Abstract— MANETs (Mobile Ad hoc NETworks) are drawing interest because it can provide a means of communication when an existing public network has been damaged by a disaster, or in areas where there is no fixed-line network available. For audio/video communication to be feasible in a MANET, the routing method used must provide high real-time performance. This paper proposes a locally complementary multi-path routing protocol, which can reduce the size of the network section for which route restoration is required in the event of a disaster. This makes it possible to achieve high real-time performance and maintain existing connections, thereby avoiding interruptions in audio/video communication. Specifically, this protocol secures a spare route for every two hops on the main route. Two alternative methods for securing spare routes are presented: an independent route securing method and a simultaneously route securing method. These as well as AODV (Ad hoc On-Demand Distance Vector) have been compared in terms of the number of control packets generated. The simultaneous route securing method has been built into a MANET emulator, and the percentage of successful establishment of the initial routes has been assessed.

Keywords— MANET; multi-path routing protocol; SIP; securing spare route; AOMDV

I. INTRODUCTION

MANETs (Mobile Ad hoc NETworks) are drawing interest because it can provide a means of communication when an existing public network has been damaged by a disaster, or in areas where there is no fixed-line network available [1]. A MANET is made up of mobile terminals. Data are transferred between two terminals through a route involving multiple hops. The situations in which the network is economically viable are so limited that actual applications have not been developed. In the world of the Internet, connection-oriented applications (for audio/video communication, etc.) have been developed based on SIP (Session Initiation Protocol) [2]. Provision of SIP-based services in a MANET should encourage many applications for a MANET to be developed. Although many studies have been made on handling SIP services in a MANET [3]-[9], a lack of experimental tools available has limited their scope to handling only the processes from a session establishment request to the start of the session. The authors have developed and extended a MANET emulator for use as a service experiment tool for a MANET [10]-[16].

To make audio/video communication feasible in a MANET, the routing method used must provide high real-time performance. In a MANET, a connection between SIP clients may be broken for a number of reasons: movements of the terminals involved in the connection, loss of wireless links, and running out of terminal batteries.

Several multi-path routing methods based on AODV (Ad hoc On-Demand Distance Vector) [17] have been proposed, such as AOMDV (Ad hoc On-Demand Multipath Distance Vector) [18] and the route disjoint protocol [19]. However, since the route disjoint protocol selects candidate paths for re-routing from the entire network, it takes considerable time in reconfiguring the network, a feature detrimental to real-time performance. A more reliable routing method is required if SIP services are to be provided in a MANET.

This paper proposes a locally complementary multi-path routing protocol, which can reduce the network section for which route restoration is required, in order to achieve high real-time performance, and make it possible to maintain existing connections, thereby avoiding interruptions in ongoing audio/video communication. Section II reviews related studies on multi-path routing. Section III proposes a locally complementary routing protocol, which features high real-time performance, and two alternative methods of securing spare routes: an independent route securing method and a simultaneously route securing method. Section IV describes an evaluation system in which the simultaneous route securing method was implemented. Section V evaluates this method in terms of the percentage of successful establishment of the initial routes by conducting experiments on this evaluation system with different network models. In addition, the two spare route securing methods as well as AODV are compared in terms of the number of control packets generated.

II. RELATED WORK

A. AOMDV

AOMDV is a routing protocol that allows multiple non-overlapping routes to be secured between the originator and destination terminals, as between nodes S and D in Fig. 1. However, Node C in Fig. 1 is involved in two routes, and thus is an Achilles’ heel. If Node C comes down, both routes are lost, and communication between the two end terminals is...
disrupted. Therefore, it is necessary to avoid creating such critical nodes if real-time communication is to be provided.

**B. Route disjoint protocol**

Unlike AOMDV, the route disjoint protocol secures multiple routes without creating an Achilles’ heel node. As shown in Fig. 2, the nodes of the two routes are disjoint. The downsides of this protocol are that it is necessary to look at the entire network to reconfigure routes, and that route restoration takes a long time because, when a link failure has been detected, Terminals S and D must be notified of it before the routes concerned are switched. It is necessary to reduce route restoration time if real-time communication is to be provided.

**III. LOCALLY COMPLEMENTARY MULTI-PATH ROUTING**

**A. Overview**

This section proposes a locally complementary multi-path routing protocol. It mitigates the disadvantages of AOMDV by reducing the size of the network sections for which route restoration is required. It secures and holds a spare route for every two hops on the main route in order to allow ongoing communication to be maintained even during route restoration. Since all nodes are mobile, this protocol is based on AODV, which is a reactive protocol. Examples of the main route and spare routes are shown in Fig. 3.

Since a spare route is secured for each two hops of the main route, a route can be restored in a short time. Only up to 3 hops are allows for a spare route. For example, a spare route can be S-13-12-10 in Fig. 3. While AOMDV can involve Achilles’ heel nodes in spare routes, the locally complementary multi-path routing protocol does not. Even when node 10 in Fig. 3 fails, for example, communication can be quickly restored because spare route 11-8-5 is available. Unlike the route disjoint protocol, which examines the entire network for route restoration, the proposed protocol needs to look at only two hops in the main route. Therefore, the route concerned can be reconfigured in a short time.

Two alternative methods of securing spare routes at the time of initial route configuration are described in Subsections III.B and III.C. They are called an independent route securing method and a simultaneous route securing method. To secure spare routes at the time of route configuration, we have revised messages RREQ (Route REQuest) and RREP (Route REPLY), and added SpareRREQ and SpareRREP, as shown in Fig. 4. All the four messages are of extended packet format. The shaded parts show the added parts. Why these parts are added and how they are used are described in the next subsection. The number within each parenthesis is the number of bits. Where there is no such parenthesis, the number of bits is 1. The meaning and use of each existing field is the same as in RFC3561 [17], and thus are not explained here.
Fig. 4. Extended control packet formats(2/2).

B. Independent route securing method

This method secures spare routes by flooding the network with a SpareRREQ after the main route has been secured. It secures the main route in the same manner as AODV. When a node on the main route receives an RREP, it writes a relevant value into the Two Hop IP Address field of the RREP because it wants to send a SpareRREQ to nodes two hops away. In the example of Fig.3, when Node 1 has received an RREP from Node D, it writes the address of Node D into its Two Hop IP Address field, and sends the message to Node 5. Node 5 writes Node D’s address into the Spare Destination IP Address field, its own address into the Spare Originator IP Address field, and Node 1’s address in the Relay NG IP Address field of a SpareRREQ, and floods the network with the message with TTL=3. Although Node 1 receives this SpareRREQ, it does not rebroadcast it because the value in the Relay NG IP Address field is its own address. Consequently, this SpareRREQ is relayed on a route (5-4-3-D), which is separate from the main route. Node D sends a SpareRREP as a reply, and a spare route is secured. A problem with this method is that a large number of control packets are generated and flow in the network because each of Nodes S, 11, 10 and 5 broadcasts a SpareRREQ to secure a spare route.

C. Simultaneous route securing method

This method does not use SpareRREQ. It secures spare routes by sending a SpareRREP at the same time when the main route is secured. When an RREQ is broadcast using AODV, nodes receive multiple RREQ messages, and determine whether to discard them by examining the sequence number of each message. Flooding of the network with RREQs is shown in Fig.5, and the resulting routing table is shown in Fig.6. Each solid arrow in Fig.5 corresponds to one of the encircled parts in Fig.6, and indicates a route secured when Terminal S has flooded the network with an RREQ that is intended for Terminal D. Dotted arrows show routes that have been secured by RREQs that are to be discarded. In the simultaneous route securing method, spare routes are secured using RREQs that are to be discarded because they share the same sequence numbers. When SpareRREPs is unicast, the main route shown by solid lines and spare routes shown by dotted lines in Fig. 3 are secured. At the same time, relevant values are written into the SpareDestIPAddr field and the SpareRelayIPAddr field in the routing table so that the destination and the IP addresses of the relaying nodes of a spare route can be retained. The first node that has sent an RREQ is designated as the relaying node on the main route, and the second node that has sent an RREQ is designated as the relaying node on the spare route. For Node D, for example, Node 1 is the relaying node on the main route, and Node 3 is the relaying node on the spare route. A relevant value is written into the Two Hop IP Address field of the RREQ so that a node two hops back can be identified.

The algorithm for simultaneous route securing is described in the following, using Fig. 5. First, Terminal S floods the network with an RREQ. A node that has received this RREQ writes the address of its relaying node into the Two Hop IP Address field, and broadcasts the message. If the sequence number of the message is new, the node address is written into the routing table, and the message is rebroadcast. If the sequence number is the same as that of a previously received message, the node is registered as the relaying node of the spare route in the table. When Terminal D has received an RREQ, and if the sequence number of the message is new, it sends back an RREP to the secured route (Node 1). If the sequence number of the RREQ is the same as that of a previously received message, Terminal D sends back a SpareRREP. The node on the main route that has received the RREP writes its own IP address into the Spare Destination IP Address field, the IP address of a node two hops back into the Spare Originator IP Address field, and the IP address of the relaying node into the Relay NG IP Address field, of a SpareRREP, and sends the message to the relaying node on the spare route. The node that has received this SpareRREP sends it to the adjacent node if the IP address written in the Spare Originator IP Address field of the message is that of this adjacent node. If it is not, the node transfers the message to either the relay node on the main route or that on the spare route whichever has an IP address different from that written in the Relay NG IP Address field. Note that a spare route has been secured in the forward direction (direction towards Terminal D) when a SpareRREP is received, and in the backward direction (direction towards Terminal S) when a SpareRREP is sent.

Fig. 5. Flooding with an RREQ.

Fig. 6. Routing table created.
The main cause of a route being disrupted are a node dropping out of the network due to its battery running out, and a link being disrupted due to movements of a node on the route.

1) In the case of a node dropping out of the network: Examples of securing the main route and spare routes are shown in Fig. 7. When a node (e.g., Node b) on the main route drops out of the network, two alternative methods can be conceived to secure a new main route. Method 1 is to replace a part of the previous main route with its spare route, as shown in Fig. 7(a). Method 2 is to secure a new main route, as shown in Fig. 7(b). If the number of hops of the spare route that substitutes for the route provided by the dropout node is 2, the results of Methods 1 and 2 are more or less the same. However, if the spare route involves 3 hops, Method 1 increases the number of hops on the main route. This also means that the number of spare routes that stand by also increases. Not only do the spare routes become more redundant but also many control packets are generated and flow in the network to secure the spare routes. In contrast, with Method 2, if it is found that Node f can substitute for Node b, only Node f broadcasts a SpareRREQ. When Terminals S and D send back a SpareRREP, the spare route is restored. To sum up, when a node on the main route drops out, a new node that can substitute for the dropout node is searched for, and a different main route is secured anew using this node.

When a route on a spare route drops out, a new spare route is secured.

2) In the case of a link being disrupted: When a link on the main route is disrupted, and the two nodes connected to this link attempt to establish a new link, the number of hops between the two nodes will increase from 1 to 2. In addition, when the relevant nodes, including the node newly incorporated into the main route, try to secure a spare route for the new link, excessively many control packets will be generated in the network. However, if the above process is considered as an attempt to secure a 3-hop spare route to replace the original 2-hop spare route, all that is needed is to re-secure spare routes for the newly added node. If this process is continued, many redundant routes may be created. Therefore, it is necessary to refresh routes at certain intervals or at the trigger of a certain event.

When a link between two nodes on a spare route is disrupted, all that is required is to secure a new spare route between the spare originator node and the spare destination node.

### Extended data packet format

<table>
<thead>
<tr>
<th>Type(8)</th>
<th>Main or Spare(8)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Destination IP Address(32)</td>
</tr>
<tr>
<td></td>
<td>Originator IP Address(32)</td>
</tr>
<tr>
<td></td>
<td>Originator Sequence Number(32)</td>
</tr>
<tr>
<td>Hop count(16)</td>
<td>TTL(16)</td>
</tr>
<tr>
<td>Spare Destination IP Address(32)</td>
<td>Data Sequence Number(32)</td>
</tr>
</tbody>
</table>

**Fig. 8.** Extended data packet format.

### IV. DEVELOPMENT OF AN EVALUATION SYSTEM

The proposed multi-path routing protocol was implemented on an already developed MANET emulator [11] using VC++6.0. The system configuration of the revised MANET emulator is shown in Fig. 9. The proposed protocol was implemented by extending AODV of the routing module [Routing]. In addition, the emulator can simulate the remaining battery level [Battery], the interface with the monitor [Monitor IF], conversion between the virtual and real IP addresses [CNV], a mobility model [Movement], the MAC (Media Access Control) layer [MAC], radio coverage [Zone], etc. Module [EN] simulates inter-SIP client communication within the emulator.
V. EVALUATION

A. Initial spare route configuration success ratio for the simultaneous route securing method

The ratio of successful spare route configuration attempts was measured for the different network models with different numbers of hops on the main route, shown in Fig. 10. The result is shown in Fig. 11. If there are N hops on the main route, N-1 spare routes can be secured. The Initial spare route configuration Success Ratio (ISR) was calculated using Eq. (1). It was considered successful if N-1 spare routes were secured without sending SpareRREQs. In the evaluation experiment, five route configuration attempts were made for each model.

ISR \( = \frac{N_A}{N_C} \)  

where 
\( N_A \) = Total number of spare route configuration attempts 
\( N_C \) = Total number of spare route configuration candidates

Network models were fixed for networks with up to 5 hops. In the network model in which the number of hops is larger than 5, all nodes other than the originator and destination nodes were placed at random, and then the initial route configuration was executed. Network configuration examples for 4 hops and 6 or more hops on the main route are shown in Fig. 11.

In the network model of 4 hops, 3 spare routes can be secured. Among these, the number of spare routes that were secured only with RREQ, RREP and SpareRREP was counted. The initial spare route configuration situation for every attempt on 4 hop model is shown in Fig. 12. There are 3 candidate spare routes. Since 2 spare routes could be secured at first, second and 4th attempt, the ISR was calculated to 0.66. Also, at 5th attempt, 3 spare routes could be secured, and then the ISR was 1. At third attempt, the numbers of hops on the main route are 4 hops. However, 2 spare routes could be secured, and then the ISR was 0.5. Therefore, when five attempts were added together, the ISR was as follows.

\[
\text{ISR}_{4\text{hop}} = \frac{(2+2+2+2+3)}{(3+3+4+3+3)} = 0.68
\]

For the network models with 2 hops and 3 hops, the success ratio was 1 because the proposed algorithm can secure spare routes without fail. For network models with 4 or more hops, the average ratio of successfully securing spare routes was 0.68. This is because the proposed algorithm selects any second node that sent an RREQ as a relay node on a spare route, which may cause a relay node to be used for multiple spare routes. When this happens, not all spare routes can be secured successfully. A way to avoid a relay node being used for multiple spare routes and thereby to raise the ratio of successfully securing spare routes is to define a new response message to a SpareRREP, consider the third and fourth nodes that sent an RREQ as a candidate relay node on spare routes, and send a SpareRREP to the next node if there was no reply.
B. Comparison in terms of the number of control packets generated

The number of control packets sent during route configuration was counted. Different route securing methods are compared in terms of the number of control packets generated in Fig. 13. The network models used were those shown in Fig. 10.

With the independent route securing method, nodes on the main route flood the network with a SpareRREQ to secure spare routes. Therefore, as the number of hops on the main route increases, so does the number of control packets generated. With the simultaneous route securing method, spare routes are secured only with RREQs and SpareRREPs. Therefore, this method generates fewer control packets than the independent route securing method. It can be seen in Fig. 12 that spare routes can be secured by sending only as many SpareRREPs as are required.

VI. CONCLUSIONS

This paper has proposed a locally complementary multi-path routing protocol, which can reduce the size of the network section for which route restoration is required in the event of a disaster, in order to achieve high real-time performance and make it possible to maintain existing connections, thereby avoiding interruptions in ongoing audio/video communication. This protocol secures multiple routes by unicasting a SpareRREP for route configuration using AODV. Two alternative spare route securing methods have been presented: the independent route securing method and the simultaneous route securing method. These two methods as well as AODV were compared in terms of the number of control packets generated. The simultaneous route securing method can reduce the generation of control packets. This method was implemented in a MANET emulator to measure the initial route configuration success ratio. It was shown that the success ratio was about 70% even when the number of hops on the main route is 6 or more.

The issues that remain to be studied include implementation of SIP-based real-time communication using the proposed protocol to verify the protocol’s feasibility in real communication.

REFERENCES