DONM: Domain-based Opportunistic Networks Model in Emergency Scenarios

Xia Wang, Wen-Wen Pan, Xu-Hong Li, Xiao-Fei Sun, Wei Zhang, Tao Xu

College of Information Science and Engineer, Zaozhuang University, Shandong Province, China
E-mail: wangxia1026@163.com

Abstract-Sudden Disaster always damages communications infrastructure, adding to the difficulties of rescue efforts. To address this problem, this paper studies the features of post-disaster emergency communication scenario and proposes specific Domain-based Opportunistic Network Model (DONM) which divides an opportunistic network into different domains according to the geographic location and node attributes. Further, Domain-based Message Dispatching Scheme (DMDS) is proposed to resolve efficiently the problem of message dispatching in DONM. DMDS utilizes the frequently moving of active rescue mobile nodes to implement message distribution among domains. Simulation results show that DONM and DMDS can implement poster- disaster emergency communication efficiently and completely.

Keywords-emergency communication; DONM; DMDS

I.   INTRODUCTION

Huge sudden natural disasters and accidents invariably damage or even destroy public communication infrastructure. How to build up an efficient post-disaster emergency communication network to guarantee the communication capabilities is an important problem for post-disaster rescue and recovery. Although many advanced emergency communication technologies have be proposed, they need massive resources support and are difficult to set up in a short time [1]–[4].

Opportunistic networks (OppNet) utilize encounter opportunities to complete message propagation among mobile nodes, which provides a great way to establish emergency communication networks for post-disaster rescue and recovery. In this paper, we propose the specific application of OppNet in emergency scenarios. Our objective is to build up efficient opportunistic networks model for emergency communication and establish specific message dispatching scheme for transmitting the message between the rescue nodes and victim nodes in a time-efficient and completely way.

By careful investigation into poster-disaster situation of the Wenchuan and Yushu earthquakes and other nature disasters, we find that post-disaster emergency communication devices include four nodes: (1) Victim Node - smartphones from the victims or missing, (2) Active Node - smart devices from rescuers, (3) Circuiting Node - mobile rescue devices from the recovery aircrafts, and (4) Rescuing center Node - communication devices in rescuing center. And poster-disaster emergency communication introduces three following features: (1) earthquake-prone terrain mostly strikes in the very mountainous areas or the coastal regions, and often trigger other nature disasters,

which makes fixed network infrastructure not be used to establish the emergency networks in a long time; (2) victims of disaster mostly crowd around some villages, communities, or refuges; (3) rescue nodes' fluidity is greater. Fig. 1 shows the post-disaster scenario.
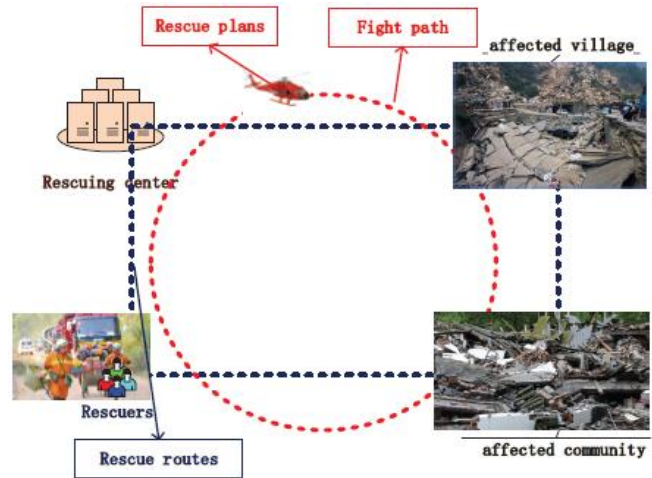

Figure 1.   Emergency communication scenario.

In light of this, we in this paper propose Domain-based Opportunistic Networks Model (DONM) to build up an efficient model suitable for post-disaster scenario. DONM divides an OppNet into two kinds of domain according to the geo- graphic location and node attributes: (1) branch domain which is formed by dividing all victim nodes into different clusters according to the geographic location; (2) backbone domain which consists of securing center nodes, active nodes and circuiting nodes. And we also propose Domain-based Message Dispatching Scheme (DMDS) for message dispatching in DONM, which satisfies the following three requirements: efficiency that means achieving the dispatching task in a time- efficient way; accuracy means receiving the correct message by sink node; completeness that means dispatching every message with certainty. To achieving this goal, DONM first votes the speakers in each branch domain which can communicate with backbone domain directly, and later DMDS constructs the forwarding table for forwarding the datagram inside each fixed domain.

The main contributions of this paper are summarized as follows: 1) To the best of our knowledge, we formulate specific OppNet model DONM under post-disaster scenario; 2) we propose a time-efficient, complete and accurate message dis- patching scheme DMDS; 3) we conduct extensive simulations to evaluate our scheme's performance.

The rest of the paper is organized as follows. Section II states related work. Section III states the poster-disaster emergency communication problem and proposes DONM model. V present Domain-based Message Dispatching Scheme DMDS. Section VI evaluates our scheme. Finally, Section VII concludes this paper.

II. RELATED WORK

In recent years, Most of studies on opportunistic network shift to routing protocols [5], [6] and Crowdsensing [7], [8]. A few studies on poster-disaster communication focus on opportunistic networks, such as [1],[9],[10]. An observer-based distributed scheme is proposed for sel.sh-node detection in a post-disaster communication environment in [1]. A coherent global view is proposed for poster-disaster situation awareness in [9]. A Group-based Multilayer Encryption Scheme is proposed for secure dissemination of post-disaster situational data in [10]. Although these works proposed advanced technologies, they have not build up proper model and message dispatching scheme aiming at poster-disaster emergency communication.

III. PROBLEM STATEMENT

Post-disaster emergency communication network is usually composed of substantial victim Nodes (VN), multiple Active Nodes (AN), one or more Circuit Nodes (CN) and one Rescuing center Node (RN). In order to analyze our problem more clearly, we just de.ne one RN node, one CN node, n AN nodes and m VN nodes in our system model (n .. m). According to the analysis, we .nd VN nodes have a community distribution, and the mobility of AN nodes and CN nodes has regular routes. CN nodes can .y around the stricken areas independently and communication with the rescue center. AN nodes can be brought into some community by rescuers. Most of VN nodes are limited into a community. Four kind of nodes are formulated for ease of presentation of problem. (1) VN nodes: represents the victim nodes which refer to smartphones nodes carried by victims or missings and are divided into different domains according to geographic location. (2) AN nodes: represents the active nodes which refer to smartphones nodes carried by ' rescuers and belong to a domain. (3) CN nodes: represents the circuit nodes which refer to intelligent devices belong to a domain. (4) RN node: represents the rescuing center node which is responsible for collecting, storing and relaying the post-disaster rescuing information.

With the knowledge of these nodes a priori, the problem of this paper is to build up opportunity network model and message dispatching scheme. Our objective is to transmit the message to sink node in a time-ef.cient, accurate, and complete way.

IV. DOMAIN-BASED OPPORTUNISTIC NETWORKS MODEL

In this section, we propose a Domain-based Opportunistic Networks Model (DONM) which can build up an opportunistic network model for post-disaster emergency communication.
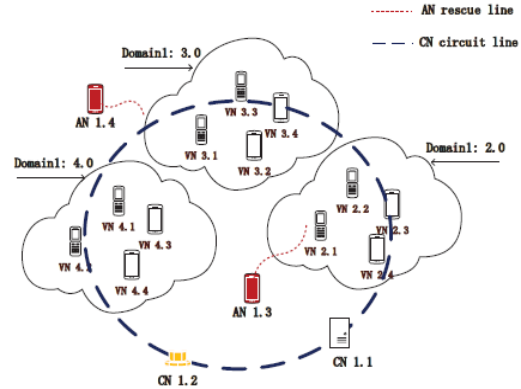

Figure 2. DONM model.

A. Model Overview

Based on the above, we build up a Domain-based Opportunistic Network Model. In DONM, the whole OppNet is divided into multiple domains according to location and node attributes. According to the attributes of inner nodes, domains fall into two categories: backbone domain and branch domain. Each domain is denoted as two-byte dotted-decimal notation. The system model is shown as Fig. 2. Two domains in our model are formulated for ease of presentation later.

1) Backbone domain

which is denoted by D1 which refers to RN, CN, and AN node set. The network address of backbone domain is ' 1.0 ' . CN node in backbone domain is responsible for collecting the data from branch domains either directly or indirectly and transferring the data to RN node. In our model, D0 contains three kinds of nodes. The network address of RN is '1.1', the network address of CN is '1.2', and the network address of AN is '1.3', '1.4', ... '1.5'.

2) Branch domain

which is denoted by Di (i> 2) which refers to VN node set. In opportunistic network, all VN nodes is divided into multiple subsets according to location, and each subset corresponds to a branch domain represented by Di = {VN1,VN2, ...V Nl} of l nodes. The network address of each branch domain is 'i.0'. The network addresses of victim nodes in Di are 'i.1', 'i.2 ', ... ' i.m' .

B. Model Details

For emergency communication, how to build up DONM model reliably and fleetly under current conditions is a key problem. DONM constructing consists of three phases: (1) Defining the backbone domain. All CN nodes, AN nodes, and RN node are classified into backbone domain. Backbone domain is responsible for the message transferring among domains by constantly moving. (2) Dividing the whole opportunistic network into different branch domains according to the map. A village or a community range often is defined as a branch domain. All VN nodes can position their domains by GPS module in smart devices. (3) Spreading the DONM topology to all nodes. DONM spreads the network topology to all nodes by flooding.

1) Defining backbone domain

In this model, we de.ne a backbone domain. Backbone domain consists of two kinds of nodes: (1) one RN node who is in charge of collecting, storing and analyzing the message, and helps dividing the branch domains and deciding rescuing scheme; (2) one CN node and many AN nodes who are in charge of message transferring between the RN node and branch domains.

2) Dividing branch domains

In this phase, RN node divides the whole OppNet into the different branch domains by investigating the affected disaster areas. The whole dis-aster area is divided into different branch domains roughly according to the distribution of villages and communities. Each branch domain is further verified seamlessly according to latitude and longitude. Branch domain is also divided into many geographical units (G-unit), multiple modes have the same network address. Each VN node determines its network address according to the latitude and longitude provided by the GPS module in smartphones.

3) Spreading DONM topology

Each node floods the abstract of the topology of backbone domain to the nodes who can communicate with it until all nodes knows. After the flooding, all nodes have the knowledge of backbone domain.

Through above three phases, DONM is constructed. And during the build process, the profile of DONM topology is stored in AN node. Each node stores the network address of the backbone domain and its own branch domain. Algorithm 1 shows the process of DONM constructing.

Algorithm 1: DONM Constructing

1: Define the backbone domain and branch domain.

2: Rescuing center determines RN node, CN node and

all AN nodes belongs to the backbone domain 1.0.

3: Rescuing center assigns RN node address as '1.1 ',

CN node address as '1.2', and AN node address as

'1.3', ... '1.n'.

4: Rescuing center assigns addresses to branch domain.

5: Partition a branch domain into many G-unit and assign

each unit an address following certain rules.

6: Flooding the information of DONM topology.

7: **for** each node **do**

8: Calculate its latitude and longitude by GPS module.

9: Determine network address according to its G-unit.

10: **end for**

V. DOMAIN-BASED MESSAGE DISPATCHING SCHEME

For achieving efficient communication effect in post-disaster emergency communication network, we propose Domain-based Message Dispatching Scheme (DMDS) whose objective is completing message dispatching efficiently in DONM.

A. Overview

To achieve the objective, each domain votes the speaker nodes which are responsible for transiting the messages between the branch domain and backbone domain. Each node stores two tables: (1) speaker table which stores the speakers' information in its domain, and (2) forwarding table which gives the node routing information of dispatching the message. The items in two tables are shown as Tab. I and II respectively.

TABLE I. SPEAKER TABLE

Speaker	Distance	Time

TABLE II. FORWARDING TABLE

Destination address	Next hop	Hop count

In Tab. I, the item of speaker stores the network address of speakers in this domain, the item of distance stores the hop count between itself and speaker, and item of time stores the timestamp of the speaker.

B. Protocol Details

DMDS consists of two phases: defining the domain speakers, building up forwarding table and dispatching message.

1) Defining the domain speakers

Speakers refers to the nodes on the way of CN circuiting or AN walking. Speakers can communicate with CN node or AN node directly. CN node and AN node send hello datagram continually when they are flying or walking. When a node in a branch domain receives hello datagram from the backbone domain directly, the node considers itself as speaker and floods the information in the branch domain. Defining speaker process is shown as Algorithm 2.

Algorithm 2: Defining Speakers

1: CN node and AN nodes broadcast 'Hello' datagram

when they are circuiting and walking.

2: The node receives 'Hello' datagram.

Searching the speaker table:

4: L = num of records in speaker table.

5: **for** (i = 0; i < L; i + +) **do**

6: S.A. = source address of datagram

7: **if** S.A. != speaker **then**

8: Append the record of (S.A., 1, timestamp) to

speaker table.

9: **else**

10: Update the existing record to (S.A., 1, timestamp).

11: **end if**

12: **end for**

All nodes in the same domain share their speaker table with each other by sending the abstract of speaker table periodically. The datagram which encapsulates the abstract of speaker table is called as update datagram. Each node updates its speaker table dynamically by sharing speaker table. Algorithm3shows the process of sharing the speaker table.

2) Building up forwarding table and dispatching message

In DMDS, each node in branch domain stores a forwarding table. When the node receive a message, it dispatches the message according to the forwarding table. Forwarding table is built up in Algorithm 4.

Algorithm 3: Sharing Speaker Table

1: The node sends 'Update' datagram periodically.

2: The node receives 'Update' datagram.

3: Searching the speaker table in itself:

4: Compare the speaker table in 'Update' datagram with its own speaker table.

5: Update the speaker table.

Algorithm 4: Forwarding table constructing

1: Receive the message and read the source address of the message.

2: S.A. = source address

3: Search the forwarding table:

4: L = num of records in forwarding table

5: **for** (i = 0; I < L; i + +) **do**

6: **if** S.A. != destination address **then**

7: Append the record of (S.A., S.A., 1) to forwarding table.

8: **end if**

9: **end for**

10: Search the forwarding table:

11: Read the destination address.

12: Traverse the forwarding table and matching any record.

13: **if** Destination address matches any record **then**

14: Forward the message to next hop.

15: **else**

16: Broadcast the message.

17: **end if**

VI. EVALUATION

In this section, we evaluate the performance of DONM and DMDS through simulations. We study the features of delay and packet loss rate.

A. Simulation Setting

Our simulation environment is Matlab R2014a. We generates 100 nodes randomly in 100*100 area. The area is partitioned into 100 grid units, each of which is 10*10 square. The node steps a grid unit as a hop. A hop also express the distance from speaker node to AN or CN node, and the distance from AN or CN node to RN node. The simulation design is shown in Fig. 3.

B. Delay and Loss Rate

Now we study in greater details the delay and packet loss rate. In order to describe the performance more clearly, we set the hop count from the source node to RN node as the delay of the packet. We simulate each node sending the packet randomly for 100 trials, and we gain the average of 100 hop counts as delay of packet. The simulation result is shown in Fig. 4. We generate 100 nodes randomly for 100 round, and gain the packet loss rate in each round. The simulation result is shown in Fig. 5. By of simulation result, the average delay is 5.57 hop count and the average packet loss rate is 7.66%.
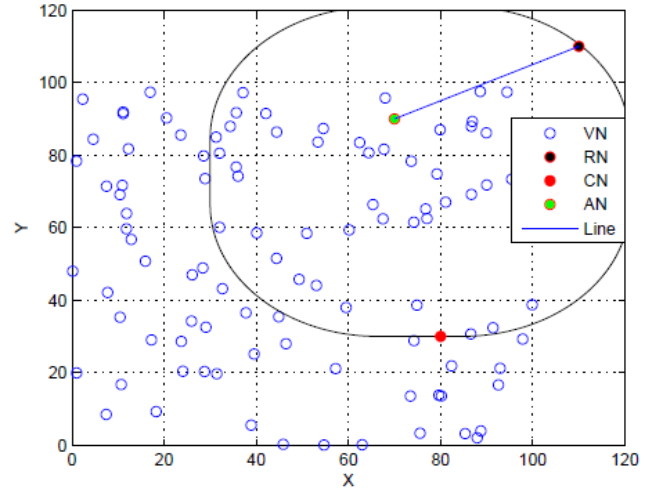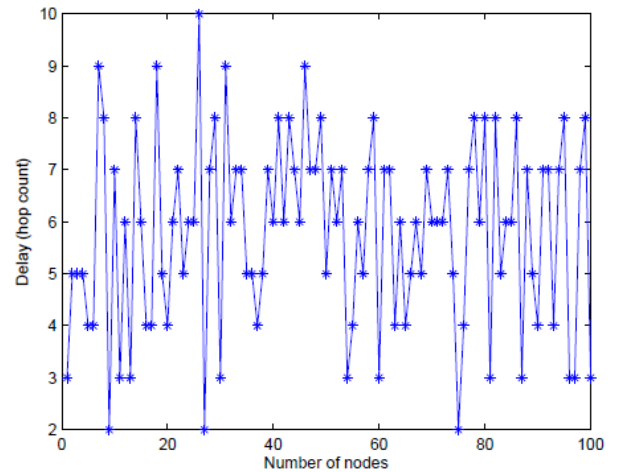

Figure 3. Simulation Design.
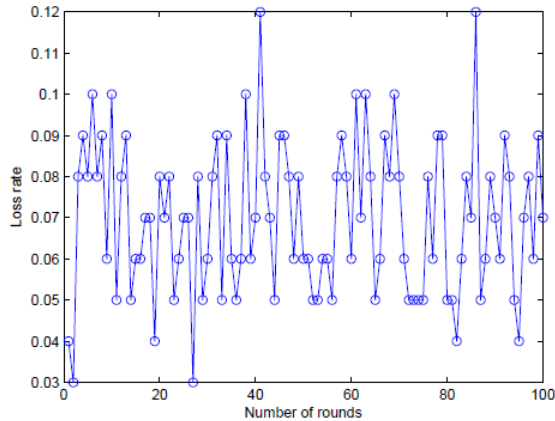

Figure 4. Delay of DONM.

Figure 5.   Packet loss rate of DONM.

VII.   CONCLUSION

This paper investigates the problem of how to build up OppNet model and message dispatching scheme in post-disaster emergency communication. To address this problem, we propose the specific Domain-based Opportunistic Networks Model (DONM) and Domain-based Message Dispatching Scheme (DMDS) that divides an opportunistic network into different domains according to the geographic location and utilizes the frequently moving of active rescue mobile nodes to implement message distribution among domains. Simulation results show that DMDS can implement poster-disaster emergency communication efficiently and completely.

ACKNOWLEDGMENT

REFERENCES

[1] [1] R. S. Chakrabarti C, Banerjee A, "An observer-based distributed scheme for sel.sh-node detectionina post-disaster communicationenvironment using delay tolerant network," in Applications and Innovations in Mobile Computing, 2014, pp. 151 – 156.

[2] [2] R. S. Chakrabarti C, "Adapting mobility of observers for quick repu-tation assignment in a sparse post-disaster communication network," in Applications and Innovations in Mobile Computing, 2015, pp. 29 – 35.

[3] [3] M. M. Hasegawa G, Kamei S, "Emergency communication services based on overlay networking technologies," in International Conference on NETWORKING and Services, 2008, pp. 159 – 164.

[4] [4] R.S.TakahiroM, "Aglobal reputation estimation and analysis technique for detection of malicious nodes in a post-disaster communication environment," in Applications and Innovations in Mobile Computing, 2014, pp. 179 – 185.

[5] [5] F. Z.W.T.WentaoWang, Feng Guo and J.Wang, "Research on routing protocols and simulation analysis for opportunistic networks," Interna-tionalJournalof Multimedia and Ubiquitous Engineering, vol. 10, no. 3, pp. 181–202, 2015.

[6] [6] J. K. J. O. Suzan Bayhan, Esa Hyytia, "Two hops or more:on hop-limited search in opportunistic networks," in ACM MsWiM 2015, 2015, pp. 115

[7] – 124.

[8] [7] K. I. Karaliopoulos M,Telelis O, "User recruitment for mobile crowd-sensing over opportunistic networks," in IEEE INFOCOM, 2015, pp. 2254 – 2262.

[9] [8] H.T. e. a. HiguchiT,Yamaguchi H, "A neighbor collaboration mecha-nism for mobile crowd sensing in opportunistic networks," in IEEE ICC, 2014, pp. 42 – 47.

[10] [9] R. S. e. a. Mukherjee A, Basu S, "Developing a coherent global view for post disaster situation awareness using opportunistic network," in International Conference on Communication Systems and Networks, 2015, pp.1 – 8.

[11] R. S. Basu S, "A group-based multilayer encryption scheme for secure dissemination of post-disaster situational data using peer-to-peer delay tolerant network," in International Conference on Advances in Computing, 2014, pp. 1566 - 1572.