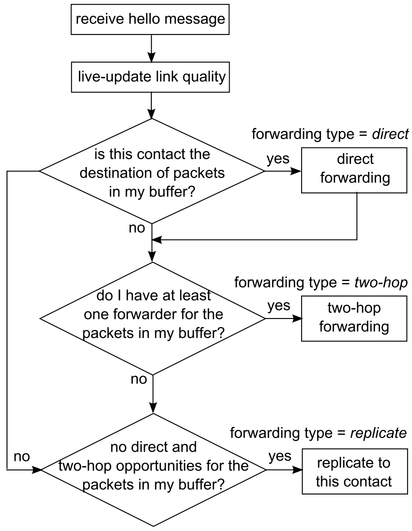


FIGURE 2. Data forwarding decision when a node gets contact.

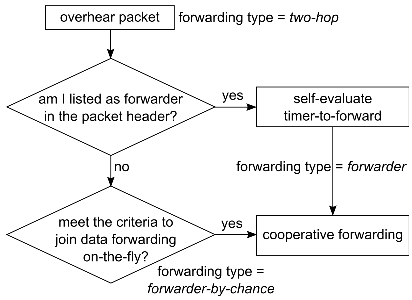


FIGURE 3. Cooperative data forwarding.

IP header		
contact ID 1	p with ID 1	p_{rev} with ID 1
...	...	...
contact ID k	p with ID k	p_{rev} with ID k

(a)

IP header
Forwarding type
Forwarder list {fwd ID 1, fwd ID 2}
...

(b)

FIGURE 4. Header format (a) Hello packet (b) Data packet.

of each packet are transitioned from one state to another and how packet infection is deterred using partially-immunized vaccine and fully-immunized vaccine.

IV. LIVE-UPDATE LINK QUALITY

In SCCF algorithm, nodes conduct live-updating link qualities to monitor the unreliable and probabilistic nature of wireless channel and to have local topology awareness so as to timely exploit the forwarding opportunities in the vicinity.

Each node broadcasts a hello message periodically, at an average period of τ (we use one second in the performance evaluation). The format of the hello message is shown in Fig. 4a. Nodes calculate the delivery probabilities of the links connecting to the direct contact nodes. This link quality denoted as p is calculated as $p = p_{fwd} \times p_{rev}$, where p_{fwd} refers to the link quality from a node to its contact node and p_{rev} refers to the link quality in reverse direction. p_{fwd} is called forward link quality and p_{rev} is called reverse link quality. We define that a node gets contact with another node if the link quality p is non-zero. The p_{fwd} and p_{rev} are obtained as follows.

The reverse link quality p_{rev} with a contact node is calculated based on the received hello packet ratio during the last w seconds from that node. For each contact node n_j, a node n_i calculates p_{rev} using the equation shown below.

$$p_{rev}(t) = \frac{r(t-w,t)}{w/\tau} \tag{1}$$

where $p_{rev}(t)$ denotes the reverse link quality at time t, $r(t-w,t)$ denotes the number of hello received from the contact node n_j during the last w seconds, and w/τ denotes the number of hello the contact node n_j sent during the last w seconds. For each contact node n_j, a node live-updates the $p_{rev}(t)$. We call the table recording this information reverse link information table. The format of this table is shown in Table 2.

TABLE 2. Reverse link information table.

contact ID	p_{rev} during the last w seconds
n_2	0.7
n_3	0.8
n_5	0.85
...	...

As shown in Fig. 4a, each hello sent by a node n_i contains the $p_{rev}(t)$, i.e. the received hello ratio from each contact node n_j during the last w seconds. This allows node n_j gets the p_{fwd} value to node n_i upon receiving a hello from n_i.

A node maintains a contact information table where it live-updates its local contact information. Upon receiving a hello message from a contact node, the node creates/updates an entry in the table. The format of the table is shown in Table 3. This table is used to monitor the data forwarding opportunities in the vicinity. The p_{fwd} value is updated when another hello message with update information from respective contact node is received. The p_{rev} value is updated whenever there is an update in reverse link information table. The link is considered lost and the entry is deleted when there is no update for p_{fwd} value within timeout period or when the p_{rev} value becomes zero.

TABLE 3. Contact information table.

contact ID	p_{fwd}	p_{rev}	p	one-hop contact list
n_2	0.8	0.7	0.56	(n_1, 0.56), (n_3, 0.7), (n_4, 0.7) ...
n_3	0.9	0.8	0.72	(n_1, 0.72), (n_2, 0.7), (n_4, 0.9) ...
n_5	0.9	0.85	0.77	(n_1, 0.77), (n_4, 0.9), (n_6, 0.8) ...
...	...	...	...	...

V. ROUTING

In this section, we discuss the details of the SCCF data forwarding algorithm. We first describe the five different types of forwarding mechanism: *direct, two-hop, forwarder, forwarder-by-chance,* and *replicate* for data delivery. We then elaborate the first four forwarding mechanisms in V-B and the *replicate* forwarding mechanism in V-E. The procedure about when the respective forwarding mechanism is triggered is also illustrated in Fig. 2 and Fig. 3. We also present the additional components of the protocol that complement data forwarding which include network layer acknowledgement, packet buffers (primary and temporary), and handling link loss.

TABLE 4. SCCF forwarding types.

Forwarding type	Definition	Addressing mode
direct	send to the destination by direct broadcasting.	broadcast
two-hop	send to the forwarder(s) by two-hop forwarding.	broadcast
forwarder	send from a forwarder to the destination.	broadcast
forwarder-by-chance	send from a non-candidate forwarding node to the destination.	broadcast
replicate	send packet copies to a contact node.	unicast

A. FORWARDING TYPE

A forwarding type is defined in data packet header to inform the contact nodes the forwarding type of the data packet that is being sent. SCCF protocol forwarding types and their definitions are discussed in Table 4. We add this field in the data packet header, which is shown in Fig. 4b, so that the receiver or nodes which overhear the transmission can obtain the information and/or process accordingly. A node will modify the forwarding type in the packet header based on the type of data forwarding it will use before passing the packet to lower layers for transmission.

B. OPPORTUNISTIC FORWARDING

Upon receiving a hello message from n_j and updating n_j's contact information in the contact information table, the node n_i makes forwarding decisions to forward the packets in its buffer based on the contact information table. Firstly, the node obtains all destination IDs of the packets in the buffer which are listed as one-hop contact in its contact information table. It will then broadcast the data packets to their destination node. This type of forwarding is called *direct* broadcasting.

The node will then check if the destination IDs of the remaining data packets in the buffer are listed as contacts of its direct contact nodes in the contact information table. Suppose a node n_1 has a contact information table with contents as shown in Table 3 and the destination IDs are identified as n_4 and n_6. It will then build the forwarding table for each destination ID as shown in Table 5. The direct contact nodes are assigned as potential forwarding nodes in the forwarding table. n_1 will select the two best forwarding candidates based on the expected number of transmissions (ETX) to

TABLE 5. Forwarding table format.

dst ID	fwd list (fwd ID, p between fwd and dst)
n_4	(n_2, 0.7), (n_3, 0.9), (n_5, 0.9)
n_6	(n_5, 0.8)
...	...

destination, which is calculated as follows.

$$ETX_{src,dst} = ETX_{first\_hop} + ETX_{second\_hop} \quad (2)$$

$$ETX_{first\_hop} = \frac{1}{1-(1-p(src,f_1))(1-p(src,f_2))} \quad (3)$$

$$ETX_{second\_hop} = p_1 ETX(f_2, dst) + p_2 ETX(f_1, dst) + p_3 min\{ETX(f_1, dst), ETX(f_2, dst)\} \quad (4)$$

where, $ETX_{src,dst}$ refers to the expected number of transmissions from source/sender node src (n_1 is the source/sender in this example) to destination node dst, ETX_{first_hop} refers to the expected number of transmissions required so that at least one of the two forwarders f_1 and f_2 successfully receive the data packet from src, and ETX_{second_hop} refers to the expected number of transmissions from two forwarders to destination node dst. $p(src, f_1)$ refers to the delivery probability of the link between src and f_1. We calculate $ETX(f_1, dst) = 1/p(f_1, dst)$ and $ETX(f_2, dst) = 1/p(f_2, dst)$. p_1 (p_2) denotes the probability that forwarding node f_1 (f_2) fails to receive the packet and p_3 is the probability that both node receive the packet. We assume that p_4, the probability of both nodes fail to receive is zero and p_1, p_2, and p_3 are evenly distributed, which is 1/3.

The node will then add the candidate IDs to the packet header and broadcast the packet. We also require that the two selected candidates be in contact so that they can overhear each other and can avoid duplicated transmissions. This type of forwarding is called *two-hop* forwarding. The format of the data packet header is shown in Fig. 4b.

The following discussion details the cooperative data forwarding which includes 1) how the candidates cooperatively forward the data packet from the source/sender node to the destination node; 2) how nodes not being assigned as candidate join the data forwarding on-the-fly so as to have resiliency under hostile environments; and 3) how a candidate handles when it finds link lost to the destination.

Cooperative data forwarding - before the forwarding candidate broadcasts the packet to the destination, it will decide which candidate in the list should broadcast first. Here, the decision is based on the link quality between the forwarding candidates and the destination. The two candidate nodes f_1 and f_2 will self-evaluate the length of delay (timer-to-forward), and will broadcast the packet when the timer expires. The length of the delay at candidate node f_1 is calculated as follows.

$$Delay(f_1) = \frac{1}{p(f_1, dst)} \times k + x \quad (5)$$

where $p(f_1, dst)$ is the link delivery probability from f_1 to dst. k refers to the average one-hop delay, i.e, the time taken from the transmitter network layer to the receiver network layer, which includes processing time, queuing time, and transmission time. We set $k = 0.01$ sec as it is the average one-hop delay in our simulation environment. x is the jitter which follows uniform distribution. If $p(f_1, dst) > p(f_2, dst)$, f_1 will have a smaller x (chosen from uniform distribution $[a, b)$) and f_2 will have a larger x (chosen from uniform distribution $[c, d)$) so that f_1 will be likely to broadcast earlier than f_2 and f_2 will overhear the transmission of f_1. Note that $a < b < c < d$. In this case, node f_2 will broadcast only if it does not overhear the transmission from f_1. When a candidate node overhears transmission from another candidate, it will stop the timer-to-forward and discard the packet. By adding the parameter x, it prevents collisions due to simultaneous transmission from the two candidates and avoids duplication by overhearing. If $p(f_1, dst)$ and $p(f_2, dst)$ are equal, x will be chosen randomly. By adding one more relay node, the success probability of data delivery from n_i to the destination dst is improved. Note that the forwarding type is set to *forwarder*.

As the node movement affects link connectivity, a node might encounter inaccuracies in the timer-to-forward self-evaluation if many forwarding candidates are involved, hence, we limit the number of forwarders to two. However, to increase the probability of successful delivery, a node can join the data forwarding on-the-fly. A node n_k can help cooperatively forward the data packet if the following conditions are satisfied. 1) Node n_k overhears the transmission from n_i; 2) its link quality to the destination is higher than $p(f_1, dst)$ and $p(f_2, dst)$; and 3) it has non-zero link quality to both f_1 and f_2.

If the above three conditions are satisfied, n_k chooses a jitter value x (picked from uniform distribution $[x, y)$, where $x < y < a$) and forwards the packet. Note that the forwarding type in this case is set to *forwarder-by-chance*. The two forwarding candidates will discard the packet when it overhears the transmission from n_k. By doing this, the forwarding is resilient in case the link delivery probabilities of the assigned candidates are affected due to node movement or changes in environments.

We observed that due to the opportunistic links and dynamic topology environments, a node might have only one potential forwarding candidate available. In this case, the node will still forward the packet so as to achieve data delivery in the shortest possible time. With one forwarding candidate, the expected number of transmissions to destination will become as follows.

$$ETX_{src,dst} = \frac{1}{p(src, f_1)} + \frac{1}{p(f_1, dst)} \quad (6)$$

As any node can join the data forwarding on-the-fly if conditions discussed above are satisfied, the probability to successfully deliver the packet can be further increased.

In two-hop forwarding, when a forwarding candidate finds that the link to the destination is lost, it will first broadcast the forwarder error message. It will then check its contact information table if there is any direct contact node which has a link to the destination. The node then selects a contact node with the lowest *ETX* to the destination node as in (6) and delays the transmission until it can overhear another candidate or *forwarder-by-chance* transmission if there is any. If it does not overhear any transmission for t interval (chosen from uniform distribution $[u, v)$ and $d < u < v$), it will replicate the packet to the selected node using unicast. If there is no direct contact node to the destination, the node will store the packet in its buffer and wait for future contact opportunities. Upon receiving/overhearing the forwarder error message, the receiver updates its contact information table and forwarding table. It will then inspect the interface queue and discard the packet if the erroneous forwarder is being assigned in the packet header.

C. PACKET BUFFER

In the proposed protocol, a node maintains two types of buffer to store data packets as follows.

Primary packet buffer (buffer) - It is used to store data packet when a node finds that the destination of that packet is not in its transmission range (not in contact) and it cannot find forwarding candidates to that destination.

Temporary packet buffer (temporary buffer) - It is used to keep copies of packets which are being broadcasted (direct broadcasting or two-hop cooperative forwarding) but waiting for acknowledgement to ensure the successful reception. After the node overhears the acknowledgement from the forwarding node or the destination, the corresponding packet copy will be removed from the temporary buffer. Otherwise, the node will retrieve the packet from the temporary buffer and store it in the primary buffer after acknowledgement timeout.

D. NETWORK LAYER ACKNOWLEDGEMENT

In *direct, two-hop, forwarder,* and *forwarder-by-chance* transmissions, a node uses IEEE 802.11 broadcast mode to forward the data packet. In the proposed algorithm, we use network layer acknowledgement scheme as IEEE 802.11 broadcast mode does not provide any acknowledgement for the broadcast packet. When a node receives a broadcast data packet, it will send the acknowledgement if it is the destination or the forwarding candidate of that packet. We use cumulative acknowledgement instead of acknowledgement for individual packet to reduce the control overhead and collisions to data packet transmissions. This acknowledgement is transmitted in broadcast mode. Therefore, it informs not only the sender about successful reception of the data packet but also other nodes who are within the communication range.

E. REPLICATION-BASED FORWARDING

Node n_i replicates the packets in its buffer to node n_j only if the direct and cooperative forwarding opportunities discussed above are not available. In this case, node n_i first sends packet state vector request to node n_j.

Packet state vector is an information table a node maintains to track the progress of data packet. There are four possible packet states. They are *No_copy*, *Have_copy*, *Local_fwd*, *Delivered*. Details of the packet state vector and the state transitions are discussed in Section VI.

Upon receiving n_i's request, node n_j broadcasts its packet state vector. Due to broadcasting, node n_i and all the other nodes in contact with node n_j are able to receive/overhear and update their packet states as per the state transition rules shown in Fig. 5. For example, if the overheard packet state is *Local_fwd*, a node will update its packet state to *Local_fwd* if its current state is *No_copy* /*Have_copy*. Similarly, if the overheard packet state is *Delivered*, a node will update its packet status to *Delivered* if its current state is *No_copy* /*Have_copy* /*Local_fwd*. The detail of the information epidemics control algorithm is discussed in Section VI.

After updating the packet state vector based on the received vector from n_j, node n_i gets the copies of packets in the buffer as in (7) and send to node n_j.

$$packets\_to\_be\_replicated = X_A + \overline{Y_A} + \overline{X_B} \tag{7}$$

where X_A refers to a set of IDs of packets that node n_i has in its primary packet buffer, Y_A refers to a set of IDs of packets with states *Local_fwd* in node n_i's packet status vector, and X_B refers to a set of IDs of packets with states *Have_copy* in node n_j's packet status vector. Note that packets in temporary buffer and packets with *Local_fwd* state are not replicated, and the proposed protocol uses unicast to transmit these packets. The forwarding type in this case is set to *replicate*. In contrast to original epidemic routing [8] where n_i and n_j exchange the missing packets with each other, the proposed protocol does not exchange the packets as n_j may have direct or cooperative forwarding opportunities to deliver its data packets.

When a node receives a packet transmitted by replication-based forwarding, it updates the packet status in the status vector to *Have_copy* if the current state is *No_copy* or discard otherwise. The node then checks whether the destination of the packet is its contact (direct) or it has forwarding candidate(s) to that destinations (two-hop). If those opportunities are available, it will deliver the packet using broadcast-based vicinity-aware cooperative forwarding module. Otherwise, it will store the packet in the buffer and wait for future contact opportunities.

F. HANDLING LINK LOSS

Due to the opportunistic and unreliable nature of wireless link, the communication link can be lost while packets are being forwarded. Therefore, the link layer maintains a link delivery information table and passes the packets to interface queue only if the link delivery probability is non-zero. In case of link loss, the link layer will discard the packet. The information in the link information table is created/updated/deleted if the corresponding link information is created/updated/deleted in the routing layer.

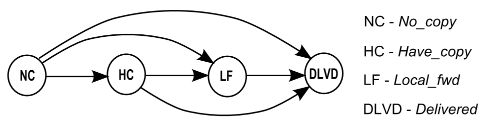


FIGURE 5. Four packet states and state transitions.

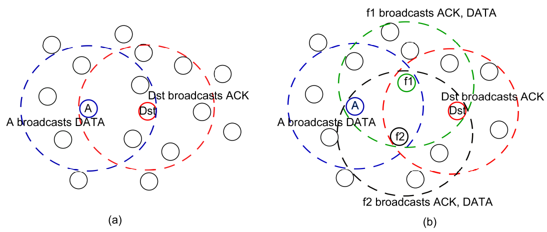


FIGURE 6. (a) Direct broadcast. (b) Two-hop broadcast.

VI. INFORMATION EPIDEMICS CONTROL

In the existing information epidemics control approach, a vaccine is generated only when a node successfully delivers a packet to the destination. However, in opportunistic links and dynamic topology environments, due to the effect of mobility and fading, having a direct contact with the destination is scarce. Therefore, this results in late information epidemics control and more infections. In this paper, we propose a vaccinating scheme which provides early control signal distribution, and therefore leverage the information epidemics control in the network. A conference version of this work is appeared in [37].

The vaccinating module monitors the broadcast-based vicinity-aware forwarding transmissions over the air and translates the information overheard into packet states. We call the database maintaining the state for each packet "packet state vector". We define 4 packet states as ***No_copy***, ***Have_copy***, ***Local_fwd***, and ***Delivered***. The default state for each packet is set to ***No_copy***. The four packet states, their definitions, and state transitions are discussed as follows. Fig. 5 shows the packet states and the state transitions.

Have_copy - A packet is set to *Have_copy* status when a node received a packet 1) from the upper layer; 2) from another node where data packet is transmitted by replication-based forwarding; and 3) from overhearing *two-hop* transmissions (i.e. the transmission from node *A* shown in Fig. 6b).

If a packet is in this status, a node will not accept the packet copy. That is to say, the node is immune to this packet infection. We call this information epidemics control *SCCF self-healing*.

Local_fwd - A packet status is set to *Local_fwd* when a node is aware that the data packet has been/is being forwarded by *direct* (i.e. the transmission from node *A* shown in Fig. 6a), *forwarder* (i.e. the transmission from node f_1 or f_2 shown in Fig. 6b), and *forwarder-by-chance* transmissions. This happens when a node 1) overhears the *direct*, *forwarder*, and *forwarder-by-chance* transmissions; and 2) receives/overhears acknowledgement from forwarding node(s) (i.e., the acknowledgement transmissions from node f_1 or f_2 shown in Fig. 6b).

Upon learning the *Local_fwd* status, a node will not accept the packet copy and will be able to vaccinate others in order not to get infected. When a node is transmitting a packet using *direct*, *forwarder* and *forwarder-by-chance* transmissions, it implies that the sender is in contact with the destination in one or two-hops. That is to say, most likely, the packet will be delivered to the destination. In addition, replicating this packet is no longer necessary as it will incur bandwidth consumption and collision to other data transmissions. Therefore, if a node happens to have a copy of the packet in its buffer, it will no longer use replication-based forwarding for this packet delivery to the destination. However, to ensure the reliability, the node will still use vicinity-aware forwarding until it gets information that the destination has received the packet. This type of information epidemics control is called vaccinating using partially-immunized vaccine.

Delivered - A packet status is set to *Delivered* when a node is aware that the data packet has been successfully delivered to the destination. This happens 1) when the destination node receives the packet; and 2) when a node receives/overhears acknowledgement from the destination node (i.e., the acknowledgement transmissions from node *Dst* shown in Fig. 6a and Fig. 6b).

Upon learning this status, a node becomes fully-immunized. It will no longer accept any incoming copy. It will also discard if there is a corresponding packet copy in its buffer. It will also be able to vaccinate others so that others can discard the packet in their buffer as well if any. This type of information epidemics control is called vaccinating using fully-immunized vaccine.

No_copy - A packet will be in *No_copy* status if a node does not have any information discussed above. A node will involve in both vicinity-aware forwarding and replication-based forwarding for this packet delivery.

In the existing protocols using VACCINE approach, it takes one bit for each packet inside the summary vector to tell if the node has the packet copy or not and another one bit for each packet inside the VACCINE vector to tell if the packet has been delivered to the destination or not. In the proposed algorithm, it uses only one vector called packet status vector and takes two bits for each packet to tell *No_copy, Have_copy, Local_fwd,* and *Delivered* packet status. As a result, the proposed algorithm requires transmission for one single vector only, which results in less number of vector transmissions compared to the protocols using existing recovery schemes. In addition, each vector provides further information including advance delivery progress while using the same number of bits as in the existing protocols. Moreover, the replication-based forwarding in proposed algorithm is reactive that it is initiated only if the direct and cooperative forwarding opportunities are not available and the packets have never been forwarded by those forwarding. Therefore, this reactive nature results in lower number of replication-based forwarding and hence, lower packet state vector transmissions. The size of the vector can be further minimized 1) by using compression mechanism [32] and 2) by setting the timer based on the desired confidence level of the packet delivery and purge the corresponding information inside the vector when timeout.

We use the IEEE 802.11 broadcast mode to send the status vector in contrast to unicast in existing SCF routing. As a result, not only the intended node but also the other nodes in the vicinity receive the progress of data delivery and update their knowledge accordingly, as per the state transition rules shown in Fig. 5. In the network layer, by having the information of packet state information from overhearing *direct*, *two-hop*, *forwarder*, and *forwarder-by-chance* transmissions, network layer acknowledgements, and packet state vectors, node B will be infected with a packet copy from node A only if B's packet state is *No_copy* and A's packet state is neither *Local_fwd* nor *Delivered*. This results in a lower number of infections/replications, lower bandwidth consumption, and lesser buffer occupancy.

VII. SIR MODEL FOR THE INFORMATION EPIDEMICS IN NETWORK

Susceptible-Infected-Recovered (SIR) is a model used to study the spread of packet copies in the network. As information dissemination in a network is same as disease spreading in a population, the SIR model has been widely used to model the packet dissemination in Epidemic routing variants [23]–[25]. The Markov chain model of an infectious disease using the SIR model with and without vaccination are shown in Fig. 7, where S, I, and R refers to the susceptible, the infected, and the recovered population in the system, respectively.

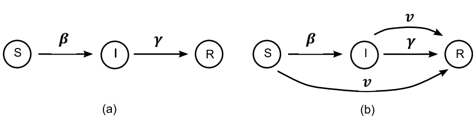


FIGURE 7. Markov chain model of an infectious disease: (a) SIR model without vaccination; (b) SIR model with vaccination.

A. SIR MODEL WITHOUT VACCINATION

Consider the SIR model without vaccination. Let $S(t)$ refers to the susceptible node population which does not have a packet copy at time t, $I(t)$ refers to the infected node population which have the packet copy at t, and $R(t)$ refers to the recovered node population which has successfully delivered the packet to the destination at t. The total population in network N is equal to $S(t) + I(t) + R(t)$. Assume β is the contact rate for a node to meet another node (infection rate) and γ is the contact rate of a node to the destination node (recovery rate). Accordingly, the total infection rate and the total recovery rate in the network are $\beta S(t)I(t)$ and $\gamma I(t)$, respectively [23], [24]. Using the Markov chain model shown in Fig. 7a, we obtain the first order differential equations as in (8).

$$\begin{aligned}
\dot{S}(t) &= -\beta S(t)I(t), \\
\dot{I}(t) &= \beta S(t)I(t) - \gamma I(t), \\
\dot{R}(t) &= \gamma I(t), \\
S(t) + I(t) + R(t) &= N.
\end{aligned} \tag{8}$$

Assume that at time $t = 0$, only one node in the network (source node) has the packet. So, the initial conditions are $S(0) = N - 1$, $I(0) = 1$, and $R(0) = 0$. Therefore, we obtain the number of infected nodes as a function of time, $I(t)$ by solving the differential equations in (8), that is,

$$I(t) = \frac{N}{1 + (N-1)e^{-\beta N t}} \tag{9}$$

Recalling that β is the contact rate for a node to meet another node which can be calculated as $\beta = \frac{2\omega R E[V^*]}{L^2}$ [24]. Note that ω is a constant specific to the mobility model, R is the radio transmission range, $L \times L$ is the network size, and $E[V^*]$ is the average relative speed between the two nodes.

B. SIR MODEL WITH VACCINATION

We extend the original SIR model without vaccination to include the vaccinating process as follows. In the SIR model with vaccination, $R(t)$ represents the recovered node population which includes 1) infected nodes successfully delivered the packet to the destination and 2) the infected nodes and susceptible nodes which have successfully received the vaccine.

Incorporating the vaccinating process, we show the Markov chain model of information dissemination in the network in Fig. 7b. From the model, we obtain the first order differential equations as in (10).

$$\begin{aligned}
\dot{S}(t) &= -\beta S(t)I(t) - v(t)S(t), \\
\dot{I}(t) &= \beta S(t)I(t) - \gamma I(t) - v(t)I(t), \\
\dot{R}(t) &= \gamma I(t) + v(t)I(t) + v(t)S(t), \\
S(t) + I(t) + R(t) &= N.
\end{aligned} \tag{10}$$

where $v(t)$ is the successful vaccination rate in the system at t. The infected node population as a function of time under the vaccinating process, $I(t)$, can be obtained using early-stage analysis as discussed in [25].

C. CONTROL SIGNAL DISTRIBUTION

Assume that v_f and v_p are the successful vaccination rate of the nodes in the network using fully-immunized and partially-immunized vaccine, respectively. Let v_o be the successful vaccination rate of the nodes in the network using the original VACCINE method. Note that the vaccinating process using VACCINE approach can be initiated only when a node meets the destination. Assume T_{VAC} be the time instance the vaccinating process is initiated or the control signal distribution time in VACCINE. We describe $v(t)$, the vaccination rate in the network at time t using original VACCINE method as follows,

$$v(t) = \begin{cases} 0, & t < T_{VAC} \\ v_0, & t \geq T_{VAC} \end{cases} \tag{11}$$

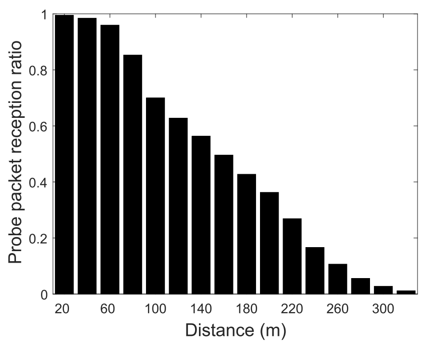


FIGURE 8. Probe packet reception ratio over distance.

We then describe $v(t)$ for the proposed vaccinating process as follows.

$$v(t) = \begin{cases} 0, & t < T_{P\_VAC} \\ v_p, & T_{P\_VAC} \leq t < T_{F\_VAC} \\ v_p + v_f, & t \geq T_{F\_VAC} \end{cases} \quad (12)$$

where T_{P_VAC} and T_{F_VAC} are the time instance for the partially-immunized and fully-immunized control signal distribution in proposed vaccinating scheme. We state that $v_f \geq v_o$ as v_f is the rate using one-to-many vaccination (broadcast) whereas v_o is the pairwise vaccination. Note that the control signal distribution using fully-immunized vaccine and the original VACCINE scheme can be initiated only when a node meets the destination. However, having the local topology information and exploiting broadcast-based vicinity-aware forwarding make a node delivering the packet to the destination much earlier compared to the pairwise packet exchange. Therefore, we claim that the control signal distribution using the fully-immunized vaccine can be initiated much earlier than the vaccination using the original VACCINE scheme (i.e. $T_{F\_VAC} \leq T_{VAC}$). In addition, using the partially-immunized vaccine can further advance the vaccinating process as it is initiated when there is a local-forwarding opportunity.

We implement the integrated data delivery solution in network simulator (NS-2). We show that having early control signal distribution provides a higher vaccination rate and recovery rate. This results in a lower infection rate and hence, requires fewer packet copy transmissions.

VIII. PERFORMANCE EVALUATION

A. EVALUATION METHODOLOGY

We use network simulator (NS-2.33) to evaluate the performance of the proposed scheme. Two main studies: 1) the susceptible-infected-recovered population study; and 2) the routing performance are conducted. let $inf(t)$ be the number of nodes that get infected at each time instance t, $rec_i(t)$ be the number of infected nodes that get recovered at each time instance t, and $rec_s(t)$ be the number of susceptible nodes that get recovered at each time instance t. Using the simulation, we obtain $inf(t)$, $rec_i(t)$, and $rec_s(t)$ under *Epidemic self-healing*, *SCCF self-healing*, under the vaccination without having partially-immunized vaccines, and under the vaccination with both paritally-immunized plus fully-immunized vaccines. Note that the recovered population in Epidemic routing is 0 as the nodes in the network continues spreading the packet copies until all the nodes in the network get infected. We then plot the SIR population in the network under each scheme using the following equations.

For Epidemic routing,

$$\begin{aligned} I(t) &= \sum_{t=0}^{t} inf(t), \\ S(t) &= N - I(t). \end{aligned} \quad (13)$$

For SCCF routing,

$$\begin{aligned} R(t) &= \sum_{t=0}^{t} rec_s(t) + \sum_{t=0}^{t} rec_i(t), \\ I(t) &= \sum_{t=0}^{t} inf(t) - \sum_{t=0}^{t} rec_i(t), \\ S(t) &= N - I(t) - R(t). \end{aligned} \quad (14)$$

For the routing study, we have the following three metrics to compare data delivery efficiency.

- Packet Delivery Ratio (PDR). The amount of packets delivered over the amount of packets generated.
- End-to-End Delay (E2ED). The time taken from the packet generated at the source application layer to the packet delivered at the destination application layer.
- Transmission Count (TXC). The number of times a packet is transmitted (including retransmissions) across the air. This metric is also known as forwarding cost.

For performance comparison in connected environment, we choose a multi-hop unicast protocol "AODV" [4] as it is shown to be one of the best protocols for such network. The implementation of AODV is obtained from NS-2.33 package. For comparison in network with dynamic and probabilistic links, we choose a multi-hop cooperative broadcast protocol "CORMAN" as it is the first cooperative protocol proposed for such environment without requiring position information. We obtain the scenario and result trace files from the authors of CORMAN [6], reproduce the AODV results from the paper [6], and conduct the performance comparison by using the same network, mobility, traffic scenario, and propagation model as in the paper. For comparison in disrupted/disconnected environment, we choose a replication-based forwarding protocol "ER" [8] as it provides the highest delivery success rate with lower end-to-end delay in such network if the given bandwidth and buffer resource are sufficient, which is shown in recent studies [16], [22], [33]–[35]. We implement the ER protocol in NS-2.33 and verify the implementation by using the same parameter settings and reproducing the results as in [17]. We also compare the ER simulation model with the analytical model as shown in Fig. 9a.

The scenarios studied and the simulation parameters are described in Table 6. First we compare with CORMAN under varying network densities (from highly dense to relatively

TABLE 6. Simulation parameters.

Parameters	SIR study	Comparison with CORMAN [6]	Effect of fading	Effect of obstacles	Effect of mean speed	Mobile social network model
Network area ($lxl\ m^2$)	1000	250, ..., 1000	1000	1000	1000	1600
No. of nodes (N)	100	50	25	20 to 50	25	41, 78
Mobility model	RWP	RWP	RWP	MCM [29]	RWP	SWIM [30]
Avg. Speed (m/s)	10	5	15	15	5, 10, 15, 20, 25	SWIM [30]
Propagation model	Two-ray-ground	Nakagami	Freespace, Nakagami, Rayleigh	MCM [29]	Nakagami	Freespace
Traffic per flow	1 packet	400 Kbps	400 Kbps	400 Kbps	400 Kbps	16 Kbps
No. of CBR flows	1	1	10	10	10	420

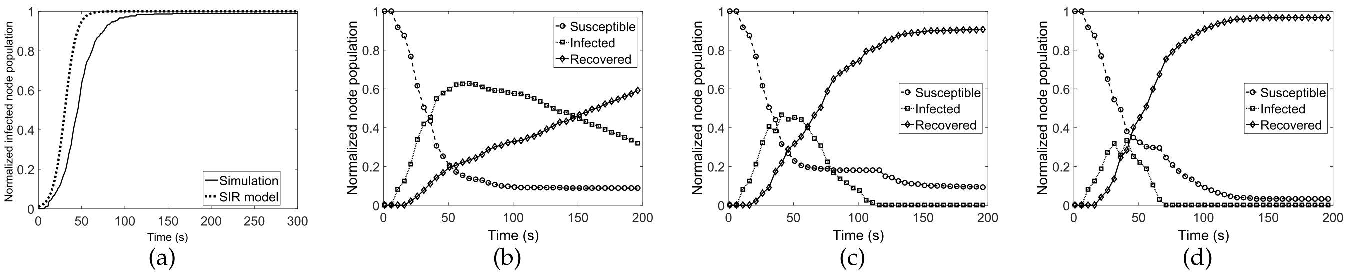


FIGURE 9. **(a) Infected population under ER self-healing. (b) SIR population under SCCF self-healing; (c) without partially-immunized vaccination; and (d) with both partially-immunized and fully-immunized vaccination.**

sparse). We then study the network performance in relatively sparse and hostile environments where we vary fading distribution, add obstacles, and vary speed. At last, the performance study in mobile social networks is conducted.

We use the newly revised IEEE 802.11 MAC and PHY layer modules [26]. The IEEE 802.11a standard with BPSK modulation is used in all the simulation studies in this paper. The transmission ranges under Freespace and Two-ray ground propagation models are 200 m and 160 m, respectively. Under Nakagami and Rayleigh fading, the transmission range between the two nodes becomes probabilistic. Fig. 8 shows the probe (HELLO) packet reception ratio over distance under Nakagami fading. It can be observed that the link delivery probability drops significantly when the distance between the two nodes is larger than 80 m. Note that the Rayleigh fading here causes more severe link delivery probability degradation than the Nakagami fading. The fading model parameters can be found in [27].

We collect simulation results using identical traffic model with 10 different randomly generated mobility scenarios. Each simulation is run for 900 seconds except for the study under mobile social network model for which we use the same parameters as in [30]. For studies on effect of obstacles and effect of speed, average network performance results are plotted with 95% confidence intervals. For studies on comparison with CORMAN, effect of fading, and mobile social network environment, confidence intervals are provided in Tables 9, 10, and 11.

B. STUDY ON SIR POPULATION IN THE NETWORK

The normalized infected node population (i.e., $I(t)/N$) under self-healing used in Epidemic routing is shown in Fig. 9a. It also shows the result with the SIR model (9). As a node with a copy continues infecting other nodes without a copy, the number of infected population increases over time. In addition, as it does not have the mechanism to deter the transmissions of packets that have been successfully delivered to the destinations, the recovered population under self-healing Epidemic routing is zero.

The SIR population in SCCF under different proposed vaccinating algorithms is shown in Fig. 9b, Fig. 9c, and Fig. 9d. We observe that the infected population is substantially reduced under SCCF complete (both partially and fully immunized) vaccination compared to the SCCF self-healing and the SCCF without partially-immunized vaccines. In SCCF self-healing (Fig. 9b), a node gets recovered only when it delivers the packet using direct-broadcast or two-hop broadcast. Therefore, the infected population is increased dramatically in the initial stage and gradually decreased in the later stage. In SCCF without partially-immunized vaccines (Fig. 9c), a node also maintains packet delivery information and also shares with others. From the delivery information, a node becomes able to stop transmitting unnecessary packet copies. Thus, the infected population is greatly reduced and the vaccinated population is greatly increased compared to SCCF self-healing. In SCCF with complete vaccination (Fig. 9d), a node also maintains the information of packet which has been locally-forwarded, i.e. higher probability to be received at the destination. By having this information in addition to the ones in the other two schemes, a substantial amount of infected population can be further reduced.

C. ROUTING PERFORMANCE STUDY

1) COMPARISON WITH CORMAN

Using the same scenarios as in CORMAN [6], we obtain the results for SCCF and AODV. The packet delivery

TABLE 7. PDR comparison with CORMAN.

network area(m)	SCCF	AODV	CORMAN [6]	AODV [6]
250	1.000	0.958	0.981	0.781
300	1.000	0.850	0.926	0.755
350	1.000	0.821	0.911	0.790
400	1.000	0.660	0.986	0.633
450	1.000	0.595	0.937	0.579
500	1.000	0.615	0.938	0.425
550	0.999	0.509	0.789	0.247
600	1.000	0.254	0.883	0.402
650	0.986	0.194	0.818	0.390
700	0.998	0.473	0.844	0.476
750	0.982	0.270	0.758	0.253
800	0.975	0.160	0.572	0.141
850	0.989	0.381	0.553	0.183
900	0.960	0.262	0.605	0.170
950	0.961	0.244	0.763	0.406
1000	0.947	0.150	0.478	0.153

TABLE 8. E2ED comparison with CORMAN.

network area(m)	SCCF	AODV	CORMAN [6]	AODV [6]
250	0.441	0.062	0.082	0.208
300	0.963	0.168	0.086	0.177
350	0.994	0.130	0.094	0.193
400	1.282	1.617	0.115	0.287
450	1.582	2.241	0.153	0.246
500	1.863	0.802	0.216	0.355
550	2.887	0.636	0.433	0.522
600	5.389	1.634	0.341	0.238
650	7.945	1.489	0.311	0.277
700	5.048	0.674	0.257	0.299
750	9.953	1.307	0.410	0.438
800	16.354	2.700	0.883	0.504
850	15.706	0.792	0.723	0.795
900	12.073	1.633	0.709	0.675
950	16.775	1.038	0.475	0.580
1000	21.940	0.450	0.893	1.767

ratio and average end-to-end delay are shown in Tables 7 and 8.

In dense network (area $\leq$ 500 sq m), SCCF successfully delivers all packets while CORMAN delivers about 95 $\pm$ 3%. However, in terms of delay, due to switching the routing approach to replication-based forwarding for packets unable to be delivered in two-hop vicinity, SCCF incurs slightly longer delay for some packets compared to CORMAN which uses multi-hop forwarding approach. This shows that in connected network with probabilistic links, the CORMAN protocol is more favourable compared to the SCCF protocol.

In relatively dense network (550 sq m $\leq$ area $\leq$ 750 sq m), CORMAN delivers about 80 $\pm$ 5% while SCCF delivers about 99%. In this case, we observe that there is a trade-off between the packet delivery ratio and the end-to-end delay. In SCCF, it adaptively switches to replication-based forwarding for packets with no delivery opportunities in the vicinity while CORMAN uses multi-hop forwarding for all packets. This shows that data delivery is guaranteed by using the SCCF adaptive forwarding approach; however, it also experiences longer delay especially for packets remain undelivered when multi-hop forwarding is used. Therefore, in relatively dense network, one can be chosen over the other based on the required network performance. Note that the delay metric calculation only takes into account the time taken for the delivered packet. Hence, data packets delivered using SCCF but not in the case of CORMAN will also factor in the end-to-end delay calculation of SCCF.

When the network becomes sparser (800 sq m $\leq$ area $\leq$ 1000 sq m), the packet delivery ratio of CORMAN is dropped significantly while SCCF maintains the performance. In CORMAN, each node uses source routing and finds the shortest paths to all the other nodes in the network. This information is used by forwarding candidates to adaptively forward the data packet upon link changes. Although the CORMAN protocol is resilient to the link quality fluctuation and the node mobility, the partial/intermittent disconnection in relatively sparse network causes nodes unable to locate certain parts of the network at some point of time and hence, results in significant drop under such environments. This shows that CORMAN is not applicable for this type of scenario where about 50% of the data packets are left undelivered. In SCCF, it is observed that as the network becomes sparser, more replication-based forwarding approach is involved in seeking the broadcast-based vicinity-aware forwarding opportunities to deliver the packets. This results in longer delay. However, we see that the delay incurred in SCCF is much lower compared to the original SCF routing, which is discussed in the following section.

2) EFFECT OF FADING

In this study, we evaluate the SCCF and ER performance under different fading environments. We use a density of 25 nodes per sq km. This means that there exist only two nodes in 80 sq m which can communicate with higher link delivery probability. Note that as shown in Fig. 8, the link delivery probability drops significantly when the distance between the two nodes is larger than 80 m. The average speed of the mobile node is increased from 5 to 15 m/s. Hence, this scenario depicts a sparser and more dynamic environment compared to the previous study in Section VIII-C.1 where there are at least four nodes in 80 sq m. We also increase the number of CBR (constant bit rate) traffic flows to 10 so as to simulate a more congested environment. Each flow source generates maximum 300 packets (1000 byte each). The buffer size of a node is set to be 1500 packets for all protocols. This value is selected based on the buffer requirement study in the preliminary work [36], where it shows that ER requires 50% of the total packet for buffer space to maintain the maximum data delivery.

Firstly, we study the CDF of packet delivery with respect to delivery delay as shown in Fig. 10a. We observe that with the delay $\leq$ 50 seconds, 95%, 91% and 80% of the packets are delivered by SCCF under Freespace, Nakagami, and Rayleigh fading in contrast to 31%, 13% and 7% by ER,

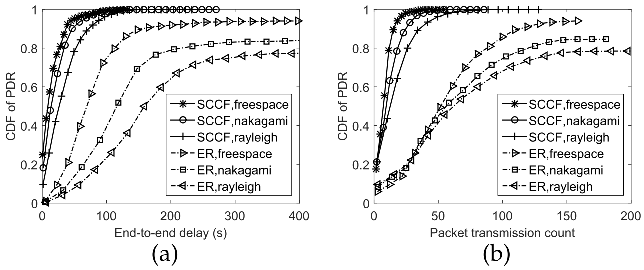


FIGURE 10. **The effect of fading: (a) CDF with respect to packet delivery delay; (b) CDF with respect to transmission count.**

respectively. Furthermore, with the delay $\leq$ 100 seconds, almost 100% packets are delivered by SCCF in contrast to 24 to 75% by ER. These facts show that SCCF delivers most packets with minimum delay and only a few percentage of packets takes extra delay. In SCCF, it scans around its contact nodes, monitors and exploits broadcast-based vicinity-aware forwarding if there is any, which significantly reduces the delivery delay. Although ER is robust to opportunistic links and dynamic topologies in the network, simply forwarding to the available contact incurs longer delay and the situation becomes severe in fading due to the higher chance of unsuccessful reception.

We then study the CDF of packet delivery with respect to the transmission count. As shown in Fig. 10b, at most 18 transmission count are required to maintain the packet delivery 80% in SCCF. Whereas in ER, the transmission count rises to 120 to maintain the same delivery percentage. These facts show that SCCF is able to reduce a larger number of unnecessary transmissions/replications using the proposed information epidemics control where nodes in the network get vaccinated and/or recovered progressively by the partially-immunized vaccines and the fully-immunized vaccines.

We then discuss the overhead of the proposed solution as follows. As SCCF does not require to have route-discovery (discussed in Section II-A), it does not incur control overhead due to the discovery process unlike the existing hybrid opportunistic network protocols. The additional control messages used in SCCF are hello, packet state vector request, forwarder error, and cumulative ACK messages. Note that, hello is a periodic broadcast message and is used in all protocols for contact discovery and link metric computation. Vector request and forwarder error messages are sent in one hop and used only when a node decides to replicate its data packets and when the forwarding node lost its contact to the destination. ACK in SCCF is a one-hop broadcast message and is sent in cumulative manner so as to reduce the control overhead whereas most existing end-to-end and SCF routing protocols use unicast ACK for individual packets. In SCF-based protocols, vector transmission is the main overhead to be evaluated when the delivery efficiency is considered. Therefore, in the following, we show the overhead caused by the vector transmissions under Nakagami fading.

Fig. 11 shows the CDF of PDR and the CDF of vector transmission count incurred for the delivery over the simulation

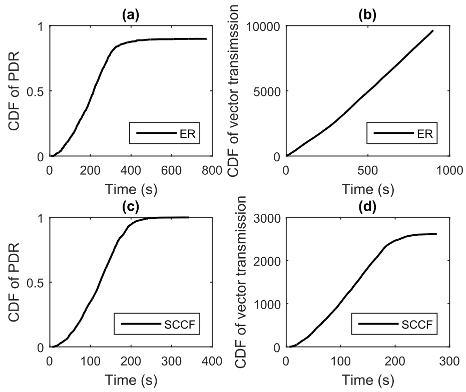


FIGURE 11. **Summary vector overhead in Epidmeic and SCCF routing.**

time. The traffic is generated from 5 seconds to 207 seconds and the simulation is run for 900 seconds. As SCCF uses reactive form of replication, there is no summary vector transmission in the beginning when there is no traffic generated in the network. It can also be observed that the vector transmissions is stopped even before some packets are not yet delivered to the destination. In SCCF, replication is triggered only when the node has the packets which have not yet been forwarded by direct and cooperative forwarding. So, for some nodes which have packet copies but know that the packet has been locally forwarded before will not use replication-based forwarding. However in ER, we can see the vector transmissions in the network even when there is no traffic in the beginning due to the proactive nature of replication. It can also be observed that the vector transmissions in ER continues even after the 90% of delivery because of the lack of delivered information.

3) EFFECT OF OBSTACLES

In this study, we evaluate the performance of SCCF, ER, and AODV under an obstacle-constrained environment. A simplified version of Mission Critical Mobility (MCM) model [29] is used. In this model, nodes move around the obstacles in the network. For the propagation model, a modified version of the two-ray-ground model [29] which takes into account the impact of the physical obstacles on signal propagation is used. We use the same obstacle-constrained environment scenario as in [29]. The width and height of the four obstacles are set as (470, 210), (150, 360), (200, 490), and (320, 270) respectively.

The packet delivery ratio, average delivery delay, and average packet transmission count under obstacle environment with different node densities are presented in Fig. 12a, Fig. 12b, and Fig. 12c. We see that the packet delivery ratio of SCCF is not affected by environment with obstacles where it is maintained at almost 100% in both with and without obstacle scenarios. Similarly, the average transmission count of SCCF remains unaffected, with only a negligible increase in the obstacle scenario. Furthermore, we note that, in SCCF, increasing node density does not increase the transmission count unlike ER and it is just a few times more than the

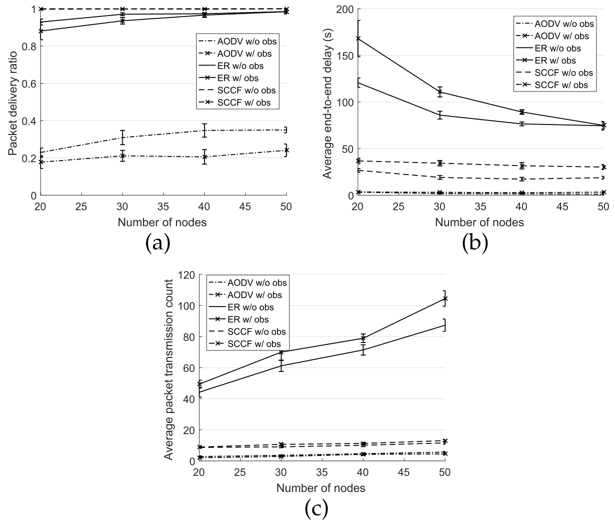


FIGURE 12. The effect of obstacle-constrained environment. (a) Packet delivery ratio. (b) Average end-to-end delay. (c) Average packet transmission count.

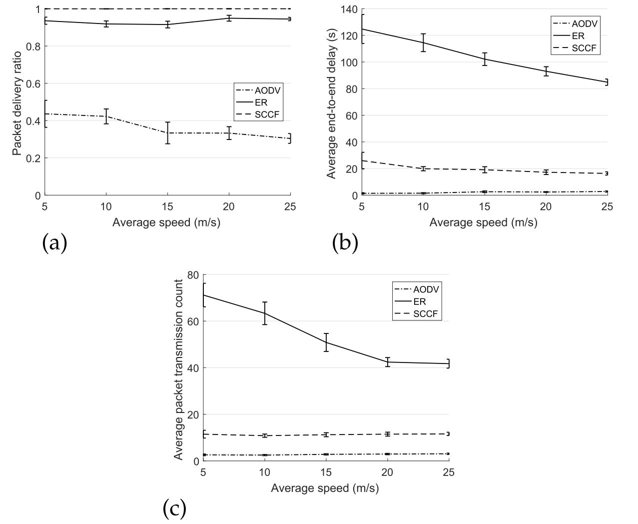


FIGURE 13. The effect of varying mean speed. (a) Packet delivery ratio. (b) Average end-to-end delay. (c) Average packet transmission count.

transmission count of end-to-end routing, due to the advantage of the proposed information epidemics control. However, for the average delay of SCCF, there is an increase in delivery delay in the obstacle-constrained scenario. This happens due to the fewer opportunities to timely exploit the *direct, two-hop, forwarder,* and *forwarder-by-chance* forwarding approaches. We also observe that ER needs higher node density to achieve better packet delivery ratio and delivery delay in contrast to SCCF which maintains the similar performance in networks with low node density as well.

4) EFFECT OF SPEED

In this study, we evaluate the performance of SCCF, ER, and AODV under different mean speed. The packet delivery ratio, average delivery delay, and average packet transmission count under Nakagami fading environment with different mean speeds are presented in Fig. 13a, Fig. 13b, and Fig. 13c. We note that SCCF is robust to the node speed maintaining almost 100% packet delivery ratio with minimum replications whereas in ER, higher contact rate among nodes (higher speed) is required to have minimum delivery delay. We also note that in ER, when the contact rate is low and the contact time is longer (this happens when the node speed is relatively low), the network incurs more unnecessary transmission/replications and also longer delay. However, in SCCF, we observe that the data forwarding is robust to high/low contact rate and contact time. This is due to 1) nodes always scan and exploit the better forwarding opportunities in their vicinity; 2) nodes also give copies to their contacts to help scan and forward if no opportunities is found; and 3) unnecessary transmissions/replications are well controlled by the vaccinating scheme.

5) STUDY UNDER MOBILE SOCIAL NETWORK MODEL

In this study, we evaluate the performance of SCCF and ER under a mobile social network model. We use the SWIM

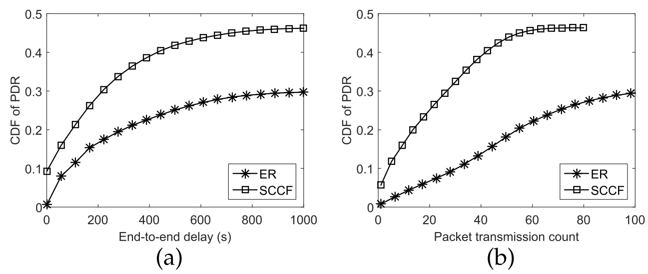


FIGURE 14. N=41 (a) CDF with respect to packet delivery delay; (b) CDF with respect to packet transmission count.

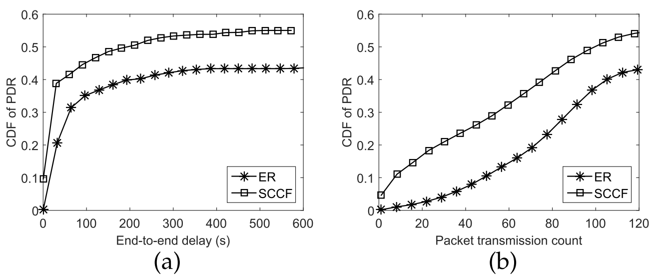


FIGURE 15. N=78 (a) CDF with respect to packet delivery delay; (b) CDF with respect to packet transmission count.

model [30] to generate the scenarios. The SWIM model was shown to have the same statistical properties of real social network traces and predict the performance of the SCF protocols accurately [31]. We use the same parameters as in [30] to model the real-world traces in the Infocom05 and Infocom06 [28]. We use 802.11a with the freespace propagation model and a transmission range of 160 m. We do not add the fading in this study as the model provides the inter-contact time distribution, contact distribution, and number of contacts per pair of nodes. We consider a network area of 1600 x 1600 m^2 so as to keep the transmission range parameter in the SWIM model as 0.1.

TABLE 9. 95% confidence intervals for comparison with CORMAN study.

Network area(m)	PDR		E2ED	
	SCCF	AODV	SCCF	AODV
250	1.000 ± 0	0.958 ± 0.044	0.441 ± 0.221	0.062 ± 0.099
300	1.000 ± 0	0.850 ± 0.124	0.963 ± 0.548	0.168 ± 0.163
350	1.000 ± 0	0.821 ± 0.166	0.994 ± 0.784	0.130 ± 0.131
400	1.000 ± 0	0.660 ± 0.192	1.282 ± 0.513	1.617 ± 2.686
450	1.000 ± 0	0.595 ± 0.280	1.582 ± 1.250	2.241 ± 2.515
500	1.000 ± 0	0.615 ± 0.221	1.863 ± 1.063	0.802 ± 0.956
550	0.999 ± 0.002	0.509 ± 0.278	2.887 ± 1.815	0.636 ± 0.643
600	1.000 ± 0	0.254 ± 0.199	5.389 ± 2.971	1.634 ± 1.419
650	0.986 ± 0.030	0.194 ± 0.191	7.945 ± 4.026	1.489 ± 2.338
700	0.998 ± 0.004	0.473 ± 0.282	5.048 ± 4.688	0.674 ± 0.756
750	0.982 ± 0.022	0.270 ± 0.185	9.953 ± 7.669	1.307 ± 1.632
800	0.975 ± 0.022	0.160 ± 0.160	16.354 ± 13.447	2.700 ± 2.571
850	0.989 ± 0.014	0.381 ± 0.280	15.706 ± 13.879	0.792 ± 1.000
900	0.960 ± 0.047	0.262 ± 0.210	12.073 ± 8.844	1.633 ± 1.902
950	0.961 ± 0.049	0.244 ± 0.207	16.775 ± 11.894	1.038 ± 1.251
1000	0.947 ± 0.040	0.150 ± 0.158	21.940 ± 10.236	0.450 ± 0.207

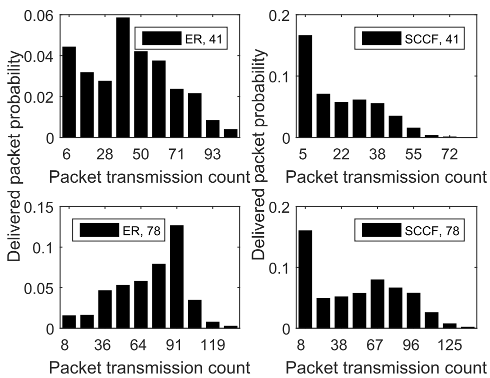


FIGURE 16. Delivered packet probability with respect to packet transmission count.

TABLE 10. 95% confidence intervals for effects of fading study.

	Fading model	SCCF	ER	AODV
PDR	Freespace	0.999 ± 0.0001	0.941 ± 0.02	0.568 ± 0.08
	Nakagami	0.999 ± 0.0001	0.846 ± 0.04	0.234 ± 0.08
	Rayleigh	0.999 ± 0.0001	0.785 ± 0.03	0.138 ± 0.06
E2ED	Freespace	15.41 ± 2.50	75.25 ± 4.54	1.225 ± 0.35
	Nakagami	21.51 ± 2.60	113.35 ± 7.31	5.428 ± 2.94
	Rayleigh	33.52 ± 3.37	145.93 ± 7.55	4.375 ± 2.68
TXC	Freespace	8.445 ± 0.73	54.14 ± 3.83	3.122 ± 0.27
	Nakagami	11.90 ± 0.85	54.44 ± 3.30	2.484 ± 0.24
	Rayleigh	16.98 ± 1.41	55.39 ± 3.07	1.906 ± 0.59

We first study the Infocom05 scenario. The number of nodes in the network is 41. The CDF of packet delivery with respect to end-to-end delay and the packet transmission count are shown in Fig. 14a and Fig. 14b. Overall, we observe that given the same time interval taken by the ER, SCCF delivers data packets far beyond what ER does with much less replication/transmission count. It is noted that exploiting the cooperative forwarding opportunities whenever available and adaptively switching to SCF forwarding guarantee faster delivery compared to the flooding protocol. This encourages

TABLE 11. 95% confidence intervals for study under mobile social network model.

	No. of nodes	SCCF	ER
PDR	41	0.467 ± 0.095	0.304 ± 0.058
	78	0.564 ± 0.090	0.446 ± 0.075
E2ED	41	163.42 ± 40.54	200.67 ± 48.53
	78	40.52 ± 15.67	67.53 ± 12.62
TXC	41	18.44 ± 2.45	37.87 ± 7.33
	78	45.25 ± 6.22	67.12 ± 7.63

adding the vicinity aware forwarding on top of SCF forwarding for faster delivery. This observation is much in line with the findings in [21], where it shows that a large amount of delay can be reduced using two-hop opportunity compared to using 1-hop contact only. In addition, having early control signal distribution using partially-immunized vaccine and fully-immunized vaccine results in lower infection rate. Therefore, most packets are delivered with less number of forwarding count in SCCF compared to ER, as shown in Fig. 14b. We then study the Infocom06 scenario, where the number of nodes in the network is 78. Similar observations can be seen in this case as well. However, with more nodes in the network, the number of contacts and the contact rate are increased. Therefore, faster delivery is achieved for both SCCF and ER protocols, shown in Fig. 15a, compared to the network with 41 nodes. For the transmission count, we note that more replications are being made in this case due to more number of contacts with more nodes. However, as shown Fig. 16, regardless of the node density, SCCF delivers most packets with fewer replications whereas, in ER, a large number of replications is made and it becomes more significant when the network is denser.

IX. CONCLUSION

We have proposed a data delivery solution for opportunistic networks. Two main algorithms: SCCF routing and information epidemic control are proposed to solve long delivery delay problem and information epidemic problem. The SIR population study shows that having both partially-immunized and fully-immunized vaccines and broadcasting the vaccines over the air give immunity to a large population of nodes and therefore deter a substantial amount of infections in the network. Network performance studies are conducted in relatively sparse networks with fading, obstacles, and social contact patterns. We found that 1) proactive replication incurs substantial forwarding cost and longer delay; 2) exploiting cooperative vicinity-aware forwarding and eliminating the infections proactively result in minimum delivery delay without incurring unnecessary forwarding cost; and 3) using reactive replication-based forwarding approach only for packets which are unable to be delivered in the vicinity ensures the delivery performance. This shows that the joint adaptive data forwarding and information epidemic control solution works well in highly dynamic MANET and opportunistic networks such as disaster recovery and military communications where the lack of infrastructure, high mobility, unstable link connectivity, fading, and obstacle-constrained environments are the major concerns on the data delivery performance.

ACKNOWLEDGMENT

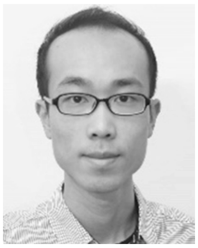
The authors would like to thank Cheng Li and Zehua Wang for providing the detail simulation scenarios and the numerical results of CORMAN routing protocol. The authors would also like to thank Christos Papageorgiou and Konstantinos Birkos for providing the source code of the mission critical mobility model.

REFERENCES

[1] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun.*, 2003, pp. 27–34.
[2] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 134–141, Nov. 2006.
[3] N. Chakchouk, "A survey on opportunistic routing in wireless communication networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2214–2241, 4th Quart. 2015.
[4] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt, doi: 10.17487/RFC3561.
[5] S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 1, pp. 69–74, Jan. 2004.
[6] Z. Wang, Y. Chen, and C. Li, "CORMAN: A novel cooperative opportunistic routing scheme in mobile ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 289–296, Feb. 2012.
[7] S. Yang, C. K. Yeo, and B. S. Lee, "Toward reliable data delivery for highly dynamic mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 1, pp. 111–124, Jan. 2012.
[8] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Duke Univ., Durham, NC, USA, Tech. Rep. CS-200006, 2000.
[9] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: An efficient routing scheme for intermittently connected mobile networks," in *Proc. ACM SIGCOMM Workshop Delay-Tolerant Netw.*, 2005, pp. 252–259.
[10] T. Matsuda and T. Takine, "(p,q)-Epidemic routing for sparsely populated mobile ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 5, pp. 783–793, Jun. 2008.
[11] T. Kimura, T. Matsuda, and T. Takine, "Multi-Spreader Routing for sparsely populated mobile ad hoc networks," *Wireless Netw.*, vol. 20, no. 1, pp. 155–175, 2014.
[12] R. Ramanathan, R. Hansen, P. Basu, R. Rosales-Hain, and R. Krishnan, "Prioritized epidemic routing for opportunistic networks," in *Proc. 1st Int. MobiSys Workshop Mobile Opportunistic Netw.*, 2007, pp. 62–66.
[13] J. Ott, D. Kutscher, and C. Dwertmann, "Integrating DTN and MANET routing," in *Proc. SIGCOMM Workshop Challenged Netw.*, 2006, pp. 221–228.
[14] J. Lakkakorpi, M. Pitkänen, and J. Ott, "Adaptive routing in mobile opportunistic networks," in *Proc. 13th ACM Int. Conf. Modeling Anal., Simulation Wireless Mobile Syst.*, 2010, pp. 101–109.
[15] C. Raffelsberger and H. Hellwagner, "A hybrid MANET-DTN routing scheme for emergency response scenarios," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshops)*, Jun. 2013, pp. 505–510.
[16] J. Whitbeck and V. Conan, "HYMAD: Hybrid DTN-MANET routing for dense and highly dynamic wireless networks," *Comput. Commun.*, vol. 33, no. 13, pp. 1483–1492, 2010.
[17] L. F. Xie, P. H. J. Chong, and Y. L. Guan, "Routing strategy in disconnected mobile ad hoc networks with group mobility," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, p. 105, 2013, doi: 10.1186/1687-1499-2013-105.
[18] H. Chen and W. Lou, "GAR: Group aware cooperative routing protocol for resource-constraint opportunistic networks," *Comput. Commun.*, vol. 48, no. 7, pp. 20–29, Jul. 2014.
[19] C. Liu and J. Wu, "On multicopy opportunistic forwarding protocols in nondeterministic delay tolerant networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1121–1128, Jun. 2012.
[20] X. Tie, A. Venkataramani, and A. Balasubramanian, "R3: Robust replication routing in wireless networks with diverse connectivity characteristics," in *Proc. 17th Annu. Int. Conf. Mobile Comput. Netw.*, 2011, pp. 181–192.
[21] T. Phe-Neau, M. D. De Amorim, and V. Conan, "The strength of vicinity annexation in opportunistic networking," in *Proc. IEEE, INFOCOM*, Jun. 2013, pp. 3369–3374.
[22] X. Zhang and G. Cao, "Efficient data forwarding in mobile social networks with diverse connectivity characteristics," in *Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2014, pp. 31–40.
[23] Z. J. Haas and T. Small, "A new networking model for biological applications of ad hoc sensor networks," *IEEE/ACM Trans. Netw.*, vol. 14, no. 1, pp. 27–40, Feb. 2006.
[24] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," *Comput. Netw.*, vol. 51, no. 10, pp. 2867–2891, 2007.
[25] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Optimal control of epidemic information dissemination over networks," *IEEE Trans. Cybern.*, vol. 44, no. 12, pp. 2316–2328, Dec. 2014.
[26] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, "Overhaul of IEEE 802.11 modeling and simulation in NS-2," in *Proc. 10th ACM Symp. Modeling Anal., Simulation Wireless Mobile Syst.*, Jul. 2007, pp. 159–168.
[27] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein. *Overhaul of IEEE 802.11 Modeling and Simulation in NS-2 (802.11 Ext)* [Online]. Available: https://dsn.tm.kit.edu/medien/downloads_old/Documentation-NS-2-80211Ext-2008-02-22.pdf
[28] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau. (Jan. 2006). *CRAWDAD Dataset Cambridge/Haggle (v. 2006-01-31)*. [Online]. Available: http://crawdad.org/cambridge/haggle/20060131 and https://doi.org/10.15783/C77G6X
[29] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos, "Modeling human mobility in obstacle-constrained ad hoc networks," *Ad hoc Netw.*, vol. 10, no. 3, pp. 421–434, 2012.
[30] A. Mei and J. Stefa, "SWIM: A simple model to generate small mobile worlds," in *Proc. INFOCOM*, Oct. 2009, pp. 2106–2113.
[31] S. Kosta, A. Mei, and J. Stefa, "Large-scale synthetic social mobile networks with SWIM," *IEEE Trans. Mobile Comput.*, vol. 13, no. 1, pp. 116–129, Jan. 2014.
[32] Z. Ren, W. Liu, X. Zhou, J. Fang, and Q. Chen, "Summary-vector-based effective and fast immunization for epidemic-based routing in opportunistic networks," *Commun. Lett.*, vol. 18, no. 7, pp. 1183–1186, Jul. 2014.
[33] K. Wei, D. Zeng, S. Guo, and K. Xu, "On social delay-tolerant networking: Aggregation, tie detection, and routing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 6, pp. 1563–1573, Jun. 2014.
[34] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE Rap: Social-based forwarding in delay-tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 11, pp. 1576–1589, Nov. 2011.

[35] Q. Yuan, I. Cardei, and J. Wu, "An efficient prediction-based routing in disruption-tolerant networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 1, pp. 19–31, Jan. 2012.
[36] C. Y. Aung, P. H. J. Chong, and R. J. Cai, "Hybrid opportunistic routing in highly dynamic MANET," in *Proc. 23rd Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2014, pp. 1–6.
[37] C. Y. Aung, G. G. M. N. Ali, M. Zhao, R. Cai, and P. H. J. Chong, "Information epidemics control for data delivery in opportunistic networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dec. 2016, pp. 1–6.

CHERRY YE AUNG received the B.Eng. degree in electrical engineering and electronic engineering from Yangon Technological University, Myanmar, in 2009, and the M.Sc. degree in electrical engineering and electronic engineering from Nanyang Technological University, Singapore, in 2010, where she is currently pursuing the Ph.D. degree with the School of Electrical and Electronic Engineering. She then joined ASM Pacific Technology, Singapore, as a Software Engineer, from 2010 to 2011. Her research interests are protocol design and development in cooperative opportunistic networks and V2X communication system development in vehicular networks.



IVAN WANG-HEI HO received the B.Eng. and M.Phil. degrees in information engineering from The Chinese University of Hong Kong, in 2004 and 2006, respectively, and the Ph.D. degree in electrical and electronic engineering from Imperial College London, U.K., in 2010. He was with the System Engineering Initiative, Imperial College London, as a Post-Doctoral Research Associate. In 2007, he spent a summer with the IBM T.J. Watson Research Center, Hawthorne, NY, USA. In 2010, he co-founded P2 Mobile Technologies Ltd., Hong Kong Science Park, and served as the Chief Research and Development Engineer. He is currently a Research Assistant Professor with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University. He was on the Mobile Environmental Sensing System Across a Grid Environment Project funded by EPSRC and the Department for Transport, U.K., and the International Technology Alliance Project funded by the U.S. Army Research Laboratory and United Kingdom Ministry of Defence during his Ph.D. He is also the holder of a U.S. patent. His research interests are in wireless communications and networking, specifically in vehicular ad hoc networks and intelligent transportation systems, physical-layer network coding, and wireless mesh networks. The MeshRanger series wireless mesh embedded system primarily invented by him received the Silver Award in Best Ubiquitous Networking in Hong Kong ICT Awards 2012.

PETER HAN JOO CHONG received the B.Eng. degree (Hons.) from the Technical University of Nova Scotia, Halifax, NS, Canada, in 1993, and the M.A.Sc. and Ph.D. degrees from The University of British Columbia, Vancouver, BC, Canada, in 1996 and 2000, respectively, all in electrical engineering.

From 2000 to 2001, he was with Agilent Technologies Canada Inc., Canada. From 2001 to 2002, he was with the Nokia Research Center, Helsinki, Finland. From 2002 to 2016, he was with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, as an Associate Professor (Tenured). He was an Assistant Head of Division of Communication Engineering from 2011 to 2013 and the Director of Infinitus with the Centre for Infocomm Technology, from 2013 to 2016. Since 2016, he joined the Department of Electrical and Electronic Engineering, Auckland University of Technology, New Zealand, as a Full Professor and Head of Department. He is currently an Adjunct Faculty of The Chinese University of Hong Kong. His research interests are in the areas of mobile communications systems, including radio resource management, multiple access, MANETs, multihop cellular networks, and vehicular communications networks.

Dr. Chong was a Technical Program Committee Chair at the Mobility Conference in 2005 and 2006, a Chair at the Mobility Conference in 2007 and 2008, a TPC Co-Chair at the IEEE International Conference on Networks in 2012, and a General Chair at the International Conference on Information, Communications, and Signal Processing in 2013. He served as a lead Guest Editor of the *IEEE Communications Magazine* in 2007 and the IEEE Wireless Communications in 2011. He is an Editorial Board Member of *Security and Communication Networks* and an Editor of *KSII Transactions on Internet and Information Systems*.