A Reliable Routing Scheme for Post-Disaster Ad Hoc Communication Networks

Muhammad Ibrahim Channa, Kazi M. Ahmed
School of Engineering and Technology, Asian Institute of Technology, Thailand
Email: {muhammad.ibrahim.channa, kahmed}@ait.ac.th

***Abstract*— The natural or man-made disaster demands an efficient communication and coordination among first responders for successful emergency management operations. During emergency situations such as an earthquake or a flood, the traditional telecommunication infrastructure may be damaged and may not provide adequate communication services to emergency management teams. Mobile ad hoc networks are used in such type of situations for exchanging emergency related information. During emergency situation, the deployed ad hoc communication network may itself be prone to failures and vulnerable to malicious threats. The first responders use real-time applications for exchanging emergency related information, which may create network congestion. The significant loss of emergency related information may cause mismanagement of emergency response efforts. We propose a reliable routing scheme for post-disaster ad hoc communication networks, which finds the shortest possible routes with all reliable nodes. The proposed scheme also detects packet forwarding misbehavior caused by network fault or congestion in an active route and reroutes packets through other reliable route. The performance of the proposed scheme is evaluated in terms of packet delivery ratio, end-to-end delay and routing overhead through extensive simulations.**

***Index Terms*— Post-disaster communications, Mobile ad hoc network, Reliable routing, Broken nodes, Network congestion**

I. INTRODUCTION

It is a great challenge for public emergency services to cope with the crisis situations arising due to natural or man-made disasters. The most common disasters include earthquakes, floods and nuclear explosions. It is necessary to provide relevant information to concerned rescue workers in a timely manner for coping with such disasters in an effective and coordinated manner [1]–[4]. As coordination requires current information within and among various rescue organizations in real time, the deployment of an integrated information and communication system is essential for efficient, reliable and secure exchange of information [5]. A large scale emergency response operation involves multi-organizational teams including public authorities, volunteer organizations and the media. These entities work together as a virtual team to save lives and other community resources [6].

The availability of telecommunication services is of great importance during emergency situations, as it is the only means of communication among first responders, affected people and emergency management centers. During Hurricane Katrina [7], [8], the existing telecommunication infrastructure was badly damaged and the remaining parts of the network were not able to provide adequate communication services to the first responders [9]. In such type of situations, mobile ad hoc networks [10] are commonly used for exchanging emergency related information. These networks don't rely on existing infrastructure such as access points or base stations and configure automatically [11] when the network size varies dynamically. Figure 1 shows the deployment of an ad hoc communication network in a disaster affected area. The emergency site ad hoc communication network is connected with emergency management centers, hospitals, NGOs and media centers through gateway nodes and wide area network.

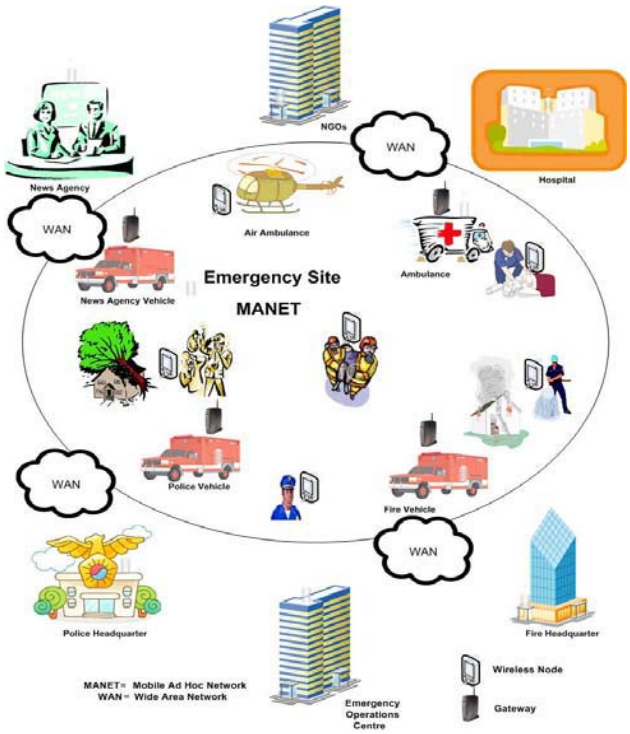

Figure 1. The deployment of an ad hoc communication network at emergency site

An emergency response network comprises of mobile devices such as smart phones and PDAs used by different rescue workers belonging to different rescue

Manuscript received February 05, 2011; revised April 30, 2011; accepted June 05, 2011

doi:10.4304/jcm.6.7.549-557

organizations. Reliable and robust communication is vital for successful emergency response operations [9]. The reliability of a network is its ability to perform a designated set of functions under dynamically changing conditions. During emergency situation, the deployed ad hoc communication network may itself be prone to failures and vulnerable to malicious threats [6]. An ad hoc communication network failure has life-or-death significance during emergency situations. A node may be broken by experiencing some software or hardware fault which prevents it from forwarding the packets successfully. A malicious node may launch a Denial of Service (DoS) attack [12] to create communication interruptions among first responders and is beyond the scope of this article. The first responders use real-time applications for exchanging emergency related information. The increasing number of simultaneous communications among first responders may create congestion in some parts of the network. A congested node may lack the CPU cycles, buffer space or available bandwidth to forward packets successfully. The significant loss of emergency related information may cause mismanagement of emergency response efforts.

Several reliable routing schemes have been proposed for mobile ad hoc networks. In weight-based reliable routing scheme [13], a route having more energy, less error rate and shorter length is selected for data transmissions. In cross-layer energy aware reliable routing scheme [14], the node's residual energy is used as a route selection metric. The mobility sensitive routing approach [15] is a multi-protocol scheme which activates an appropriate routing scheme based on the mobility pattern of the network nodes. In distributed long lifetime routing scheme [16], the source node forwards data through the shorter route while keeping longer route as backup. In reliable source routing scheme [17], the source node finds a route meeting the reliability requirements of the application. The stable and energy efficient routing scheme [18] uses node stability and energy efficiency as route selection metrics. The cross-layer reliable routing scheme [19] uses received signal strength to find reliable links in an stable route. The reliable multi-rate ad hoc routing protocol [20] uses route assessment index (RAI) to find the shortest possible route with high capacity links. The reliable dynamic source routing for video streaming [21] uses service feedback information to compute reliability of paths. The reliability map based routing (RMR) scheme [22] constructs reliability maps of deployment region and performs routing by avoiding compromised cells. The secure neighbor discovery scheme [23] prevents a legitimate or a malicious node from being incorrectly added to the neighbor list of another legitimate node. The network coding with imperfect overhearing scheme [24] improves overall system performance in cooperative relay networks. The secure packet transfer scheme [25] uses repeated games to identify malicious nodes in wireless sensor networks.

The proposed schemes use node energy [13], [14], [18], node mobility [15], route lifetime [16], successful data transmissions [17], signal strength [19], link capacity [20] and service feedback [21] as reliability metrics. None of the schemes addresses dynamic detection of packet forwarding misbehavior caused by network fault or congestion. We propose a reliable routing scheme for post-disaster ad hoc communication networks, which finds the shortest possible routes with all reliable nodes. The reliability of a node is computed by aggregating its packet forwarding behavior information. The proposed scheme also reroutes packets through other reliable route if some faulty or congested node performs packet forwarding misbehavior in an active route. The proposed scheme uses node reliability and end-to-end delay as route selection metrics.

The rest of the paper is organized as follows. Section II presents network model. Section III describes the proposed reliable routing scheme. Section IV comprises of the simulation results and section V concludes the paper.

II. Network Model

An ad hoc network is modeled as a graph $G = (V, E)$, where V represents the set of nodes and E represents the set of links between nodes. A path P of length l consists of a set of nodes $i, j, k, ..., n \in V$ and $(i, j) \in E$. We assume that the links are bidirectional, so if $(i, j) \in E$ then $(j, i) \in E$. Node i establishes wireless links with all its neighbors N_i, which are within its transmission range T_i. If the distance between node i and node j is greater than T_i, link (i, j) is assumed to be broken. All nodes are uniformly distributed over the network and each node moves independently in a random direction with a random speed. We model the behavior of a faulty or congested node j through a random variable $X(j)$, which follows the Bernoulli distribution as follows:

$$X(j) = \begin{cases} 1 & j \text{ forwards packet to } k \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

We further assume that a faulty node performs packet forwarding misbehavior continuously by dropping random number of received packets. A reliable node may perform packet forwarding misbehavior randomly while experiencing significant congestion.

III. Proposed reliable routing scheme

The proposed reliable routing scheme comprises of three major components namely Reliability Manager, Route Setup and Route Maintenance. The *Reliability Manager* is responsible for maintaining reliability information about neighbor nodes and stores this information in reliability database. The *Route Setup* establishes the shortest possible route comprising of only reliable nodes. If some broken or congested node performs packet forwarding misbehavior in an active route, the *Route Maintenance* is initiated by Reliability Manager to inform the source node to establish a new reliable route.

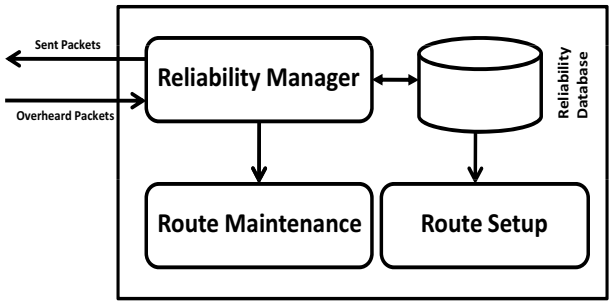

Figure 2. Reliable routing scheme model

The proposed reliable routing scheme is implemented by extending Ad Hoc On Demand Distance Vector (AODV) [26] routing protocol. The AODV routing protocol is preferred as it is on-demand, provides fresh enough routes and is more scalable. The on-demand approach enables AODV to find routes when desired and reduces control packet overhead. The sequence numbers act as time stamps and help AODV to find up-to-date route to a destination. In AODV, if a node is part of a route, it stores single entry for the destination in its routing table. This reduces storage overhead at each node and makes AODV more scalable. The proposed reliable routing scheme model is shown in figure 2.

A. Reliability Manager

The Reliability Manager maintains reliability information about neighbor nodes by overhearing their transmission in promiscuous mode [27] and identifies misbehaving nodes dynamically. In promiscuous mode, if node j is within transmission range of node i, node i can overhear transmission to and from node j even if those communications don't involve node i. When a data packet is sent by node i to node j, the Reliability Manager at node i stores the packet information such as packet ID, source address and destination address in its buffer and increments the value of $S_{i,j}$ by one. When node i overhears a packet from one of its neighbors, it compares the ID, source address and destination address of the overheard packet with all entries in its buffer. If there is a match, the Reliability Manager at node i assumes successful forwarding of the packet by node j to its next hop and increments the value of $F_{i,j}$ by one. The corresponding entry is then removed from the buffer at node i.

The Reliability Manager at node i evaluates the packet forwarding behavior of neighbor j for every n consecutively forwarded packets. This helps the Reliability Manager at node i to obtain the latest packet forwarding behavior of neighbor j. The value of n should be selected based on certain assumptions. First, the Reliability Manager at node i takes reasonable amount of time to evaluate packet forwarding behavior of neighbor j. Second, if node j is a broken node, the packet loss should be minimum. Third, if node j stay near the boundary of the transmission range of node i and starts moving away from node i, node i overhears n packets from node j to complete its behavior evaluation before node j moves out of its transmission range. The value of n is computed as the product of application's packet rate per second A_r and behavior evaluation time interval Δ_t as follows:

$$n = A_r \times \Delta_t \tag{2}$$

We assume that all applications generate the same number of packets per second. When the number of packets sent by node i to node j reaches n, the Reliability Manager at node i computes the packet forwarding ratio of node j as follows:

$$Pfr_{i,j} = \frac{F_{i,j}}{S_{i,j}} \tag{3}$$

where $S_{i,j} = n, F_{i,j} \leq n$ and $n > 0$

The Reliability Manager at node i categorizes the packet forwarding behavior of neighbor j in one of the two categories. If the packet forwarding ratio of node j is greater than or equal to packet forwarding threshold Th_{pfr}, it is known as positive behavior of node j observed at node i, otherwise; it is known as negative behavior of node j observed at node i. The positive and negative behaviors of node j observed at node i can be represented by $B_{p_{i,j}}$ and $B_{ni,j}$ respectively. If there is a positive behavior of node j observed at node i, $B_{p_{i,j}}$ is incremented by one as follows:

$$B_{p_{i,j}} = \begin{cases} B_{p_{i,j}} + 1 & Pfr_{i,j} \geq Th_{pfr} \\ B_{p_{i,j}} & Pfr_{i,j} < Th_{pfr} \end{cases} \tag{4}$$

Similarly, if there is a negative behavior of node j observed at node i, $B_{ni,j}$ is incremented by one as follows:

$$B_{ni,j} = \begin{cases} B_{ni,j} + 1 & Pfr_{i,j} < Th_{pfr} \\ B_{ni,j} & Pfr_{i,j} \geq Th_{pfr} \end{cases} \tag{5}$$

If there is a negative behavior of node j observed at node i, the Reliability Manager at node i initiates the *Route Maintenance* to inform the source node to establish a new reliable route. The value of Th_{pfr} should be selected in such a way that if node j drops significant number of received packets, the remaining packets may be rerouted through other reliable route. After each evaluation of node j made by node i, the value of $S_{i,j}$ and $F_{i,j}$ is reset to zero.

The Reliability Manager at node i uses Beta probability density function [28] to compute the expected probability of positive behavior of neighbor j. The Beta family of probability density functions is a continuous family of functions indexed by two parameters α and β. The Beta distribution $f(p|\alpha, \beta)$ can be expressed by using Γ function as follows:

$$f(p|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{(\alpha-1)}(1-p)^{(\beta-1)} \tag{6}$$

where $0 \leq p \leq 1, \alpha > 0$ and $\beta > 0$

If there is a binary process with two possible outcomes $\{x, \bar{x}\}, r$ represents the observed number of outcome x and s represents the observed number of outcome $\bar{x}$, then the probability density function of outcome x in future can be obtained by setting the values of α and β as follows:

$$\begin{aligned} \alpha &= r + 1 \\ \beta &= s + 1 \end{aligned} \tag{7}$$

where $r, s \geq 0$.

The probability expectation value of Beta distribution function is given by:

$$E(p) = \frac{\alpha}{\alpha + \beta} \tag{8}$$

Let r represents the number of positive behaviors of node j observed at node i i.e $B_{p_{i,j}}$, and s represents the number of negative behaviors of node j observed at node i i.e $B_{ni,j}$. The expected probability of the positive behavior of node j observed at node i can be computed by using Eq.(7) and Eq.(8) as follows:

$$E(p)_{i,j} = \frac{(B_{p_{i,j}} + 1)}{(B_{p_{i,j}} + 1) + (B_{ni,j} + 1)} \tag{9}$$

where $B_{p_{i,j}} \geq 0$, and $B_{ni,j} \geq 0$

The expected probability of positive behavior of a node also represents its reliability index. If a node's expected probability of positive behavior is higher, its reliability index is also higher and vice versa. During initial communications, a reliable node may experience congestion and may drop significant number of received packets exhibiting negative behavior. It is preferable to obtain at least m number of behavior evaluations of a node in order to predict its future behavior. The value of m should be selected in such a way that it gives a reasonable evidence about the packet forwarding behavior of a node. If a node performs packet forwarding misbehavior continuously due to some fault, the expected probability of its positive behavior decreases gradually. If a node performs packet forwarding misbehavior randomly due to congestion, the expected probability of its positive behavior varies accordingly.

Let $C_{i,j}$ represents the class of node j evaluated by node i. If node j is reliable, the value of $C_{i,j}$ will be 1 and 0 otherwise. Node i classifies node j based on the following criteria. If the number of behavior evaluations made by node i for node j is less than m, node i assumes node j as a reliable node. Node j is also said to be reliable if the total number of behavior evaluations made by node i for node j is greater than or equal to m, and the expected probability of the positive behavior of node j evaluated by node i i.e $E(p)_{i,j}$ is greater than or equal to positive behavior probability threshold Th_{prob}. If the value of

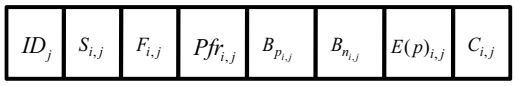

Figure 3. The structure of reliability database at node i

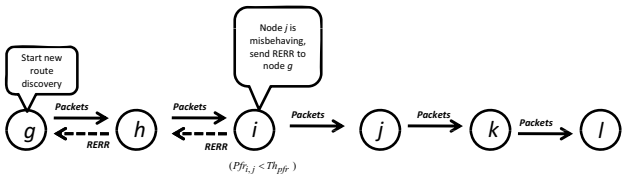

Figure 4. The route maintenance process

$E(p)_{i,j}$ is less than Th_{prob} after m behavior evaluations, node i assumes node j as unreliable as follows:

$$C_{i,j} = \begin{cases} 1 & B_{p_{i,j}} + B_{ni,j} < m \\ 1 & B_{p_{i,j}} + B_{ni,j} \geq m, E(p)_{i,j} \geq Th_{prob} \\ 0 & B_{p_{i,j}} + B_{ni,j} \geq m, E(p)_{i,j} < Th_{prob} \end{cases} \tag{10}$$

The value of Th_{prob} may be selected in such a way that the maximum number of reliable nodes may be used for routing packets. For example; a node having an equal probability of positive and negative behavior may be selected for routing packets. The Reliability Manager at node i stores the reliability information about neighbor j in reliability database as shown in figure 3.

B. Route Maintenance

In traditional AODV [26] routing protocol, the Route Maintenance is initiated when a link break occurs in an active route. In our proposed scheme, the Route Maintenance is also initiated when some node performs packet forwarding misbehavior in an active route. When an intermediate node along a given route identifies a link break or packet forwarding misbehavior, it generates a Route Error (RERR) message and sends it to the source node. All nodes including the source node and the reporting node invalidate the route to the destination and the source node initiates a new route setup process. The Route Maintenance process is described in figure 4. When the condition $Pfr_{i,j} < Th_{pfr}$ becomes true, the Reliability Manager at node i assumes node j as a misbehaving node and sends *RERR* message to source node g for finding a new reliable route. Node i, node h and node g delete the route to destination l from their routing tables and source node g starts a new route setup process as described in the following section.

C. Route Setup

The proposed scheme extends the route setup process of AODV [26] routing protocol to find the shortest possible route with all reliable nodes. The Route Setup uses node reliability and end-to-end delay as route selection metrics. The reliable nodes deliver the packets to destination with high probability. The shortest possible route

reduces power consumption in the network as fewer nodes participate in packet forwarding along a given route. We assume that the network topology does not change during the route setup process.

We assume a network where node e is the source and node k is the destination. When node e wants to send data to node k and it does not have route to the same, it starts route discovery by broadcasting Route Request (RREQ) message to its neighbors N_e. Node e specifies the packet rate per second A_r in the *RREQ* packet's *Reserved* field. The nodes in N_e compute the value of n as described earlier, make reverse route entry for node e and forward *RREQ* message to their neighbors. This process continues until the *RREQ* reaches at node k. Node k makes reverse route entry for node e and unicasts Route Reply (RREP) message to node e along the reverse route. If node k receives multiple *RREQ* messages from node e through different routes, it generates multiple *RREP* messages and unicasts them to node e along the reverse routes. This helps node e to select a route among available routes consisting of only reliable nodes, as a given route may have some broken nodes. Node j is said to be downstream neighbor of node i if node i sends *RREQ* message to node j. Similarly, node i is said to be upstream neighbor of node j if node i receives *RREP* message from node j.

The decision of route selection is made by the source and all intermediate nodes along a given route. When an intermediate node i receives *RREP* message from its downstream neighbor j and the downstream neighbor j is not the destination, node i checks for reliability information of node j from reliability database R_i. If node j is reliable, node i includes node j in route P_i, makes forward route entry for node k and forwards *RREP* message to its upstream node. If node j is unreliable, node i drops *RREP* message. This process continues until the *RREP* reaches at node e.

Let M represents the number of possible reliable routes between node e and node k with variable delay such that $P_1, P_2, P_3, ...P_M \in M$. Let $t_{i,j}$ represents the average transmission delay of link (i, j) on route P_i. If the length of route P_i is l hops, the average end-to-end delay of route P_i is computed as follows:

$$P_{id} = \sum_{i=1}^{l-1} t_{(i,j)_i} \tag{11}$$

The source node e selects the shortest possible route to destination node k from M available reliable routes as follows:

$$P_{e,k} = \min_{i=1}^{M} P_{id} \tag{12}$$

When the source node e selects the route, it makes forward route entry for destination node k and starts transmitting data over the established route.

Figure 5 shows the route setup process, where all network nodes are assumed to be reliable and one reliable route exists between source e and destination k. Figure 6

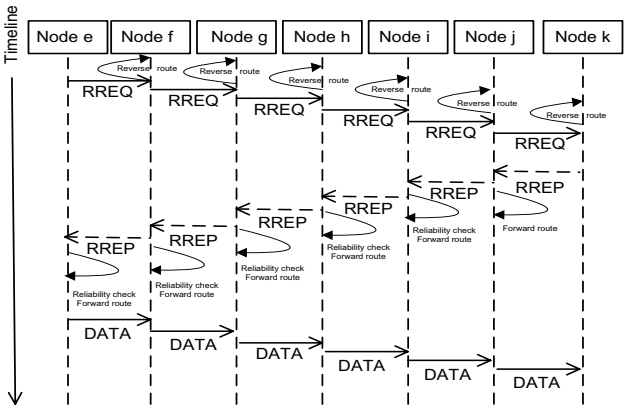

Figure 5. The route setup process in a network with all reliable nodes

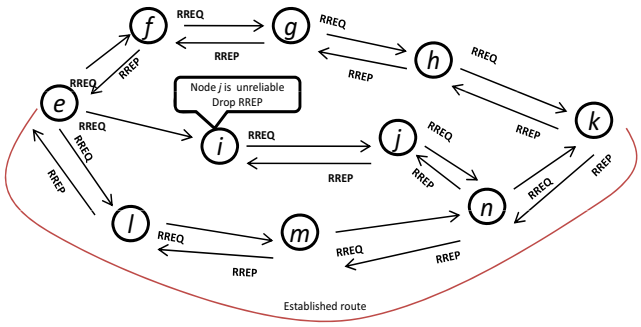

Figure 6. The route setup process in a network with some unreliable nodes

shows the route setup process in the presence of some unreliable nodes in the network and multiple reliable routes exist between source e and destination k. Node i drops *RREP* received from node j as node j is unreliable. Node e receives first *RREP* message from reliable neighbor l, makes forward route entry for node k and starts sending data over the route $e \rightarrow l \rightarrow m \rightarrow n \rightarrow k$. Node e ignores *RREP* message received afterwards from node f.

Consider a network with $k + 1$ nodes labeled as n_0, n_1, n_2,.. , n_k, with n_0 as the source and n_k as the destination. The current node is represented by n_i and R_i represents the reliability database at node n_i. The upstream neighbor of n_i is represented by n_{i-1} and the downstream neighbor of n_i is represented by n_{i+1}. Let N_i represents the neighborhood of node n_i such that $n_{i-1}, n_{i+1} \in N_i$. The $RREQ_b$ describes the broadcast of *RREQ* message and $RREP_u$ represents the unicast of *RREP* message. Moreover, $C_{i,i+1}$ and $C_{i,j}$ represent the same information. Algorithm 1 describes the route setup process.

IV. Simulation Scenario and Results

We simulate an emergency response scenario caused by an earthquake or a flood as shown in figure 1. The traditional telecommunication infrastructure is assumed to be totally collapsed and a mobile ad hoc network comprising of smart phones and PDAs has been established for exchanging emergency related information. The majority of first responders such as medical teams,

input : $C_{i,i+1}$
output: *Shortest route with all reliable nodes*
set $n_i = n_0$
if (n_i *has route to* n_k) **then**
  $n_i : Data \Rightarrow n_k$
end
else
  $n_i : RREQ_b \Rightarrow N_i$
  set $n_i = n_{i+1}$
end
repeat
  $n_i \Leftarrow RREQ : n_{i-1}$
  n_i computes $n = A_r \times \Delta_t$
  n_i makes reverse route entry for n_0
  $n_i : RREQ_b \Rightarrow N_i$
  set $n_i = n_{i+1}$
until ($n_i = n_k$ *AND* $n_i \Leftarrow RREQ : n_{i-1}$);
if ($n_i = n_k$ *AND* $n_i \Leftarrow RREQ : n_{i-1}$) **then**
  n_i makes reverse route entry for n_0
  $n_i : RREP_u \Rightarrow n_{i-1}$
  $n_{i-1} \Leftarrow RREP : n_i$
  n_{i-1} makes forward route entry for n_k
  $n_{i-1} : RREP_u \Rightarrow n_{i-2}$
  set $n_i = n_{i-2}$
end
repeat
  $n_i \Leftarrow RREP : n_{i+1}$
  $n_i \Leftarrow C_{i,i+1} : R_i$
  if ($C_{i,i+1} == 1$) **then**
    n_i makes forward route entry for n_k
    $n_i : RREP_u \Rightarrow n_{i-1}$
    set $n_i = n_{i-1}$
  end
  else if ($C_{i,i+1} == 0$) **then**
    $n_i : Drop \Leftarrow RREP : n_{i+1}$
  end
until ($n_i = n_0$ *AND* $n_i \Leftarrow RREP : n_{i+1}$);
if ($n_i = n_0$ *AND* $n_i \Leftarrow RREP : n_{i+1}$) **then**
  $n_i \Leftarrow C_{i,i+1} : R_i$
  if ($C_{i,i+1} == 1$) **then**
    n_i makes forward route entry for n_k
    $n_i : Data \Rightarrow n_k$
    n_i ignores pending $RREP$ messages
  end
  else if ($C_{i,i+1} == 0$) **then**
    $n_i : Drop \Leftarrow RREP : n_{i+1}$
  end
end

Algorithm 1: Route setup process

TABLE I.
SIMULATION PARAMETERS

Parameter	Value
Number of nodes	50
Coverage area	1000x1000 meters
Propagation model	Two ray ground
Mobility model	Random way point
MAC protocol	802.11
Routing protocol	AODV, $AODV_r$
Radio range	250 meters
Channel bandwidth	11Mbps
Traffic type	CBR
Packet size	512 bytes
Application's packet rate A_r	100 packets per second
Behavior evaluation time interval Δt	5 seconds
Node movement speed	0-10 meter per second
Interface queue size	100 packets
Positive behavior probability threshold Th_{prob}	0.5
Minimum number of behavior evaluations m	10
Packet forwarding threshold Th_{pfr}	0.2-0.8
Simulations time	1000 seconds

NGO teams and fire fighters are engaged in saving the life of trapped survivors at the disaster site. Some first responders use ambulance services to transfer the victims to remote hospitals. The mobile nodes choose random destinations and move towards those destinations with different movement speeds. The mobile nodes stay at a particular place for random period of time and then move to next destinations. We simulate the faulty node behavior as a node which drops alternate received packets. We assume that on average, there are three to five simultaneous communications in the network at a time and we name it as an average traffic load. The simulations are run by using NS2 [29] simulator. The performance of the proposed scheme is evaluated against the traditional AODV scheme in terms of packet delivery ratio, end-to-end delay and routing overhead. For convenience, we name our proposed scheme as reliable AODV and represent it by $AODV_r$. The simulation parameters are summarized in table I.

Figure 7, figure 8 and figure 9 show the packet delivery, end-to-end delay and routing overhead performance of the proposed scheme in a network having some broken nodes with an average network traffic and random node mobility speed. When all network nodes are reliable, the packet delivery ratio of AODV and $AODV_r$ is almost similar. The proposed scheme identifies and isolates faulty nodes dynamically, so its packet delivery ratio increases with the increasing number of faulty nodes against the traditional scheme. The end-to-end delay performance of the proposed scheme is also better as it switches to new routes while experiencing random congestion. The proposed scheme finds additional routes to avoid faulty or congested nodes, so its routing overhead increases against the AODV routing scheme. The overall performance of

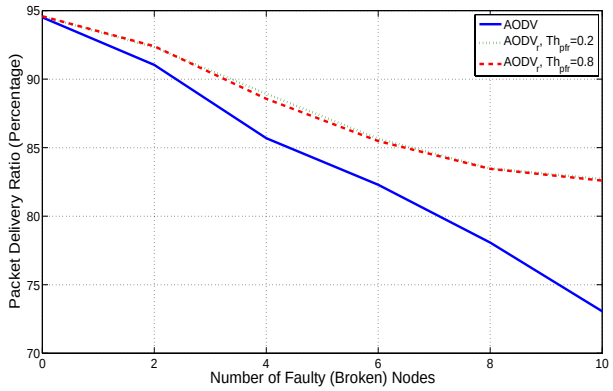

Figure 7. Packet delivery performance in a network having some broken nodes with an average network traffic and random node mobility speed

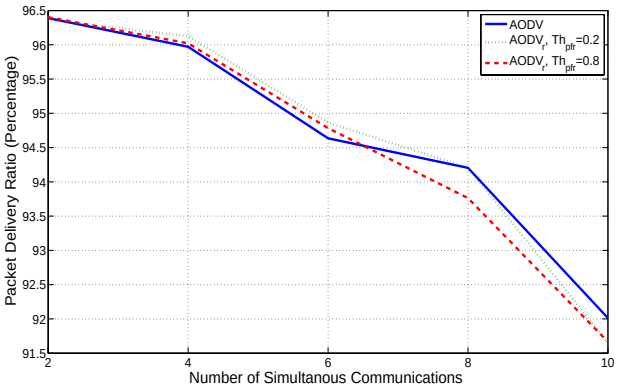

Figure 10. Packet delivery performance in a network having all reliable nodes with variable network traffic and random node mobility speed

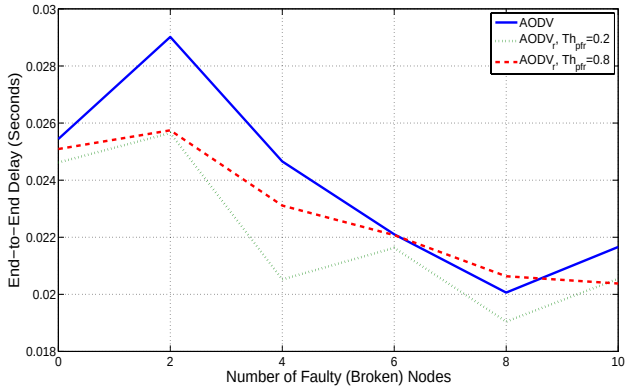

Figure 8. Delay performance in a network having some broken nodes with an average network traffic and random node mobility speed

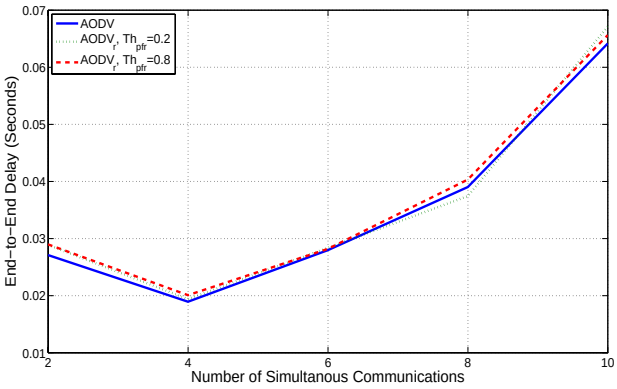

Figure 11. Delay performance in a network having all reliable nodes with variable network traffic and random node mobility speed

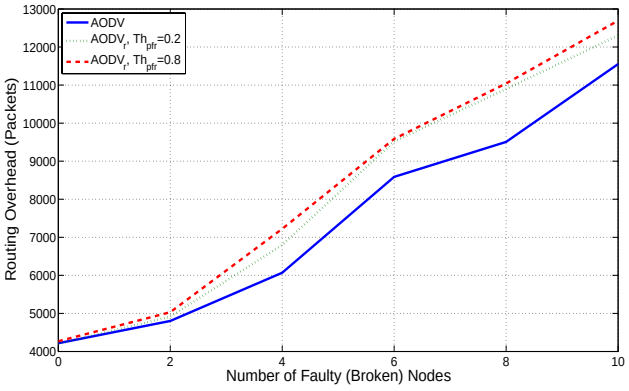

Figure 9. Routing overhead performance in a network having some broken nodes with an average network traffic and random node mobility speed

the proposed scheme improves at lower value of packet forwarding threshold, as the frequency of route maintenance calls decreases.

Figure 10, figure 11 and figure 12 show the packet delivery, end-to-end delay and routing overhead performance of the proposed scheme in a network having all reliable nodes with variable network traffic and random node mobility speed. At low traffic load, the packet delivery ratio of AODV and $AODV_r$ is almost similar as there is no significant congestion. As the network traffic increases and there is some random congestion, the packet delivery ratio of $AODV_r$ improves. When the network traffic increases significantly, the level of congestion also increases and the packet delivery ratio of $AODV_r$ degrades due to increasing number of route maintenance calls. The end-to-end delay of the proposed scheme remains almost similar to that of AODV for variable network traffic. The routing overhead of $AODV_r$ increases as the frequency of route maintenance calls increases to avoid significant network congestion.

Figure 13, figure 14 and figure 15 show the packet delivery, end-to-end delay and routing overhead performance of the proposed scheme in a network having all reliable nodes with an average network traffic and variable node mobility speed. The packet delivery ratio, end-to-end delay and routing overhead performance of AODV and $AODV_r$ is almost similar for lower packet forwarding threshold value. However, there is some overlapping in the packet delivery and end-to-end delay performance of AODV and $AODV_r$ if the value of packet forwarding threshold increases. The routing overhead of $AODV_r$ increases than AODV as the node mobility speed and the value of packet forwarding threshold increases.

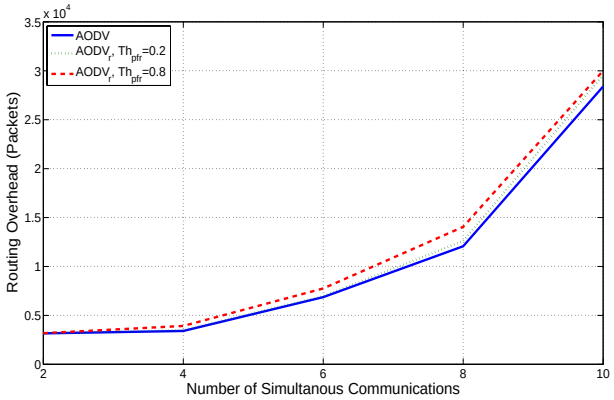

Figure 12. Routing overhead performance in a network having all reliable nodes with variable network traffic and random node mobility speed

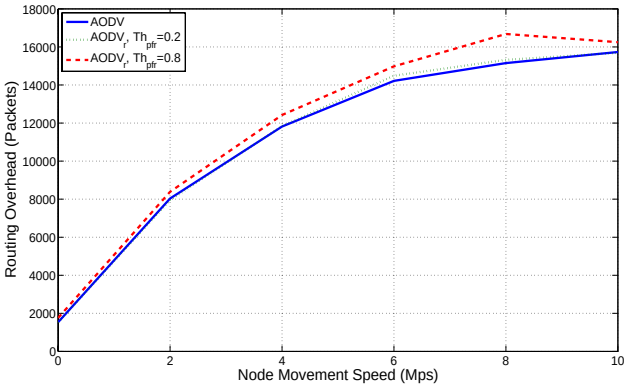

Figure 15. Routing overhead performance in a network having all reliable nodes with an average network traffic and variable node mobility speed

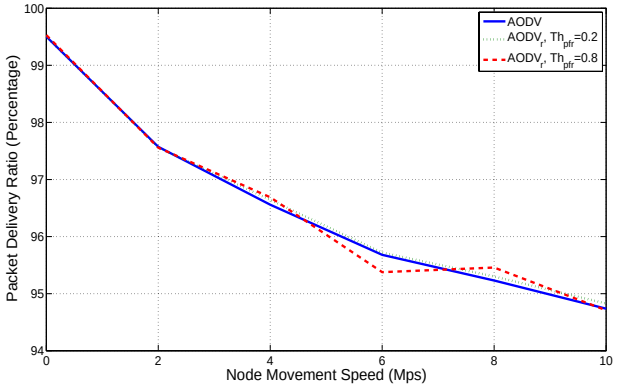

Figure 13. Packet delivery performance in a network having all reliable nodes with an average network traffic and variable node mobility speed

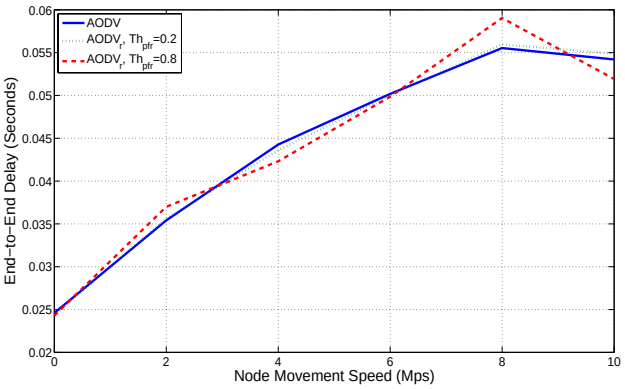

Figure 14. Delay performance in a network having all reliable nodes with an average network traffic and variable node mobility speed

V. Conclusion and Future Work

We propose a reliable routing scheme for post-disaster ad hoc communication networks, which finds the shortest possible routes with all reliable nodes. The proposed scheme also detects packet forwarding misbehavior dynamically and reroutes packets through other reliable routes. The performance of the proposed scheme is compared against the traditional scheme in terms of packet delivery ratio, end-to-end delay and routing overhead. The proposed scheme performs better in terms of packet delivery ratio and end-to-end delay with a reasonable increase in routing overhead, when the network contains some broken nodes, there is an average network traffic and the nodes move with random mobility speed. If the network contains all reliable nodes, there is variable network traffic and the nodes move with random mobility speed, the packet delivery ratio, end-to-end delay and routing overhead of the traditional and the proposed schemes almost match. The packet delivery ratio, end-to-end delay and routing overhead performance of the proposed scheme is almost similar to that of the traditional scheme, when the network contains all reliable nodes, there is an average network traffic, the nodes move with variable mobility speeds and the value of packet forwarding threshold decreases. However, the packet delivery and end-to-end delay performance of the traditional and the proposed schemes overlap with a little increase in routing overhead, if the value of packet forwarding threshold increases. We are in the process of extending the proposed scheme to address malicious node behavior in addition to network fault and congestion.

References

[1] E. Der Heide and R. Irwin, *Disaster response: principles of preparation and coordination*. Mosby, 1989.

[2] M. Kyng, E. Nielsen, and M. Kristensen, "Challenges in designing interactive systems for emergency response," in *Proceedings of the 6th conference on Designing Interactive systems*, 2006, pp. 301–310.

[3] H. Kirchner and T. Risse, "Challenges in information systems for disaster recovery and response," *3. GI/ITG KuVS Fachgespräch Ortsbezogene Anwendungen und Dienste*, pp. 16–19.

[4] B. Manoj and A. Baker, "Communication challenges in emergency response," *Communications of the ACM*, vol. 50, no. 3, pp. 51–53, 2007.

[5] A. Meissner, T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner, "Design challenges for an integrated disaster management communication and information system," in *The First IEEE Workshop on Disaster Recovery Networks (DIREN 2002)*, 2002.

[6] S. Mehrotra, T. Znati, and C. Thompson, "Crisis management," *Internet Computing, IEEE*, vol. 12, no. 1, pp. 14–17, 2008.
[7] T. Lueck, "Grant to help city broaden radio network," *New York Times*, 2005.
[8] C. Thompson, "Talking in the dark," *New York Times Magazine*, 2005.
[9] M. Portmann and A. Pirzada, "Wireless mesh networks for public safety and crisis management applications," *IEEE Internet Computing*, pp. 18–25, 2008.
[10] J. Hubaux, T. Gross, J. Le Boudec, and M. Vetterli, "Toward self-organized mobile ad hoc networks: The terminodes project," *Communications Magazine, IEEE*, vol. 39, no. 1, pp. 118–124, 2001.
[11] M. Ad, C. Perkins, and S. Das, "Ip address autoconfiguration for ad hoc networks," Internet Draft draftietfmanetautoconf-01. txt, Internet Engineering Task Force, MANET WG, Tech. Rep., 2000.
[12] A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.
[13] S. Rahebi and M. Asadi, "Wbrr: A weight based reliable routing method in mobile ad hoc network," *Australian Journal of Basic and Applied Sciences*, vol. 3, no. 3, pp. 1888–1897, 2009.
[14] F. Xie, L. Du, Y. Bai, and L. Chen, "Energy aware reliable routing protocol for mobile ad hoc networks," in *Wireless Communications and Networking Conference, 2007. WCNC 2007.*, 2007, pp. 4313–4317.
[15] A. Bamis, A. Boukerche, I. Chatzigiannakis, and S. Nikoletseas, "A mobility aware protocol synthesis for efficient routing in ad hoc mobile networks," *Computer Networks*, vol. 52, no. 1, pp. 130–154, 2008.
[16] Z. Cheng and W. Heinzelman, "Discovering long lifetime routes in mobile ad hoc networks," *Ad Hoc Networks*, vol. 6, no. 5, pp. 661–674, 2008.
[17] I. Jawhar, Z. Trabelsi, and J. Al-Jaroodi, "Towards more reliable source routing in wireless networks," in *International Conference on Networking, Architecture, and Storage, 2008. NAS'08*, 2008, pp. 167–168.
[18] V. Rishiwal, A. Kush, and S. Verma, "Stable and energy efficient routing for mobile adhoc networks," in *Fifth International Conference on Information Technology: New Generations*, 2008, pp. 1028–1033.
[19] B. Ramachandran and S. Shanmugavel, "Received signal strength-based cross-layer designs for mobile ad hoc networks," *IETE technical review*, vol. 25, no. 4, pp. 192–200, 2008.
[20] C. Hieu and C. Hong, "A reliable and high throughput multi-rate ad hoc routing protocol: Cross layer approach," in *International Conference on Information and Communication Technology Convergence (ICTC)*, 2010, pp. 362–367.
[21] J. Muñoz, O. Esparza, M. Aguilar, V. Carrascal, and J. Forné, "Rdsr-v. reliable dynamic source routing for video-streaming over mobile ad hoc networks," *Computer Networks*, vol. 54, no. 1, pp. 79–96, 2010.
[22] A. Gohari, R. Pakbaz, and V. Rodoplu, "Rmr: Reliability based multi-hop routing in wireless tactical networks," in *Proceedings of IEEE Military Communications Conference*, 2010, pp. 1106–1112.
[23] S. Hariharan, N. Shroff, and S. Bagchi, "Secure neighbor discovery through overhearing in static multihop wireless networks," in *Fifth IEEE Workshop on Wireless Mesh Networks (WIMESH 2010)*, 2010, pp. 1–6.
[24] H. Ning, C. Ling, and K. Leung, "Wireless network coding with imperfect overhearing," *Arxiv preprint arXiv:1003.4270*, 2010.
[25] Y. Reddy and R. Selmic, "Trust-based packet transfer in wireless sensor networks," in *Proceedings of the Tenth International Conference on Networks*, 2011, pp. 218–223.
[26] M. Ad, E. Royer, C. Perkins, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," 1999.
[27] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 255–265.
[28] A. Jsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th Bled Electronic Commerce Conference*, 2002, pp. 41–55.
[29] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2*. Springer Verlag, 2008.

Muhammad Ibrahim Channa was born in Pakistan. He completed M.Sc. in Computer Science from University of Sind, Pakistan, in 1995 and M.S. in Information Technology from National University of Science and Technology, Pakistan in 2005. He is enrolled as a PhD candidate at Asian Institute of Technology, Thailand since August 2007. His field of study is Information and Communications Technologies.

He is employed as Assistant Professor, Institute of Information Technology, Quaid-e-Awam University of Engineering, Science and Technology, Pakistan since March 2000. His research interest comprises of trust management, security, routing, and quality of service in mobile ad hoc networks.

Dr. Kazi M. Ahmed was born in Bangladesh. He did his Masters in Telecommunications Engineering from the then Leningrad Electrical Engineering Institute of Communications, former USSR, in 1978. He finished his Ph.D. in Electrical Engineering from the University of Newcastle, NSW, Australia in 1983.

At present, he is a Professor of Telecommunications and ICT at Asian Institute of Technology, Bangkok, Thailand. Dr. Ahmed has diverse interest in different fields of Telecommunications. His main research interest is in Wireless Communications and Communications Networks.

Dr. Ahmed is a Member, IEEE; Member, IEICE, Japan; Fellow of IE Bangladesh; and Member and Advisor of many international and national associations and steering committees.