IAENG International Journal of Computer Science, 42:2, IJCS_42_2_10

Supporting User Communication in Disaster-Hit Area Using Mobile Ad Hoc Networks

Jiahong Wang, Yuhiro Yonamine, Eiichiro Kodama, and Toyoo Takata

***Abstract*—In disaster-hit area, communication supporting systems using existing mobile ad hoc network techniques could not function as expected and communication would be interrupted from time to time, since the issue of sleep, which is a general means for users to save their battery consumption, has not been taken into consideration. Especially, a phenomenon called sleep thrashing would occur, which collapses mobile ad hoc networks. This paper proposes an approach to solving the problem. For the proposed approach, firstly, a house-watching network is used to take charge of waking up the sleeping terminals, so that periodic or planned communication is supported and users can freely get into sleep at their conveniences. Secondly, sleeping activities are incorporated into the routing protocol, so that users' consideration for other people can be technically supported, and they can know if their terminals are functioning as routers, and when sleeping buttons of their terminals can be pushed down safely without interrupting the relaying in progress, and so without interfering with others' communication.**

***Index Terms*—mobile ad hoc network, energy-saving, sleep thrashing, house-watching network, routing and sleeping protocols.**

I. Introduction

On March 11, 2011, an earthquake of magnitude 9.0, which was the largest one in Japan's history, struck off the coast of the northern part of the country, churning up a devastating tsunami that swept over cities and farmland, and took away almost everything, including the power supply system and communication system. Experiencing the disaster, we found that it is necessary for us to have a communication supporting system for the emergency use in the disaster-hit area.

We really did not lack communication supporting systems. Unfortunately, no one of them functioned as expected when the earthquake and tsunami occurred. At that time the fact is that, telephone, email, internet, and television became unavailable, and people were isolated from the outside world. Since no means of communication were available, people could not communicate with each other, and thus became very anxious that, e.g., whether the foods and water in hand were enough to survive the disaster, when the basic infrastructure for livelihood could be restored, and where medical cares could be provided. A communication supporting system that could connect everyone together was really necessary.

We think the Mobile Ad Hoc NETwork (MANET) can be a good candidate to serve a communication infrastructure for emergency use in disaster-hit area. This is because for MANET, we can use the *mobile terminals* such as telephones, notebook type personal computers, and other mobile equipments (also called nodes thereafter) for communication. No power supply systems but the battery of mobile terminals, no center server for assisting communication, and no predetermined plan for the network backbone are needed. We can have a network at any time and any place, and use the network as we do just before disaster happens.

The authors are with the Faculty of Software and Information Science, Iwate Prefectural University, Takizawa, Iwate, 020-0193 JAPAN, e-mail: wjh@iwate-pu.ac.jp.

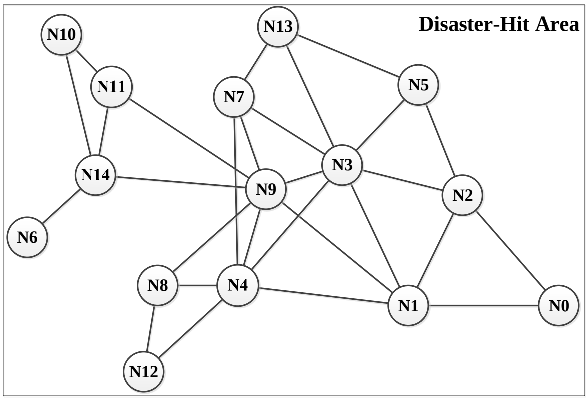

Fig. 1. In this example, terminal N_9 would function as a router for relaying data between, e.g., N_{10} and N_2.

It was found, however, in disaster-hit area, communication supporting systems based on the existing MANET techniques could not function as expected; network could not last long enough, and communication would be interrupted from time to time. There are two reasons for this problem. Firstly, mobile terminals are all battery-driven and the battery cannot be recharged due to the damaged power supply system. Secondly, existing MANET techniques have not taken into consideration the sleep operations of mobile terminal users. We observed that mobile users at the disaster-hit area have such a common and unique characteristic that, they do not change their locations very often, but very frequently take advantage of putting their mobile terminals to an energy-saving state called sleep. Unless it became necessary to communicate with others, people tended to keep sleeping to save battery consumption for use in an emergency. Especially, whenever one found her communication partner unreachable, it was highly possible for her to get to enter sleep state immediately. When putted to sleep, a mobile terminal immediately stops what it is doing, including all its routing tasks, resulting in all the routes that take the mobile terminal as a router become broken. Due to the uncontrolled seeping operations, it is difficult to have a stable and useable network. For example, the owner of mobile terminal N_9 in Fig. 1 may just finish sending an email to her friend and thus close her mobile terminal, resulting in the communication between N_{10} and N_2 becomes interrupted, since N_9 serves also as a router for relaying data.

(Advance online publication: 24 April 2015)

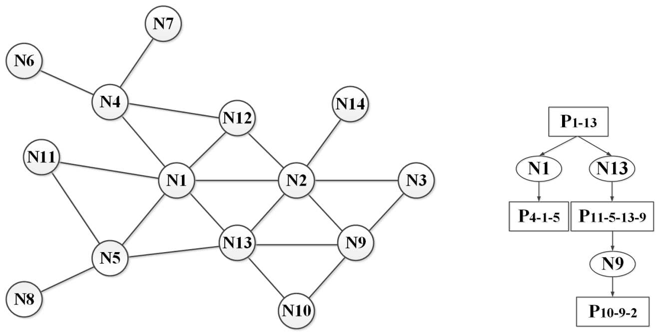

Fig. 2. An oval represents such a mobile terminal that is an end user for the communication shown in the box above it, and whose sleep can break the communication path shown in the box below it.

We have also observed a new phenomenon (named as *sleep thrashing*) for the MANET in disaster-hit area that, putting mobile terminals into sleep may bring a MANET-based communication system into a collapsing state. Take as an example the following scenario of the MANET given in the left figure of Fig. 2. Mobile terminal N_1 is talking with N_{13}. At the same time, there are three pairs of communication process are in progress such that N_4, N_{11}, and N_{10} are being connected to N_5 via N_1, N_9 via N_5 and N_{13}, and N_2 via N_9, respectively. For simplicity, we denote the communication process from N_s to N_d via N_r as $P_{s,r,d}$. Then the scenario is represented by $S_t = \{ P_{1-13}, P_{4-1-5}, P_{11-5-13-9}, P_{10-9-2} \}$. Assume that as soon as N_1 and N_{13} finish their communication, they get to enter sleep state to save battery consumption. Then caused by their sleep, the communication processes P_{4-1-5} and $P_{11-5-13-9}$ become interrupted due to the broken link, and N_4, N_5, N_{11} and N_9 get to enter sleep state, too. In turn, caused by the sleep of N_9, P_{10-9-2} becomes interrupted, and N_{10} and N_2 also get to enter sleep state. This snowball effect continues with mobile terminals entering sleep state calling for more mobile terminals entering sleep state, and finally it is possible for almost all mobile terminals to become unreachable, and the network becomes collapsed.

The sleep thrashing phenomenon exemplified above is further demonstrated in the right figure of Fig. 2. At a specific point in time, it happens that a long chain of communication paths is formed, heading with that of N_1. The sleep of N_1 triggers off the sleep thrashing. In fact, people generally communicate with only a few specific other people, and when the communication finishes or becomes impossible, to enter sleep state is beneficial to them. So the sleep thrashing essentially results from people's psychological state of excessively and anxiously saving their battery consumption. If they do not take the battery lifetime as an issue due to the existence of power supply systems, and do not hurry to put their mobile terminals to sleep, then it would be difficult for sleep thrashing to occur. Therefore, we think that without the mobile users' cooperation, the mobile terminal and MANET themselves cannot cope with the sleep thrashing problem.

Fortunately, we also noted that in the disaster-hit area, people tended to be considerate of others and actively keep discipline and order. We therefore can reasonably make such an assumption that, people in the disaster-hit area would not be so selfish as to turn off their mobile terminals given that they know others are using their mobile terminals for relaying data, and they would cooperate to maintain a MANET given that they know it would benefit all the people there, including themselves. The problem is that, however, they cannot know whether their mobile terminals are serving as routers or not, whether closing their mobile terminals would interrupt others' communication and trouble them, and for how much time they should delay closing their mobile terminals so that the communication tasks through their mobile terminals could finish without interruption.

Then in order to have an effective communication supporting system for the emergency use in the disaster-hit area, we have to solve two problems: maximize the lifetime of a MANET as a whole, and make routing activities at the IP layer viewable to users. For the purpose, in this paper we propose a system model with an effective algorithm. The first problem is solved by creating a house-watching network to take charge of waking up the sleeping terminals, so that periodic or planned communication is supported and users can freely get into sleep at their convenience. The second problem is solved by incorporating the sleeping activities into the routing protocols, so that users' consideration for other people can be technically supported, and they can know if their terminals are functioning as routers, and when sleeping buttons of their terminals can be pushed down safely without interrupting the relaying tasks in progress, and so without interfering with others' communication. We also address the issue of sleep thrashing in theory, and give a revised version of the proposed algorithm to relieve the negative effect of the sleep thrashing. Results of simulation experiments demonstrate the effectiveness of the proposed approach.

In the rest of this paper, Section II formally define the problem. Section III gives an approach to solving the problem. Results of performance study are discussed in Section IV. Sleep thrashing is addressed in Section V. Finally, Section VI concludes the paper.

II. Problem Statement

The problem to be solved in this research, as described in Section I, is formulated as follows.

Problem Statement. *Consider such a mobile ad hoc network that is located at a disaster-hit area, consists of an administration center and a group of user mobile terminals driven by batteries, and batteries cannot be recharged due to the damaged power supply system. The aim is to support communication on the network for as long time as possible. The objective is two-fold. On the one hand, lifetime of the overall network should approach the one when mobile terminals are used solely for their owners' own purposes without the duty of relaying others' data. On the other hand, a mobile terminal should be able to enter sleep state at its owner's convenience, but the communication tasks of other users should not be affected. An approach is to be devised to achieve the objective.*

For increasing the lifetime of a mobile ad hoc network, a promising solution is to construct a Connected Dominating Set (CDS) [1]–[6], and to use the CDS-based routing. In general, a Dominating Set (DS) of a graph $G = (V, E)$ is a subset $V' \in V$ such that each node in $V - V'$ is adjacent to at least one node in V', and a CDS is a DS whose induced sub-graph is connected. CDS-based routing is such a routing method that selects certain nodes from the network as gateway nodes. These gateway nodes form a CDS and are responsible for routing within network.

The CDS-based approach is widely used for constructing network backbones, and here can be used as a *house-watching network*. That is, we can take each CDS node as a watchdog node, and let other nodes sleep freely. Unfortunately, the existing CDS-based approaches cannot help to solve the problem defined above satisfactorily. Firstly, we need such a network that is of a well-defined structure, so that if a watchdog node fails to function due to, for example, battery problem or careless sleep operation, a human-intervention can be possible. Secondly, applications in the disaster-hit area require that a house-watching network should be initially constructed around the administration center, but migrate autonomously to the center site of the network area so that the network diameter and number of watchdog nodes become minimized, and thus, the delay of broadcasting a message can be minimized and the number of sleeping nodes can be maximized. More importantly, fault-tolerance can be enhanced.

Some similar work can be found in [7]–[10], where a new factor called the diameter, which is the longest shortest path between any pair of nodes, is considered, and the problem is to minimize the diameter so that routing is easier and can adapt quickly to topology changes of a network. The difference from this research is that, in this paper the diameter is the longest shortest path between the administration center or its proxy node and any other nodes, the "center" of network has to be located autonomously, and by which the diameter is minimized. Some other low cost approaches for constructing CDS have been proposed [11]–[16]. For the defined problem, however, these approaches could not be very helpful.

For avoiding interrupted communication caused by mobile terminal sleeping activities, we have not found any research results dealing with the subject of integrating the sleeping and the routing protocols. In fact, they have been considered as two independent concepts for different purposes, and integrating them has been considered unnecessary and impossible. For the disaster-hit area, however, we found the integration is really necessary so that a more effective and friendly communication supporting system can be obtained.

Some other related work can be found in [17], [18]. In [17] a novel risk notification message dissemination protocol to propagate risk notification messages from the location of origin (called the risk zone) to the vehicles approaching the risk zone was proposed. In [18], authors addressed the subject of improving performance of an ad hoc network system suffering from high resource contention by improving its packet delivery fraction when necessary. Both could be helpful in improving the communication in disaster-hit area, but could not provide an effective solution to the above defined problem.

III. House-Watching Network and Routing Aware Sleeping Protocol

As stated above, there are two factors that make an ad hoc network difficult to hold at the disaster-hit area: limited battery lifetime and frequent sleep operations. In this section, firstly, a phased communication system model is presented

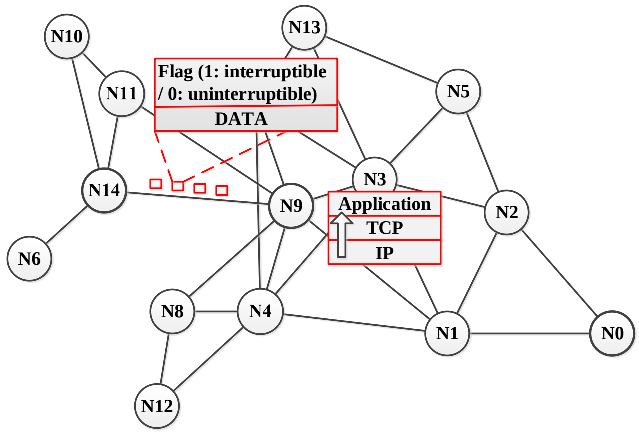

Fig. 3. An example for illustrating the system model. Node N_{14} and N_0 are exchanging messages via node N_9.

which can be helpful to sustainable communication. Then, notations, definitions, and some fundamental concepts are provided, on the basis of which, an approach to solving the problem defined in Section II is proposed.

A. Phased Communication System Model

The system for solving the problem defined in Section II is modeled as an ad hoc network $G = (V, E)$ as shown in Fig. 3. A House-Watching Network (HWN) as defined in Definition 4 is constructed. All users except the HWN ones, or all users except the proxy and the administration center can enter sleep state. The sleeping nodes will be woken up in specified time interval, or according to totalized user requests.

When users are woken up, they can communicate with each other, and then enter sleep state again to save their battery consumption. At that time, they may make requests to the administration center or its proxy to specify when they should be woken up the next time.

We also noticed that uncontrolled sleeps may make the ad hoc network disconnected, and other users' communications interrupted. Fortunately, we also found that people in the disaster-hit area would be like to help each other in various aspects, including the maintenance of an ad hoc network for their own communication. Therefore, the routing table is assumed to be viewable to users (e.g., N_9 in Fig. 3), and a user can make her decision of pushing down sleep button according to information from the IP layer, so as to not interfere with the users (e.g., N_{14} and N_0 in Fig. 3) who are using the node for relaying data.

To be not blocked for too long time, we assume that the users who are communicate with each other could indicate whether other users can push down their sleep buttons without any negative effect by setting a sleeping-save flag in the IP packets. User N_9, for example, may be so kind as to not trouble users N_{14} and N_0 by pushing down sleep button when she makes sure that the action is save by checking the sleeping-save flag. The time interval between two adjacent interruptible IP packets is called as a session as defined below.

Definition 1 (Communication Session)**.** *A session of a communication task is the time interval between two IP* *packets which sleeping-save flags have been set to 1. Note that sleeping-save flags of the first and the last IP packets are always set to 1.*

Since uncontrolled sleeps may make an ad hoc network disconnected, and communication processes interrupted, we create and maintain a multi-hop CDS. CDS nodes are given two responsibilities. On the one hand, they constitute a virtual backbone. On the other hand, they function as watchdog nodes. All users except the CDS ones can freely put their mobile terminals to sleep at their convenience. The sleeping nodes will be woken up by CDS nodes in specified time interval, or according to totalized user requests.

When a user (say, N_i) is woken up, she will select a communication time T_{N_i} from set T_{comm} according to her requirement, communicate with others for less than or equal to T_{N_i} minutes, and then enter sleep state again to save battery consumption. At that time, she may make a request to the administration center or its proxy to specify when she should be woken up the next time. The multi-hop CDS should be reconstructed before any node gets to sleep. Note that set T_{comm} (say, $\{1, 3, 5, 8\}$) is a set of valid communication times, which is defined by the administration center and broadcast to all users when the system is initially started.

B. Definitions and Preliminaries

An undirected graph $G = (V, E)$ is used to represent an ad hoc network, where V is the set of nodes and $(u, v) \in E$ is the transmission link between nodes u and v. That is, (u, v) is in E if nodes u and v are within the transmission range of each other. Without losing generality, it is assumed that the nodes in V are located in a plane, and all nodes are homogeneous, meaning that they have the same transmission range.

It is assumed that in a disaster-hit area, there is an administration center that takes charge of running it. The administration center can assign some other node as a *proxy* to take some of its duties such as broadcasting messages.

A house-watching network is a CDS as defined below, with as many nodes as possible being able to sleep, and as few nodes as possible being watchdog nodes. Watchdog nodes should be able communicate with the administration center or its proxy by the shortest route, so that important messages can be broadcast to every node with little delay.

Definition 2 (DS)**.** *A Dominating Set (DS) of* $G = (V, E)$ *is such a node set* V' *that* $\forall (v, w) \in E$, $v \in V'$ *or* $w \in V'$.

Definition 3 (CDS)**.** *A CDS of* $G = (V, E)$ *is such a DS of G that the subgraph of G induced by the nodes in this set is connected. The size of a CDS is equal to its node number.*

For a given ad hoc network G, finding a House-Watching Network (HWN) over G as defined below will be addressed in the next section.

Definition 4 (HWN: House-Watching Network)**.** *An HWN of* $G = (V, E)$ *is such a CDS of G that has a tree structure and is of the minimal diameter.*

Definition 5 (Diameter)**.** *Given an ad hoc network G = (V, E),* $N_A \in V$ *is the administration center, and* $N_P \in V$ *is a proxy of it. The diameter of G is the length of the longest shortest paths between any* $u \in V$ *and* N_A *or* N_P.

TABLE I
NOTATIONS USED IN THIS PAPER

notations	meanings
S_{HWN}	An HWN.
N_{AdminC}	The administration center, which is responsible for initializing and maintaining HWN
N_{proxy}	The proxy node of administration center.
u.Diameter	Diameter of node u.
u.House-Watch	True if u is a house-watching node
u.color	A field for assisting construction of S_{HWN}

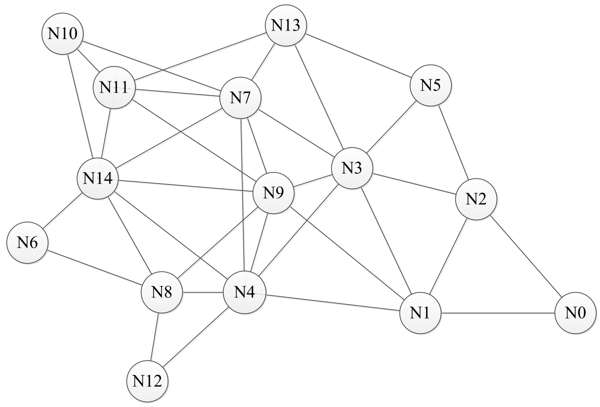

Fig. 4. An ad hoc network for illustrating the algorithm given in Func. 1.

The term thrashing generally describes a phenomenon in transaction processing systems where an increase of the load of a transaction processing system results in a decrease of its throughput. It violates the intuition that throughput should increase smoothly toward a saturation level as load increases. We have observed a similar phenomenon for ad hoc networks in the disaster-hit area, and introduce a new concept of sleep thrashing, and define it as below.

Definition 6 (Sleep Thrashing)**.** *Sleep thrashing is such an iterative process that, starting from an initial state of a few mobile terminals entering sleep state, the mobile terminals that enter sleep state cause more other mobile terminals enter sleep state, and finally, the network becomes collapsed.*

C. Algorithm for Constructing HWN

The algorithm for constructing HWN is given in Func. 1, which will be used by the administration center. Symbols used in the algorithm is summarized in Table I.

D. An Example for Illustrating Func. 1

Assume that we have an ad hoc network shown in Fig. 4, where node N_0 is the administration center.

Starting from administration center N_0, the algorithm will construct an initial HWN as shown in Fig. 5.

Because the path <N_0, N_1, N_9, N_{14}> is the longest one, in the next step, in place of N_0, N_1 becomes a proxy of the administration center, and we have the HWN shown in Fig. 6.

Function 1 Construct a house-watching network

Require: A set of mobile nodes

Ensure: A house-watching network as defined in Def. 4

1: Set $N_{proxy\text{-}pre}$ and N_{proxy} to N_{AdminC}, $N_{proxy\text{-}pre}$.*Diameter* to infinite, and $S_{HWN\text{-}pre}$ to $\emptyset$.
2: Color all nodes white. Set N_{proxy}.*House-Watch* to false, N_{proxy}.*Diameter* to 0, and S_{HWN} to $\{ N_{proxy} \}$.
3: For each node $N \in S_{HWN}$ such that *N.House-Watch* is false, set *N.House-Watch* to true, and do the following.
4: Color node N black, each white child u of N grey, and set *u.Diameter* to (*N.Diameter* + 1).
5: Each grey node invites its white child nodes to join, and sends N the set of its 1-hop white children.
6: N selects such grey nodes as temporary members of S_{HWN} that they have more children (denoted as N_{temp}), one by one until all children of all grey nodes have been covered. Then, the selected nodes are notified.
7: N_{temp} invites its white child nodes to join again, and each child node elects such N_{temp} as its parent that has more child nodes than any others. N_{temp}.*House-Watch* is set to false, and added to S_{HWN}.
8: Repeat steps 3 - 8 until all nodes have been colored black or grey.
9: If N_{proxy}.*Diameter* is less than $N_{proxy\text{-}pre}$.*Diameter*, then replace $N_{proxy\text{-}pre}$, $N_{proxy\text{-}pre}$.*Diameter* and $S_{HWN\text{-}pre}$ with N_{proxy}, N_{proxy}.*Diameter* and S_{HWN} respectively, and replace N_{proxy} with such a child node of it that is on the diameter path, and repeat steps 2 - 9.
10: Return $S_{HWN\text{-}pre}$ as a house-watching network, with diameter $N_{proxy\text{-}pre}$.*Diameter* and proxy $N_{proxy\text{-}pre}$.

Because the path <N_1, N_9, N_{14}> is the longest one, in the next step, in place of N_0, N_9 becomes a proxy of the administration center, and we have the resulting HWN shown in Fig. 7. Both HWNs shown in Figs. 6 and 7 have five nodes, but that shown in Fig. 7 is of a shorter diameter.

IV. Performance Evaluation

Simulation experiments have been done to study performance of the proposed algorithm. Network Simulator-2 were used. This section describes simulation environment, presents and discusses simulation results.

A. Experiment I: House-Watching Network Size and Diameter

In this experiment, the field configuration was set to 1000 m × 1000 m square. Five experiments were conducted with total 40, 50, 60, 70, and 100 nodes respectively. Nodes were randomly placed on the plane. Transmission range of each node was set to 250 m.

Experiment results are summarized in Table II. Topology corresponding to Experiment 1, 2, 3, 4, and 5 is given in Figs. 8, 9, 10, 11, and 12, respectively. Node 0 (the black node shown in Figs. 8 - 12) is taken as the administration center, and the grey nodes are the proxy nodes.

Comparing Figs. 8 - 10 with Figs. 11 - 12, it is known that if nodes are more evenly distributed, a smaller diameter can be achieved. This is because that, on the one hand, the algorithm can more effectively find the center of the network

TABLE II
Experiment Results for Experiment I

Experiment	Number of nodes	House-watching network size	Diameter
1	40	13 → 10	5 → 3
2	50	14 → 14	5 → 4
3	60	13 → 13	5 → 5
4	70	11 → 10	4 → 2
5	100	16 → 13	3 → 2

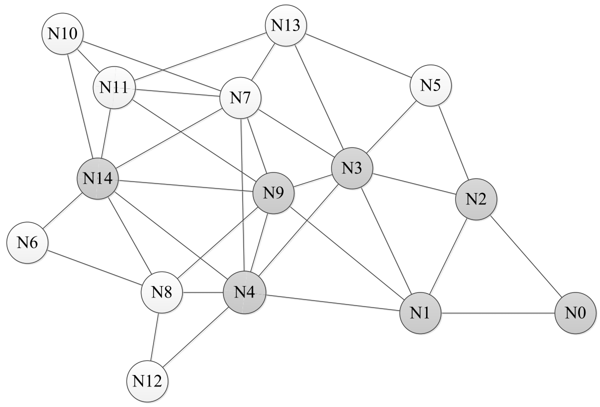

Fig. 5. Stage 1 of Func. 1. N_0 is the administrator center.

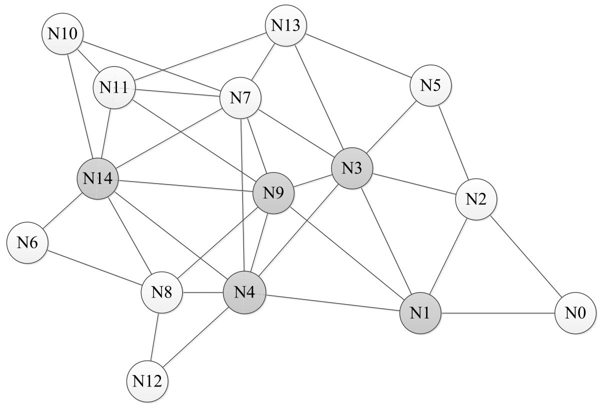

Fig. 6. Stage 2 of Func. 1. N_1 is a proxy of administration center.

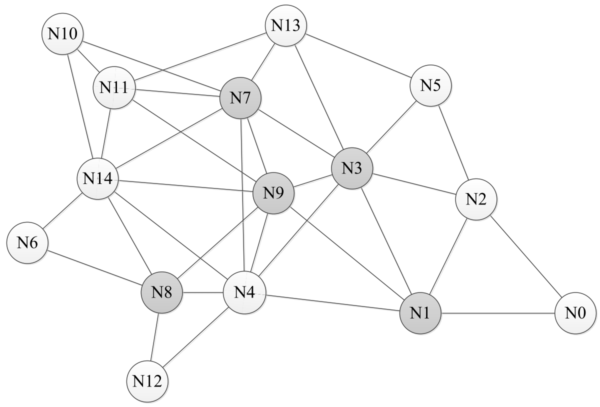

Fig. 7. Stage 3 of Func. 1. N_9 is a proxy of administration center.

area if it has a well defined one. On the other hand, as shown in Fig. 10, in some cases the diameter could not be reduced any way. For this, some other kind definition of the "center of a network area" than the "minimal diameter" may be more appropriate.

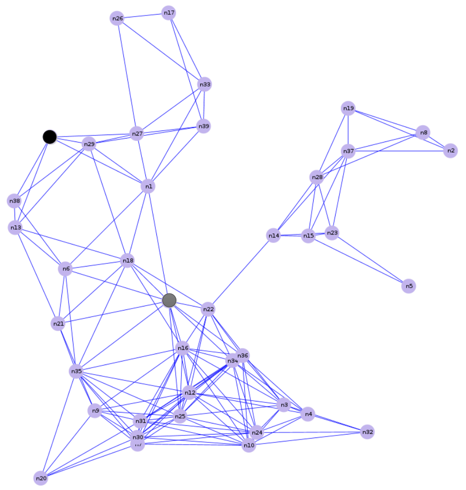

Fig. 8. Experiment 1: number of nodes is 40.

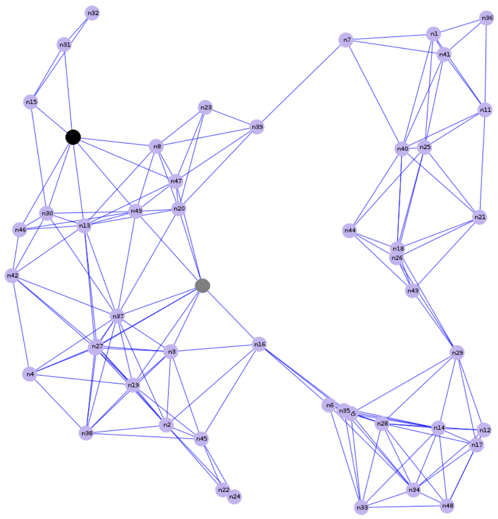

Fig. 9. Experiment 2: number of nodes is 50.

B. Experiment II: Session Size and Its Determination

This experiment examines how the size of communication session affects the waiting time for users to enter sleep state.

The field configuration was set to 500 m × 500 m square with total 50 nodes. Nodes were randomly placed on the plane. Transmission range of each node was set to 100 m. For traffic model, one node at one corner of the field was used to send files continuously to another node at the opposite corner.

As expected, experiment results show that larger session size increases average waiting time. For example, when we increased the session size from 50 packets to 200 packets, waiting time increased from about 1.1 to about 1.8 second.

Interestingly, it is also found that, in the case that more nodes are going to enter sleep state, larger session size tends to increase packet arrival ratio. For example when we increased the session size from 50 packets to 200 packets, in the case of 5 nodes going to enter sleep state, packet arrival ratios remained almost unchanged. In the case of 20 nodes going to enter sleep state, however, packet arrival ratio increased from about 71% for size 50 to about 80% for size 200.

The above experiment results suggest that we should de-

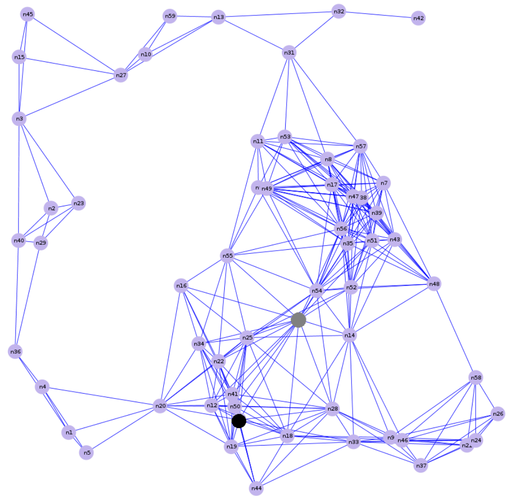

Fig. 10. Experiment 3: number of nodes is 60.

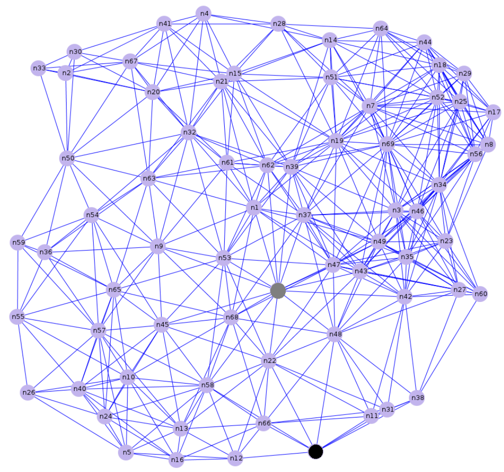

Fig. 11. Experiment 4: number of nodes is 70.

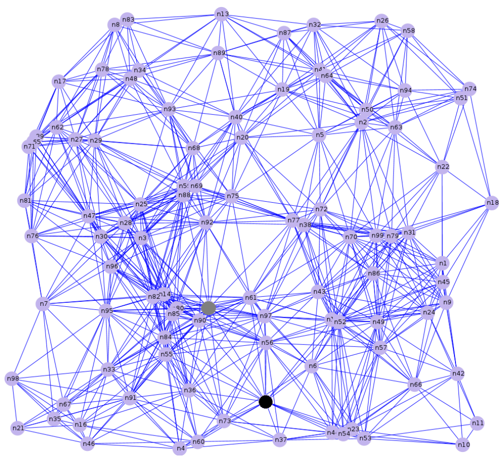

Fig. 12. Experiment 5: number of nodes is 100.

termine the session size according to two factors: the session size should not be so long that other users could not endure it; the session size should not be so short that the arrival ratio becomes negatively affecting users' communication.

V. Coping with Sleep Thrashing

This section addresses the subject of sleep thrashing problem. We introduce the concepts of trigger node and Fragile Route Dependency Relationship (FRDR) diagram. The sleep of a trigger node may cause other nodes in the corresponding FRDR diagram to sleep, and thus sleep thrashing may occur. So we introduce a performance metric called *work loss*, denoted by $\rho(\cdot)$. A trigger node u which $\rho(u)$ is greater than a specified threshold will be forced to join CDS, and thus will not be allowed to sleep. By this, sleep thrashing can be solved to a great extent.

Definition 7 (Proxy Route). *Let* P = $<N_s \cdots N_c \cdots N_d>$ *be a route between* N_s *and* N_d. Q = $<N_a \cdots N_b>$ *is called a proxy route of* N_c *if there is route* $<N_s \cdots Q \cdots N_d>$ *that connects* N_s *and* N_d *in place of* P.

Definition 8 (Direct Critical Node, Fragile Communication, and Fragile Route). *Denote the communication between* N_s *and* N_d *as* $C_{s,d}$. *If every route for* $C_{s,d}$ *shares a common intermediate node* N_c, T_{N_c} < *min*(T_{N_s}, T_{N_d}), *and there do not exist proxy routes for* N_c, *then* $C_{s,d}$, N_c, *and the route for* $C_{s,d}$ *are called the direct fragile communication, critical node with respect to* $C_{s,d}$, *and fragile route, respectively. We also say that* $C_{s,d}$ *is dependent on* N_c.

The definition of critical node is similar to that of cut vertex in graph theory, but they are different. Firstly, a cut vertex is not necessarily a critical node. For example, a cut vertex that is independent of others, and thus its sleep does not affect others, cannot be a critical node. Secondly, a non-cut vertex may be a critical node. For example, a node at the congested area may be detected as a critical node.

Let $C_{s,d}$ be a communication between N_s and N_d. The set $\{N_s, N_d\}$, denoted by CEN($C_{s,d}$), is called a compound end node of $C_{s,d}$.

Definition 9 (Conditional Critical Node, Fragile Communication, and Fragile Route). *Consider communication* $C_{s,d}$. *Let* $C_{x,y}$ *be any a communication, and* Z = $\{ C_{i,j} \}$ *with* $C_{s,d} \notin Z$ *be any a group of communications in progress.*

If every route for $C_{s,d}$ *shares a common intermediate node* N_c *that will become critical when users in* Z *enter sleep state, then we call* $C_{s,d}$ *and* N_c *the conditional fragile communication and critical node with respect to* $C_{s,d}$, *respectively.*

If every route for $C_{s,d}$ *takes either* N_x *or* N_y *as an intermediate node, and CEN(*$C_{x,y}$*) will become critical when users in* Z *enter sleep state, then we call* $C_{s,d}$ *and CEN(*$C_{x,y}$*) the conditional fragile communication and critical node with respect to* $C_{s,d}$, *respectively.*

We also say that $C_{s,d}$ *is dependent on* $C_{x,y}$ *and critical nodes, and call a route for* $C_{s,d}$ *a conditional fragile route.*

Definition 10 (Trigger Node). *Let* P = $<N_s \cdots N_c \cdots N_d>$ *be a route between* N_s *and* N_d, *and* N_c *be a critical node with respect to* P. *Then* N_c *is called a trigger node of* P, *meaning that if* N_c *enters sleep state,* P *will become broken.*

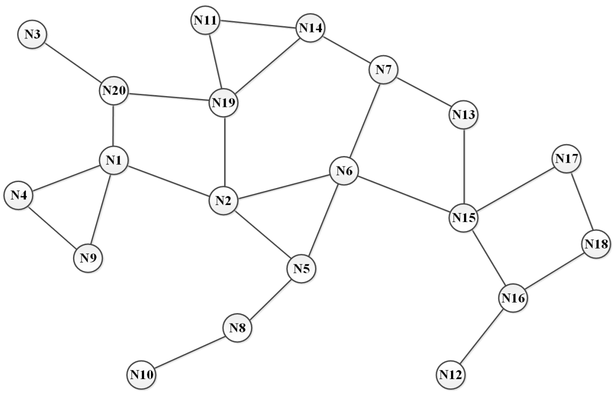

Fig. 13. An example for illustrating critical node and critical path.

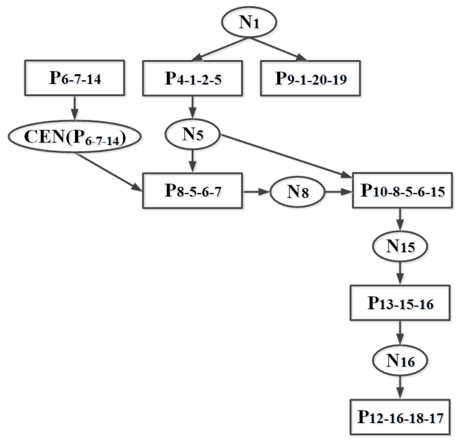

Fig. 14. An example for illustrating FRDR diagram.

Definition 11 (FRDR Diagram). *A FRDR diagram is a directed graph that is composed of trigger nodes, critical nodes, fragile routes, and the relationships between fragile routes through critical nodes. Given two communications* $C_{s,d}$ *and* $C_{x,y}$, *if* $C_{s,d}$ *is dependent on* $C_{x,y}$ *through critical node* N_c, *then the diagram represents this as a triple tuple* $<C_{s,d}, N_c, C_{x,y}>$

We use Fig. 13 to explain the above definitions. Assume that N_1 is talking with N_6. As soon as the talking is finished, they get to enter sleep state. Assume that at the same time, N_8, N_9, N_{12}, N_{13}, N_{14}, and N_{20} are connected to N_7, N_{19}, N_{17}, N_{16}, N_{15}, and N_7, respectively. Then caused by the sleep of N_1, the communication between N_9 and N_{19} becomes impossible, and they get to enter sleep state. In turn, caused by the sleep of N_{19}, the communication between N_{20} and N_7 becomes impossible, and they get to enter sleep state. This snowball effect will continue, and finally no one can be reachable, and the network becomes collapsed.

The scenario stated above can be explained using the FRDR diagram shown in Fig. 14. From this figure we known that N_1, N_5, N_8, N_{15} and N_{16} are all critical nodes, and for example, N_5 is a trigger node with respect to path $<N_8, N_5\ N_6\ N_7>$.

On the basis of the above definitions we define the performance metric *work loss* $\rho(u)$ for node u as

$$\rho(u) = \frac{\alpha\frac{|FRDR|}{|V|} + (1-\alpha)\frac{\sum_{i=1}^{|FRDR|}(T_{N_i} - T_u)}{\sum_{i=1}^{|FRDR|} T_{N_i}}}{2} \quad (1)$$

Take the FRDR diagram shown in Fig. 14 as an example, and let u be N_8. Then $|V|$ is equal to 20, the node number of the network shown in Fig. 13. $|FRDR|$ is equal to 6, the member number of the set $\{N_{10}, N_{15}, N_{13}, N_{16}, N_{12}, N_{17}\}$. α $(0 \le \alpha \le 1)$ is a user-defined parameter used to trade off the weight of node number and communication time.

From Fig. 14 we know that, if we include the nodes N_1, N_5, N_8, N_{15}, N_{16} in a CDS, and give CDS nodes the responsibility of forming a virtual backbone, then sleep thrashing would not occur and an ad hoc network would last long. On the basis of this basic idea, algorithm given in Func. 1 is modified so that a trigger node u which $\rho(u)$ is greater than a specified threshold will be forced to join CDS.

Simulation experiments have been conducted to study the sizes of CDS constructed with the modified algorithm. Since the communication time affects the CDS size, and it is difficult to know its distribution, we assume all users have the same communication time. This will result in the least possible CDS sizes, i.e. the lower bound of CDS sizes. Experiment results are given in Table III.

TABLE III
THE LEAST POSSIBLE SIZE OF CDS

Node number in MANET	30	60	90	120	150
Lower bound of CDS sizes	6.5	15.6	25.6	34.3	41.7

VI. CONCLUSIONS

We have addressed the subject of communication problems at the disaster-hit area. Because the existing ad hoc network techniques have not taken into consideration the issue of sleep, which is a very frequently used means for mobile users to save their battery consumption, at the disaster-hit area, communication supporting systems using the existing ad hoc network techniques could not function as expected, and user communication would be interrupted from time to time. We have presented a system model with an effective algorithm to solve the problem.

We have observed an interesting phenomenon called sleep thrashing for an ad hoc network in the disaster-hit area, for which a few users' sleeps collapse the whole communication system. We have investigated the sleep thrashing problem in detail, and given a solution to reduce its negative effect.

Simulation experiments have been conducted to study performance of the proposed approaches. Experiment results have shown that using the proposed approaches, only a few mobile terminals need to be powered on and all the others can go to sleep mode safely, and when a mobile user wants to sleep, she can have the chance to decide at what time the sleeping button should be pushed down so that other users would not be affected by her sleeping.

REFERENCES

[1] B. Das and V. Bharghavan, "Routing in ad-hoc networks using minimum connected dominating sets," in *Proc. IEEE International Conference on Communications (ICC'97)*, Montreal, Canada, 1997, pp. 376–380.

[2] B. Das, R. Sivakumar, and V. Bharghavan, "Routing in ad hoc networks using a virtual backbone," in *Proc. IEEE International Conference on Computer Communications and Networks (IC3N'97)*, Las Vegas, 1997, pp. 1–20.

[3] B. Das, R. Sivakumar, and Vaduvur, "Routing in ad hoc networks using a spine," in *Proc. IEEE International Conference on Computers and Communications Networks (IC3N'97)*, Las Vegas, NV., 1997, p. 34.

[4] C. Yu-Liang and H. Ching-Chi, "Routing in wireless/mobile ad-hoc networks via dynamic group construction," *Mobile Networks and Applications*, vol. 5, no. 1, pp. 27–37, 2000.

[5] J. Wu and H. Li, "On calculating connected dominating set for efficient routing in ad hoc wireless networks," in *Proc. International workshop on Discrete algorithms and methods for mobile computing and communications (DIALM'99)*, Seattle, Washington, USA, 1999, pp. 7–14.

[6] R. Sivakumar, P. Sinha, and V. Bharghavan, "Cedar: a core-extraction distributed ad hoc routing algorithm," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1454–1465, 1999.

[7] Y. Li, D. Kim, F. Zou, and D.-Z. Du, "Constructing connected dominating sets with bounded diameters in wireless networks," in *Proc. International Conference on Wireless Algorithms, Systems and Applications, 2007. (WASA'2007)*, Chicago, IL, 2007, pp. 89–94.

[8] D. Kim, Y. Wu, Y. Li, F. Zou, and D.-Z. Du, "Constructing minimum connected dominating sets with bounded diameters in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 2, pp. 147–157, 2009.

[9] S. M. Aurélio and J. J. Garcia-Luna-Aceves, "Bounded-distance multiclusterhead formation in wireless ad hoc networks," *Ad Hoc Networks*, vol. 5, no. 4, pp. 504–530, 2007.

[10] V. S. Anitha and M. P. Sebastian, "Scenario-based diameter-bounded algorithm for cluster creation and management in mobile ad hoc networks," in *Proc. IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications (DS-RT'09)*, Singapore, 2009, pp. 97–104.

[11] F. Dai and J. Wu, "An extended localized algorithm for connected dominating set formation in ad hoc wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 10, pp. 908–920, 2004.

[12] J. Bolla and D. Huynh, "Adapting connected d-hop dominating sets to topology changes in wireless ad hoc networks," in *Proc. IEEE International Performance Computing and Communications Conference (PCC'06)*, Phoenix, AZ, USA, 2006, pp. 207–214.

[13] K. Sakai, M. T. Sun, and W. S. Ku, "Message-efficient cds construction in manets," in *Proc. IEEE International Symposium on Wireless Pervasive Computing (ISWPC'10)*, Modena, Italy, May 2010.

[14] H. Y. Yang, C. H. Lin, and M. J. Tsai, "Distributed algorithm for efficient construction and maintenance of connected k-hop dominating sets in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 444–457, 2008.

[15] J. Wu, F. Dai, and S. Yang, "Iterative local solutions for connected dominating set in ad hoc wireless networks," *IEEE Transactions on Computers*, vol. 57, no. 5, pp. 702–715, 2008.

[16] M. Couture, M. Barbeau, P. Bose, and E. Kranakis, "Incremental construction of k-dominating sets in wireless sensor networks," *Ad Hoc Sensor Wireless Networks*, vol. 5, no. 1-2, pp. 47–68, 2008.

[17] N. Meghanathan and G. W. Skelton, "Risk notification message dissemination protocol for energy efficient broadcast in vehicular ad hoc networks," *IAENG International Journal of Computer Science*, vol. 37, no. 1, pp. 1–10, 2010.

[18] J. Wang, T. Mikami, K. Kanamori, E. Kodama, and T. Takada, "Improving packet delivery fraction of ad hoc network with xors-based network coding cds," *IAENG International Journal of Computer Science*, vol. 38, no. 3, pp. 275–282, 2011.