Available online at www.sciencedirect.com

SCIENCE DIRECT®

Ad Hoc Networks 3 (2005) 607–620

www.elsevier.com/locate/adhoc

An ad hoc networking scheme in hybrid networks for emergency communications

Takahiro Fujiwara [a,*], Takashi Watanabe [b]

[a] *Information Technology Lab., Enegene Co., Ltd., 619-4 Irino-cho, Hamamatsu, Shizuoka 432-8061, Japan*
[b] *Faculty of Information, Shizuoka University, 3-5-1 Johoku, Hamamatsu, Shizuoka 432-8011, Japan*

Abstract

This paper describes an ad hoc networking scheme and routing protocol for emergency communications. The objective of the network is to collect damage assessment information quickly and stably in a disaster. The network is configured with a hybrid wireless network, combining ad hoc networks and a cellular network to maintain connectivity between a base station (BS) and nodes even in a disaster. In the event that a direct link between the BS and a node is disconnected due to damage or obstacles, the node switches to the ad hoc mode, and accesses the BS via neighboring nodes by multihopping. The routing protocol proposed in this paper discovers and builds a route by way of monitoring neighbors' communications instead of broadcasting a route request packet. The network employs a dedicated medium access control protocol based on TDM (Time Division Multiplexing) for multihopping in ad hoc networks to maintain accessibility and to perform a short delay. Experiments showed that approximately 90% of nodes are capable of reaching the BS within a few hops, even in conditions where only 20% of nodes maintain direct connections to the BS. In addition, the results showed that it is feasible for the network to operate in a short delay for delivering a packet to the BS. However, throughput is not retrieved sufficiently due to the restriction of the access protocol, whereas reachability does improve sufficiently. Therefore, the network is suitable for collecting damage assessment information and transmitting urgent traffic quickly and stably, while the data is restricted to a small amount.

Keywords: Ad hoc networks; Hybrid network; Routing protocol; Multihop access; Damage assessment; Disaster communications

---

1. Introduction

Quick, accurate damage assessment information is necessary for speedy and effective rescue response in the aftermath of a large natural and man-made disaster. Current communication

---

[*] Corresponding author. Tel.: +81 53 445 0097; fax: +81 53 445 0092.

E-mail addresses: tk-fujiwara@computer.org (T. Fujiwara), watanabe@cs.inf.shizuoka.ac.jp (T. Watanabe).

1570-8705/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2004.08.007

infrastructures are sufficient for these needs, as long as telephone or mobile phone service is uninterrupted. However, when these infrastructures break down, this pipeline for essential information is cut. In the Kobe earthquake of 1995, for example, heavy phone use by the general population caused sudden and severe congestion in the phone system [1], preventing quick and efficient gathering of damage assessment information by government authorities. As a result, response efforts were delayed, causing further damage that could have been prevented with better communications. To make matters worse, the communications breakdown was not limited to the immediate aftermath of the earthquake, instead lasting three days during which rescue and recovery were severely hampered.

We have noticed from past instances that communication systems have been obviously vulnerable due to massive communication congestion beyond estimation in the aftermath of a large-scale disaster, and those obstacles to communications increased the damage. In the wake of such bitter experiences, several institutes have conducted research to develop a system for disaster communications. A system to collect and distribute safety information for people via the Internet in a disaster has been developed and presented in [6]. Regarding a monitoring system for damage on lifeline facilities, Refs. [7,8] have demonstrated a system for collecting damage assessment information, respectively. We review them in the following section.

Meanwhile, the progress of current mobile communication systems is leading to environments capable of accessing networks anytime anywhere [2]. Even with explosively increasing subscribers, mobile systems have responded to requirements by developing new technologies such as CDMA (Code Division Multiple Access), adaptive modulation, directional beam forming, and so on. The third-generation (3G) wireless mobile system covers up to 2 Mbps in indoor environments and 144 kbps in vehicular environments. The fourth-generation (4G) cellular system will challenge the data rate of 10–20 Mbps, and will reach speeds of up to at least 2 Mbps for moving vehicles [2,3]. Besides, it will provide multimedia services using higher data transmission capacity [4]. These future communication systems will be capable of maintaining communications sufficiently not only in ordinary environments but also in disaster situations, and we expect that advanced communication technology will enable a much swifter response to satisfy the requirements of speedy and effective rescue activities.

However, we should remember the primary objective of the current networks has been best-effort performances rather than secure accessibility. In the case of the attack on September 11 in New York, the most up-to-date communication systems for telephone and mobile phone services were hampered by the heavy communication congestion after the disaster. Furthermore, even on the Internet, people could not access the network due to the heavy load. These kinds of occurrences remind us that communication obstacles during a disaster have yet to be overcome.

Even if the channel capacity increases using broadband communication technologies, it may not solve heavy traffic congestion sufficiently in disaster circumstances. The same issues may lurk even in 3G and 4G systems since the network environment is more complicated and the communication load is increased significantly more, and the magnitude of disaster would be far beyond estimation. The present countermeasure for congestion is only to restrict connection from subscribers for accessing the network. Therefore, it is necessary to cope with maintaining connectivity and accessibility of the network for urgent traffic in disaster circumstances.

To overcome these kinds of issues for disaster communications, this paper discusses network architecture, focusing on maintaining the connection between nodes and a base station. We propose a hybrid wireless network, combining a cellular network and ad hoc networks. The rest of the paper is organized as follows: In Section 2, we discuss related work for disaster communications and current network schemes. Sections 3 and 4 propose a network model and a routing protocol including a medium access control protocol for emergency communications. Section 5 shows the experimental results of performances. Section 6 concludes this work.

2. Related work

2.1. Current disaster communications

One of the critical factors in disaster communications is to collect damage assessment information quickly and accurately for rescuing victims and mitigating damage. The operation for the data collection is conducted by the top-down approach or the bottom-up approach.

In governmental operations for damage assessment and emergency response strategies, the top-down approach is carried out to collect information. Ref. [10] describes an integrated disaster management communication system, and claims that several organizations should react not only efficiently and individually but also in a coordinated manner in disaster situations. A system using a similar objective for disaster management has been developed and introduced by the Disaster Management Bureau of Japan's Cabinet Office [5]. The Central Disaster Management Radio Communication Network connects several public agencies such as the fire-fighting agency, the meteorological agency, the police agency, the self-defense force, and local governments for collecting damage assessment information. The system aims to make an assessment of the magnitude of damage quickly under limited information immediately after an earthquake and to implement strategies for rescue operations.

On the other hand, rescue operations, which need individual damage information, require the bottom-up approach. Especially, relief activities to rescue survivors trapped beneath rubble require quick, accurate, and localized information. Several systems have been proposed to collect actual damage assessment information. Ref. [6] demonstrated a system to gather safety information for people in emergencies via the Internet referred to as IAA (I Am Alive). The IAA system was designed to satisfy the following functions: (1) Scalability and flexibility to expand and change in proportion to the scale of the geographical area of a disaster. (2) Robustness and fault tolerance to provide communication service without interruption even if some parts of the system have crashed. (3) Privacy and security to protect personal information against queries that would violate privacy. The IAA system is premised on the Internet operating normally and sufficiently. In reality, the Internet is useful for collecting and delivering information, and the network may be robust due to redundancy. However, it has a potential but obvious obstacle for accessing the network due to communication congestion. Thus, it is difficult to collect and deliver information quickly and stably using IAA via the Internet in the aftermath of a large-scale disaster.

Meanwhile, some dedicated wireless data collection systems have been studied to acquire damage assessment information from lifeline facilities, such as water supplies, gas supplies and electric power supplies. A monitoring and controlling system for gas pipelines was developed, as presented in [7]. The system equipped and deployed a large number of SI (Spectrum Intensity) sensors at 3600 sites to detect seismic motion, and it introduced prioritized telephone lines to maintain accessibility to terminals in a disaster. The system also controls shut-off valves according to instructions received via the communication lines from the operation center. However, operating a system involving 3600 sensor sites and operating a system which can monitor the status of the hundreds of thousands or even millions of residences using gas in a major city are two entirely different matters. Setting up a system of dedicated telephone lines to monitor the situation in a whole city would be extremely impractical, if not impossible.

A monitoring system for lifelines installed in residences was studied to collect urgent data. The experimental system was developed with a centralized hierarchical wireless network, introducing a CDMA technique and a polling access protocol to achieve a low bit error rate and to collect data efficiently [8]. The experimental results showed that it is feasible to collect data from 256,000 terminals deployed in an entire city within one minute for emergency signals without communication congestion. However, since each link between a base station and terminals is connected with a single path, it is easily supposed that some links suffer damage, and cannot maintain connections in disaster circumstances. The experiments showed that the system needed to improve connectivity to operate in deteriorated channel conditions in a disaster [9].

In the case of damage of a base station (BS) and/or a central control station (CS), Ref. [23] has presented a network architecture to access a node from a neighboring BS. Actually, the impact of damage on a BS or CS is critical. However, it is possible to implement a quakeproof design for their facilities thus preventing damage. On the contrary, terminals placed in residences or links connecting terminals to a BS are vulnerable, and it is impractical to implement such a measure in all buildings. This paper addresses network architecture to maintain connections between the BS and nodes in a cell for disaster communications.

2.2. Network models for disaster communications

Current cellular systems are capable of providing efficient and stable communications as long as the network maintains connectivity and copes with communication congestion even in disaster situations. On the other hand, since ad hoc networks may operate effectively for disaster relief operations even if infrastructure facilities do not work satisfactorily, the networking technologies are advantageous for use in disaster communications. Various routing protocols for ad hoc networks have been proposed as shown in [11,12].

In the case of on-demand routing protocols of ad hoc networks, e.g., AODV or DSR, a route request (RREQ) packet is broadcasted from a source node due to route discovery. One concern, in disaster circumstances, is that RREQ packets generated from massive nodes cause heavy traffic congestion and communication failure. Likewise, in the case of table-driven routing protocols, the networks lapse into heavy traffic conditions since a change of network environments happens suddenly and simultaneously. In addition, a significant number of papers have addressed energy issues of ad hoc networks [13,14]. The issue is especially nontrivial in terms of the environment, such as disaster circumstances, in which devices cannot be recharged easily. However, the network should not stop the transmitting of emergency signals just for the sake of saving battery power. The protocol needs to be modified in order to reduce extra transmissions such as a packet-flooding method.

Considering the advantages of a cellular network and ad hoc networks, various types of hybrid wireless networks using multihopping have been studied for the next generation mobile system to achieve high data rate, high capacity, and wide area coverage, including QoS (quality of services) control.

A multihop radio access cellular system, MRAC, was proposed in [15]. The system aims to achieve high speed, high capacity and wide area coverage using two kinds of hop-stations; one is a dedicated repeater station set up in a good propagation condition area, and the other is a user node. In the event that a mobile station detects high propagation loss on the "single-hop" path, the station selects an available hop-station to relay data. However, MRAC allows only single or double hops via the hop-station. The allocation of hop-stations requires difficult strategic decisions when operating in disaster situations.

A hybrid network, called Sphinx, is considered to be fair in terms of resource allocation and resilience in addition to high throughput and low power consumption in [16]. Mobile stations operate in two modes, a cellular mode and a peer-to-peer mode. When the mobile station detects throughput degradation in the peer-to-peer mode, it switches to the cellular mode. However, the network may not work satisfactorily in disaster situations, since the peer-to-peer mode suffers from interference in heavy traffic, and the cellular mode does not operate sufficiently due to communication congestion.

An integrated cellular and ad hoc relaying system, called iCAR, was pointed out in [17] in which the system lapses into blocking and dropping communications due to localized congestion. The system introduces ad hoc relay stations, which are placed at strategic locations, to divert traffic in one (possibly congested) cell to another (non-congested) cell. It may be possible for nodes in a congested cell to access surrounding non-congested cells, resulting in traffic load balancing. However, since the number of hops increases to relay a packet via neighboring non-congested cells, a potential issue of communication failure is a serious concern. Furthermore, most cells lapse into a state of congestion in a disaster.

3. Hybrid network

3.1. Network model and operation

Regarding network architecture for disaster communications, the primary role is to collect damage assessment information and various emergency signals quickly and stably. The network has to maintain connections between nodes and a base station (BS) in order to satisfy the requirements. Assuming that the contents of the traffic mainly consist of sensing data, emergency signals, and/or lifeline information indicating the state of damage, the size of data from each node is several tens of bytes, not including a large amount of data such as an image of several kilobytes. In addition, since nodes are fixed at a specified location, change of the network topology is moderate in normal conditions. However, in the event that a disaster or emergency happens, the network condition may change rapidly and extensively.

We propose a hybrid network composed of a BS and several nodes for a data collection system in a cell, exploiting advantages of ad hoc networks and a centralized network. The hybrid network, referred to as ECCA (Enhanced Communication Scheme Combining Centralized and Ad-hoc Networks), is configured with ad-hoc networks (AD-Net) and a centralized network (CH-Net), as shown in Fig. 1. Provided that a node is able to receive a signal from the BS and to establish the connection, the node operates in a cellular mode of CH-Net, as shown in Fig. 2(a). On the other hand, in the event that a node cannot maintain a connection with the BS, the node switches to an ad hoc mode. It searches neighboring nodes, which have a route to the destination, the BS, and then requires one of their nodes to forward its packet, as shown in Fig. 2(b). As a result, the node dynamically establishes a route to the BS. We refer to a node operating in the cellular mode as a direct connection node (DCN), and a node operating in the ad hoc mode as an indirect connection node (ICN). The DCN can relay a packet, which is transmitted from/to a neighboring node of ICN, and ECCA connects nodes of CH-Net and AD-Net seamlessly.

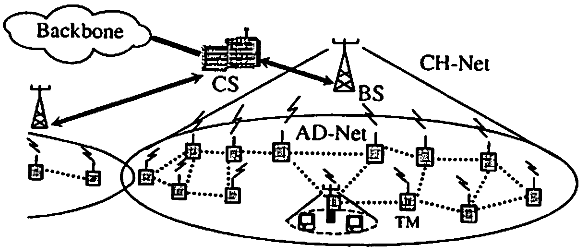
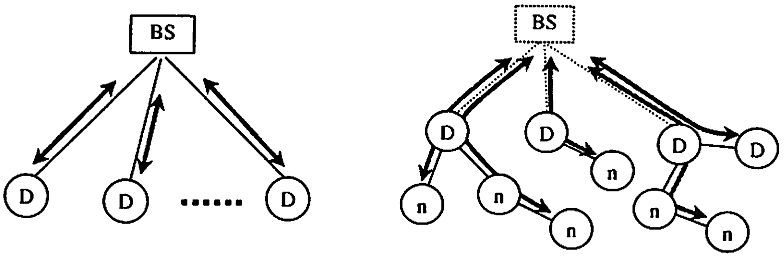


Fig. 1. ECCA network model. CS: central control station, BS: base station, TM: terminal.

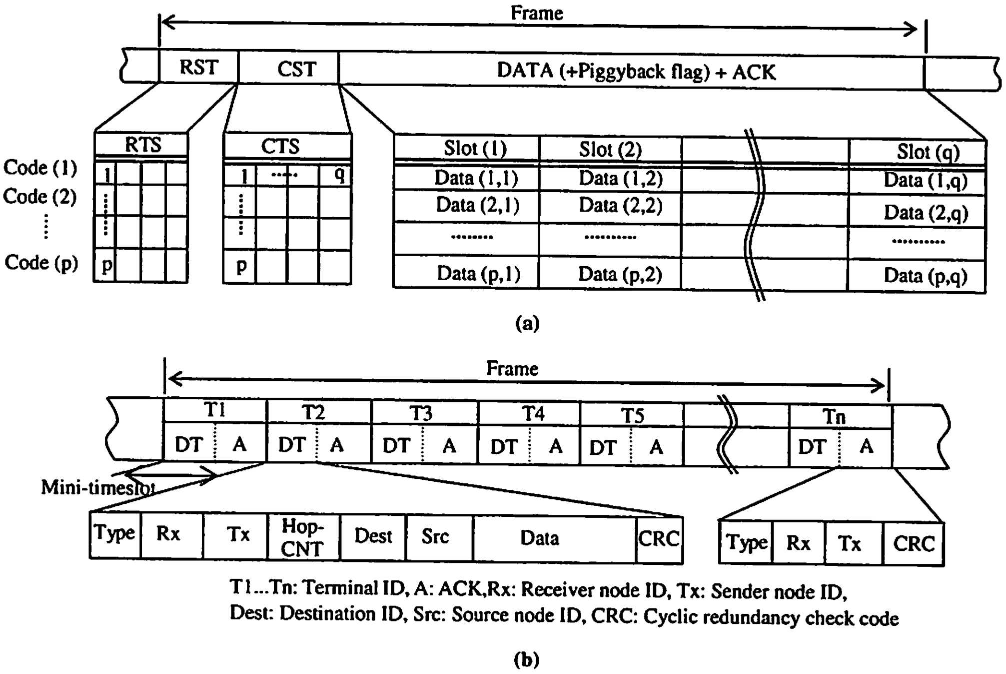
3.2. Channel structure

ECCA equips two types of channels, one is a data channel to transmit large user-data directly between a BS and nodes, and the other is a control



(a) (b)

Fig. 2. Operation modes. BS: base station, D: direct connection node, n: nodes which cannot access BS directly. (a) Cellular mode, (b) ad hoc mode.



(a)

T1...Tn: Terminal ID, A: ACK,Rx: Receiver node ID, Tx: Sender node ID,
Dest: Destination ID, Src: Source node ID, CRC: Cyclic redundancy check code

(b)

Fig. 3. Frame structure. (a) Data channel, (b) common communication channel (CCCH).

channel to send control data from the BS to nodes and status or reply data from nodes to the BS. The control channel especially plays a major role in transmitting urgent data by multihopping, as described later.

Fig. 3 illustrates the frame structure of the data channel and the control channel. The data channel is configured with CDMA (Code Division Multiple Access) sub-channels multiplexed with different spreading codes. By dividing the CDMA sub-channels into multiple timeslots, the radio system can increase the number of multiplexed channels, maintaining the orthogonality. This technique is referred to as TD-CDMA (Time Division and Code Division Multiple Access) [9]. In the figure, the number of multiplexed CDMA sub-channels is p, and the number of timeslots is q, resulting in the number of sub-channels of $p \cdot q$.

A frame of the data channel consists of RTS (request to send), CTS (clear to send) and DATA fields with the time division multiplexing (TDM) manner, as shown in Fig. 3(a). These fields are composed of sub-channels multiplexed with CDMA codes, and each field is divided into timeslots, based on TD-CDMA. Especially, the RTS and the CTS are designed in a short timeslot for sending a small request and reply packet.

When a node transmits a packet in the data channel, it, at first, sends a request packet in any one of the timeslots in the RTS field to reserve a channel of the DATA field. In conditions where the request packet reaches the BS successfully, the BS allocates one of the data channels to the node, and notifies the allocation in the CTS field with the same CDMA code whose node transmitted the request packet. When succeeding in making a reservation of the data channel, the node transmits its data packet in the designated channel, and the BS replies with the acknowledgement (ACK) sequentially in the timeslot. In addition, provided that the node has more packets in its buffer, the node sets the piggyback flag of the data packet header when transmitting data. The node is allowed continuously to use the channel for the following data. The allocation status is informed in the CTS field.

Meanwhile, a frame of the control channel is divided into short mini-timeslots, and every node in a cell is assigned to one of the mini-timeslots. Hence, the channel operates in the TDM, and every node shares the channel. Hereafter, we refer to the channel as the Common Communication Channel (CCCH). Fig. 3(b) shows its frame structure which consists of a packet header, data and a CRC (Cyclic Redundancy Check) code. The packet header includes a type of packet, addresses of a source, destination, sender and receiver, and a hop-count (HCNT), which is used for the route discovery process, as described in the following section. When receiving the packet addressed by unicasting, the node replies with the ACK in the same mini-timeslot.

For the CCCH operation, every node has to synchronize a frame with other nodes. The GPS clock is one of the solutions. However, the system requires a more flexible way to operate in disaster circumstances. For the system to be designed with the time-division technique is critical as is the case with other communication mechanisms using time synchronization, and several institutes have attempted to resolve the issue [18–21]. We assume that nodes connecting with a BS directly can synchronize with the BS's clock, and other nodes detecting surrounding communications synchronize in the autonomous frame synchronization manner in ad hoc networks as shown in [19,20].

4. Routing protocol

In this section, we propose a routing protocol using unicast-communication instead of broadcasting a route request. In either a cellular or an ad hoc mode, nodes establishing a route to the BS periodically transmit a packet in CCCH to inform the BS of the status of nodes. We premise this scheme for the protocol.

4.1. Route discovery

In the event that a node cannot access the BS in the cellular mode, the node switches into the ad hoc mode, and then initiates a route discovery process. The routing protocol employs a metrics, hop-count (HCNT) indicating the number of hops to reach the destination. The node monitors communications of neighboring nodes in CCCH instead of broadcasting a route request packet. When overhearing a packet, the node checks the HCNT of the packet, and then records the value and the sender node address as its next-hop node, provided that the value of the HCNT is smaller than or equal to the fixed limit of the system parameter. When the node transmits a packet, it sends the packet to the recorded next-hop node in unicasting by increasing the value of the HCNT by one. The required intermediate node relays the packet according to the route information which the node has already found. The packet is finally delivered to the BS.

Each node is equipped with an entry table and a route table to record its route information. The entry table contains the HCNT of a neighboring node, and the address of the node. The table is referred to for forwarding a packet toward the destination. In conditions where the HCNT contained in the packet is smaller than the value stored in its entry table, the node updates the information of the entry table. Thereby, the node comprehends the address of the smallest hop-count node. If there are multiple nodes accessible at the smallest hop-count, it can select one of them randomly. Since the proposed routing protocol chooses the shortest path, the number of accessible nodes is a trivial matter for the most part, though it may influence the redundancy of alternative paths. On the other hand, the route table contains route information, addresses of a source node and a sender node to send back from the destination to the source node. The information of the table is set up when a packet is forwarded to the destination, the BS.

Fig. 4 illustrates the scenario of the route discovery process. A node named *node-s*, which cannot access the BS, monitors communications of neighboring nodes. When *node-s* overhears a packet which is transmitted from *node-i* to *node-f*, the node checks the HCNT (=k) and knows how many hops are required to reach the BS from *node-i*. *Node-s* records the address and the HCNT of *node-i* in its entry table. *Node-s* also records a route via *node-j* as shown in Fig. 4. Provided that

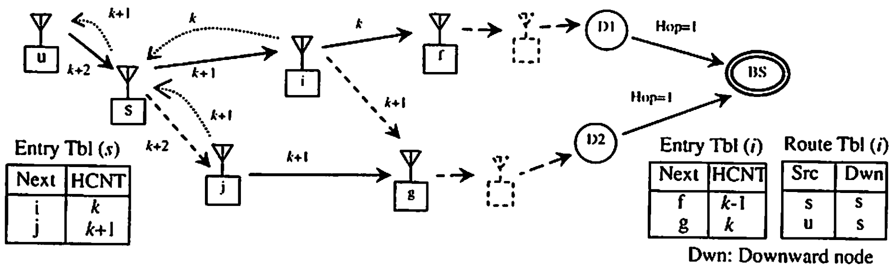


Fig. 4. Route discovery in ECCA.

node-s selects a node (*node-i*) as the next hop node according to the stored HCNT, it transmits a packet to *node-i* by unicasting, setting the HCNT at $k+1$. Receiving the packet from *node-s*, *node-i* forwards the packet according to the route, which it previously knows, to reach the BS. The packet finally reaches the BS via multihopping. Thus, nodes discover a route by monitoring neighbors' communications, and transmit a packet via the neighboring nodes by unicasting. Hence, the method is a unicast-based routing protocol.

4.2. Upward and downward route management

Since the network of ECCA transmits a packet between a BS and nodes, we refer to a route toward the BS as "Upward", and a route from the BS to a node as "Downward." As described above, an upward packet is transmitted to the BS according to the entry table of each node. On the other hand, a downward packet is sent back according to the route table.

In Fig. 4, an intermediate node, *node-i*, records a route to *node-f*, and it transmits a packet to *node-f* with the HCNT set up at *k*. When required to relay a packet by *node-s*, *node-i* forwards the packet to the next hop node, *node-f*, according to the entry table. Concurrently, *node-i* records in its route table the address of *node-s* as the send-back node for the downward packets. Likewise, *node-f* records the entry table and the route table. When a downward packet addressed to *node-s* arrives at *node-f*, the node finds the downward path, and relays the packet to *node-i* according to its route table. Finally, the packet is delivered to *node-s* according to the route table of each node.

4.3. Route error and route maintenance

In the event that an intermediate node detects failure in forwarding a packet, it does not carry out retransmission in ECCA, even though the node can retransmit a packet via another route. If some intermediate nodes execute retransmission to other routes, it may take a long time for a source node to detect the failure, despite requiring a short delay to deliver packets to the BS. In addition, the failure-prone packet transmitted in an unsteady route may rove during retransmission, and may hamper other packet transmission of the surrounding nodes.

Alternatively, ECCA introduces a mechanism to handle communication failure in order for an intermediate node to reply with a *route error message* or an *expiration message* to the downward node if it detects the failure. Provided that a node has another upward route to relay the message, the node replies with a *route error message*. On the contrary, in case the node has no route to forward the message, it replies with an *expiration message*. When the intermediate node receives a *route error message*, it relays the message to the downward node without replacement. When the intermediate node receives an *expiration message*, and provided that the node has an alternative path in the entry table, that is, it can switch the path to forward a packet, it sends back to its downward node the *route error message* instead of the *expiration*. Therefore, when the source node receives the *route error message*, it can retransmit the packet to the same next hop node, because the intermediate nodes have an alternative path. When the source node receives the *expiration message*, it must send the packet to another next hop node to transmit via another route.

Since each node transmits a packet periodically in ECCA, nodes update the freshness of the routes by monitoring surrounding communications, resulting in maintaining the connectivity to neighboring nodes. If a node notices that it has not detected a packet from the neighboring node during the time to live (TTL), the node deletes the entry to the neighboring node in its entry table. If the node has no entry in the table, it has to defers sending a packet. Thus, since the nodes do not transmit a route request packet by broadcasting, interference by the transmissions is not induced. In addition, they do not consume power caused by the unprofitable transmission of broadcasting.

4.4. Multihop access scheduling

Since a packet is transmitted in the TDM fashion as described in the previous section, it is necessary to avoid the packet excessively staying in the queue of a relay node for multihopping. We employ an access scheduling manner for multihopping in ECCA; a source node transmits a packet in a designated timeslot, while an intermediate node relays the packet in the timeslot of the source node, not in its own timeslot. Thereby, the multihopping manner allows a node to relay multiple packets within a frame interval, even if a large number of packets converge to the node. Fig. 5 shows the multihop transmission mechanism, though the figure leaves out ACK between the neighbors.

Meanwhile, the source node needs to defer sending the following packet for the drawback while other nodes are occupying the timeslot. Thereby, the BS sends back the reply packet to inform the node of the arrival of the packet and to indicate that the timeslot is idle.

5. Experiments and results

5.1. Conditions

Experiments were carried out by computer simulation for evaluating the following metrics, considering disaster conditions. The simulation conditions are assumed as follows:

- Computer simulation assumes that nodes and a BS are placed in a residential area by fixed allocation, and the BS collects damage information from nodes.
- The BS is located in the middle of the cell, and nodes are arranged in a grid, where the grid interval is assumed at 20 m, and is denoted by *d*. Experiments assume four types of cell sizes; the radius of each cell is 250 m, 340 m, 500 m and 1000 m. Hence, the number of nodes contained in each cell is 489, 901, 1961 and 7845.
- Direct connection nodes (DCNs), which are able to access the BS directly without damage, are randomly set up in the grid. The number of DCNs is decided according to *DCNR*, which is defined below. Those nodes operate in the cellular mode while the remaining nodes

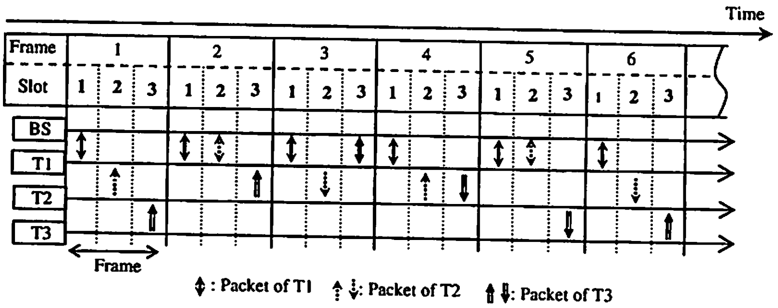


Fig. 5. Multihopping scenario.

transmit a packet by multihopping in the ad hoc mode, and they are set up in the remaining grids.

- The communication range of each node operating in the ad hoc mode is set at the grid interval (d) in order that the node is able to access four adjacent nodes.
- Experiments assume that the communication failure rate is negligible.
- Assuming that the sensing data to be transmitted always exist in a transmission buffer and every node transmits the data at the designated timing immediately, we evaluate throughput and delay for transmitting a packet by multihopping, not including delay in the queue.

5.2. Definition

We introduce certain parameters to evaluate network performances in disaster circumstances, and the metrics for the evaluation.

5.2.1. Parameters

Direct connection node ratio: Direct connection node ratio ($DCNR$), a parameter which considers disaster communications, is defined as the ratio of nodes which can access the BS directly, and is given by

$$DCNR = \frac{\text{Number of direct connection nodes}}{\text{Total number of nodes in a cell}} = \frac{m_1}{N}, \qquad (1)$$

where m_1 is the number of nodes which are able to reach the BS at one hop, and N is the number of all nodes in a cell.

Relative node density: We first define the reference density, which is the condition of the nodes being arranged in all grids, in conditions where the communication range of nodes is equal to the grid interval. Using the reference density, we define a relative node density (RND) as a parameter, which is the ratio of node density for the reference density:

$$RND = \frac{\text{Node density}}{\text{Reference density}}. \qquad (2)$$

5.2.2. Metrics

Reachability: Reachability (γ) is defined as the ratio of nodes which are able to reach the BS directly or by multihopping. The maximum hopping range (MR) is given as a parameter, which is the fixed limit of hop-count. Reachability ($\gamma(n)$) within n hops ($MR = n$) is given by

$$\gamma(n) = \frac{\sum_{i=1}^{n} m_i}{N} = \gamma_1 + \gamma_2 + \cdots + \gamma_n, \qquad (3)$$

where m_i is the number of nodes reachable to the BS at i hops, and $\gamma_1, \gamma_2, \ldots, \gamma_n$ denote the reachability in each hop-count $(1, 2, \ldots, n)$.

Throughput: Throughput within n hops ($\eta(n)$) is defined as the ratio of transmitted packets to the number of packets that all nodes can transmit during T (s), and is given by:

$$\eta(n) = \frac{\sum_{i=1}^{n} q_i(T)}{N \cdot T \cdot \xi}, \qquad (4)$$

where $q_i(T)$ is the number of packets transferred to the BS at i hops during Ts. ξ is the coefficient of the number of packets that a node is able to transmit during the frame interval, where ξ is set up at one (1) in the experiments.

Delay: We define delay as the time for two-way transmission between a node and a BS. That is, the delay is indicated in the total number of frames for a data packet to reach the BS and for the reply packet to return to the source node. The average delay (t_d) of the network within n hops is given by:

$$t_d(n) = \frac{\sum_{i=1}^{n} \sum_{j=1}^{q_i} f_{ij}}{\sum_{i=1}^{n} q_i(T)}, \qquad (5)$$

where $q_i(T)$ is the number of packets transferred to the BS at i hops during Ts, f_{ij} is the number of frames in conditions where the j-packet is transferred at i hops.

5.3. Results

5.3.1. Reachability

We show the results of reachability in Fig. 6 and 7 in conditions where the radius of the cell is 340 m, and the number of nodes is 901. Each graph of Fig. 6 indicates the results in each hop-count as a function of *DCNR*. The results show that the proportion of two hops is dominant in the case when *DCNR* is between 20% and 50%. Even in the range of 10% or less in *DCNR*, a two- or three-hop transmission is still more dominant than other hops. Fig. 7 indicates the reachability of each hopping range in cumulative form. Given that *DCNR* is 50% or higher, *reachability* is up to 90% or more if only *MR* is at two.

According to public reports, 80% of residences suffer damage of the middle level in an earthquake [22]. We assume that wireless devices placed within those residences may receive the impact of the damage. We also assume those devices are able to communicate with neighboring nodes though they cannot access the BS directly due to the impact of the damage. Based on these assumptions, we pay attention to the results when the *DCNR* is 20%. The results of Fig. 7 showed that the network is capable of maintaining reachability of approximately 90% within three hops when the *DCNR* is 20%.

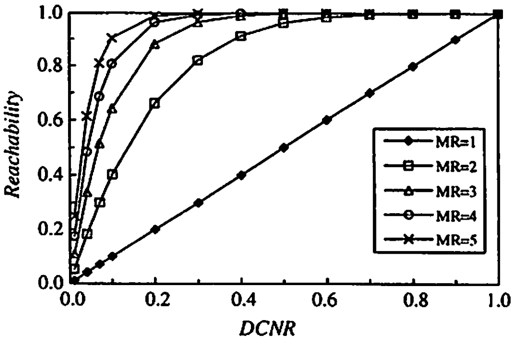


Fig. 7. Reachability in cumulative form.

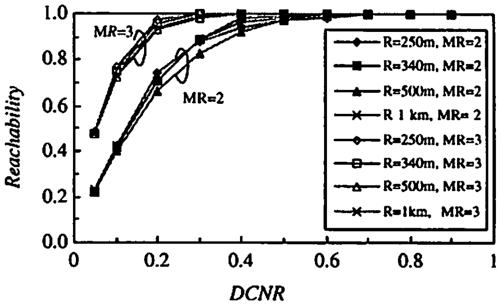


Fig. 8. Impact of a cell size on reachability.

Fig. 8 shows the impact of a cell size on reachability as a function of *DCNR*. Experiments were carried out for four cell sizes as listed in the simulation conditions. The results show that reachability depends on the extent of multihopping regardless of the cell size. Most nodes can reach the BS within a few hops regardless of the cell size, since we assume the direct connection nodes (DCNs) may remain randomly in a cell when a disaster occurs.

The impact of node density on reachability is shown in Fig. 9 in conditions where *DCNR* is 20%, and the radius of the cell is 340 m as a

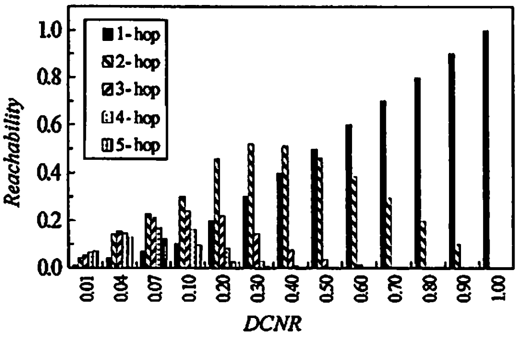


Fig. 6. Reachability in each hop-count.

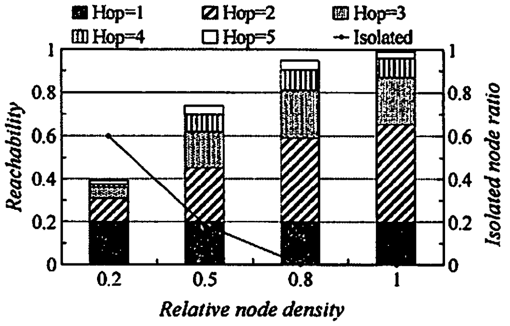


Fig. 9. Impact of node density on reachability.

function of relative node density (*RND*). Even if the node density decreases at 50%, reachability is maintained at 60% by multihopping within three hops, while it is maintained at 90% or more in the case of the reference density. The graph with the solid line indicates the isolated node ratio, which is the ratio of nodes that are isolated from surrounding nodes. The results actually show the impact of decreasing the density. Since the isolated node ratio is about 20% in conditions where *RND* is 50%, the possible reachability is up to 80% by increasing the hopping range to four hops or more.

From these results, ECCA is capable of allowing most of the nodes to reach the BS within a few hops even in disaster circumstances where available node density may decrease.

5.3.2. Throughput

Fig. 10 shows the results of throughput in conditions where the number of nodes is 901. Throughput is calculated by Eq. (4) according to the measurements of delivered packets. The graphs indicate the results of $MR = 1,2,3$ and unlimited hopping as a function of *DCNR*. In the case where *MR* is at two and three, and *DCNR* is at 20%, the throughput is retrieved up to 35% and 40%, respectively. Even if increasing *MR* up to four or more, the throughput is approximately equal to the result of $MR = 3$ in the range of $DCNR >$ 20%. ECCA can transmit only a packet in a timeslot, and in addition, it employs the end-to-end reply manner. Thereby, a source node is necessary to defer sending a follow-up packet; performance for transmitting a packet is restricted. As a result, the throughput is not improved as drastically as reachability is.

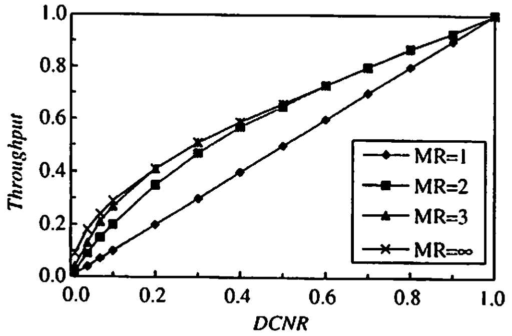


Fig. 10. Average throughput.

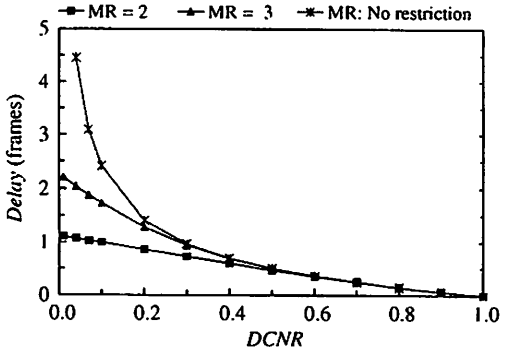


Fig. 11. Average transmission delay.

5.3.3. Delay

As described for the network operation in the experimental condition, data always exists in the buffer of a node, and a packet is immediately transmitted when a reply packet for the previous transmission has arrived. The duration to transmit a packet from a source node to the destination and to send back the reply to the source node takes $2k - 2$ frames according to the access scheduling manner shown in Fig. 5, where k is the number of hops. Fig. 11 shows the average two-way transmission delay of all nodes in the network, where *MR* of each graph is one, two, three and has no restriction number. In the case of $MR = 1$, the reply arrives immediately during the timeslot. In the cases of $MR = 2$ or 3, even if *DCNR* is at 0.2 or 0.1, average delay is one or two frames, respectively. Therefore, the network is capable of handling packets in a short delay, and the feature is suitable for disaster communications.

6. Conclusion

This paper has proposed a hybrid wireless network scheme, ECCA, which combines ad hoc networks and a cellular network, and a routing protocol. The routing protocol allows a node to discover a route via neighboring nodes by monitoring surrounding communications without a route request packet. Some experiments showed that approximately 90% of nodes are capable of reaching the base station within three hops by multihopping even if only 20% of the nodes can access the BS directly. The results also showed that the network is feasible of operating in a short delay for delivering a packet to the BS. However, throughput is not retrieved sufficiently, while reachability improves sufficiently by two or three hops. Therefore, the network is suitable for collecting damage assessment information and transmitting urgent traffic quickly and stably, while the data is restricted to a small size. We expect that the proposed network scheme and the routing protocol can satisfactorily provide operation for disaster communications without congestion even in the aftermath of a large natural or man-made disaster. Further study is underway to investigate the total performance of the network by modeling with a probability process. The access protocol is also underway for further improvement of the throughput.

Acknowledgment

This work was supported by the project funded by Telecommunications Advancement Organization of Japan.

References

[1] K. Kobayashi (Ed.), Special Issue: Information and Communication Electronics in Disasters, J. IEICE 79 (1) (1996) 1–48 (in Japanese).

[2] M. Frodigh, S. Parkvall, C. Roobol, P. Johansson, P. Larsson, Future-generation wireless networks, IEEE Personal Commun. 8 (5) (2001) 10–17.

[3] S. Omori, Y. Yamao, N. Nakajima, The future generations of mobile communications based on broadband access technologies, IEEE Commun. Mag. 38 (12) (2000) 134–142.

[4] T. Otsu, Y. Aburakawa, Y. Yamao, Multi-hop wireless link system for new generation mobile radio access networks, IEICE Trans. Commun. E85-B (8) (2002) 1542–1551.

[5] Cabinet Office Government Japan, Disaster Management in Japan, http://www.bousai.go.jp/panf/saigai.html, 2002.

[6] N. Tada, Y. Izawa, M. Kimoto, T. Maruyama, H. Ohno, M. Nakayama, IAA system (I Am Alive): the experiences of the Internet disaster drills, INET 2000 Proceedings, http://www.isoc.org/isoc/conferences/inet/00/cdproceedings/8l/8l_3.htm, 2000.

[7] Y. Shimizu, Advanced accelerometers and liquefaction meters for damage assessment of gas distribution systems, Proc. MEDAT-1, 2000, pp. 57–65.

[8] T. Fujiwara, Y. Shimazaki, H. Toyoshima, S. Ito, M. Sugiura, M. Atsumi, T. Watanabe, S. Mizushina, A TD-CDMA data collection system for city lifeline monitoring, Proc. IEEE VTC2000-Spring, Tokyo 2000, pp. 1630–1635.

[9] T. Fujiwara, S. Mizushina, A. Adachi, T. Watanabe, A wireless system for disaster damage monitoring in vulnerable ISM band, Proc. Networks, Atlanta, 2002, pp. 27–37.

[10] A. Meisser, T. Luckenbach, T. Risse, T. Kirste, H. Kirchner, Design challenges for an integrated disaster management communication and information system, Proc. IEEE DIREN2002, New York, 2002.

[11] E.M. Royer, C.-K. Toh, A review of current routing protocols for ad hoc mobile wireless network, IEEE Personal Commun. 6 (2) (2002) 46–55.

[12] C.-K. Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall PTR, Englewood Cliffs, NJ, 2002.

[13] A. Ephremides, Energy concerns in wireless networks, IEEE Wireless Commun. 9 (4) (2002) 48–59.

[14] G. Zussman, A. Segall, Energy efficient routing in ad hoc disaster recovery networks, Proc. IEEE INFOCOM 2003, San Francisco, 2003.

[15] Y. Yamao, T. Otsu, A. Fujiwara, H. Murata, S. Yoshida, Multi-hop radio access cellular concept for fourth-generation mobile communications system, Proc. IEEE PIMRC2002, Lisbon, 2002.

[16] H.-Y. Hsieh, R. Sivakumar, A hybrid network model for cellular wireless packet data networks, Proc. IEEE GLOBECOM2002, Taipei, 2002.

[17] H. Wu, C. Quiao, S. De, O. Tonguz, Integrated cellular and ad hoc relaying system: iCAR, IEEE J. Select. Areas Commun. 19 (10) (2001) 2105–2115.

[18] S.T. Stanley Chia, W.C.Y. Lee, A synchronized radio system without stable clock sources, IEEE Personal Commun. 8 (2) (2001) 45–50.

[19] H. Yahata, Autonomous master-slave frame synchronization among micro-cellular base stations, IEICE Trans. Commun. J81-B-II (4) (1998) 278–288 (in Japanese).

[20] C.D. Young, USAP: a unifying dynamic distributed multichannel TDMA slot assignment protocol, Proc. IEEE MILCOM'96, vol. 1, 1996, pp. 235–239.

[21] J. Sheu, C. Chao, C. Sun, A clock synchronization algorithm for multi-hop wireless ad hoc networks, Proc. IEEE ICDCS2004, Tokyo, 2004, pp. 574–581.

[22] Shizuoka Prefecture Disaster Prevention Bureau, Earthquake Damage Estimation Results III, no.182-2001, Shizuoka Prefecture Earthquake Preparedness Education Center, 2001.

[23] M. Oda, H. Uehara, M. Yokoyama, H. Ito, Safety information collecting network using self-organizing packet relay routing, IEICE Trans. Commun. J85-B (12) (2002) 2037–2044 (in Japanese).

Takahiro Fujiwara is a senior researcher in the Information Technology Laboratory at Enegene Co., Ltd, Japan, investing a wireless monitoring system for emergency communications. He completed his Ph.D. in Science and Technology at Shizuoka University in 2004. He is working on the disaster restoration support project with image processing and ad hoc networking, conducted by Shizuoka University and funded by NiCT of Japan. His current research interests include ad hoc networking, MAC protocols for wireless communications, especially sensor networks, and the application systems. He is a member of IEEE, IEEE Communications Society, IEEE Computer Society, ACM SIGMOBILE, IEICE (The Institute of Electronics, Information and Communication Engineers, Japan), and IEEJ (The Institute of Electrical Engineers of Japan).

Takashi Watanabe is a Professor in Department of Computer Science at Shizuoka University, Japan. He completed his Ph.D. in Communications Engineering at Osaka University, Japan in 1987. He has served on many program committees for networking conferences, IEEE, ACM, IPSJ (Information Processing Society of Japan), IEICE (The Institute of Electronics, Information and Communication Engineers, Japan). His research interests include mobile networking, ad hoc networks, sensor networks, ubiquitous networks, intelligent transport systems, specially MAC and routing. He is a member of IEEE, IEEE Communications Society, IEEE Computer Society, ACM SIGMOBILE as well as IPSJ and IEICE.