Sindh Univ. Res. Jour. (Sci. Ser.) Vol.43 (1-A) 9-16 (2011)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

A Dynamic Trust Management Framework for Emergency Ad Hoc Networks

M. I. Channa , A. H. Jalbani and S. Baseer

School of Engineering and Technology, Asian Institute of Technology, Thailand
e-mail:akhtar.hussain@ait.ac.th samad.baseer@ait.ac.th

*Corresponding author: M. I. Channa email: muhammad.ibrahim.channa@ait.ac.th

Received 12 th May 2011 Revised 13th June 2011

Abstract: Reliable and robust communication among emergency management teams is vital for successful emergency response efforts. During emergency situations, it is possible that the traditional communication infrastructure may be damaged and may not provide adequate communication services to first responders. Mobile ad hoc networks are commonly used in such type of situations. The emergency ad hoc network comprises of heterogeneous devices owned by different rescue workers belonging to different rescue organizations. The flow of real-time voice and video data over emergency ad hoc network may create network congestion. The network nodes may experience some fault or perform malicious behavior resulting into significant loss of emergency related information. The reception of incomplete information may result into more loss of life and other community resources. We propose a dynamic trust management scheme for emergency ad hoc networks which identifies faulty, congested, and malicious nodes. These nodes are isolated from the established routes to provide reliable and robust communications among first responders. The simulation results show that the network throughput is increased significantly against a little increase in delay.

Keywords: Emergency ad hoc network; trust management; faulty node; congested node; malicious node.

INTRODUCTION

It is a great challenge for public emergency services to face the disaster situations arising due to natural or man-made disasters. It is necessary to provide relevant information to concerned rescue persons in a timely manner for coping with such disasters in an effective and coordinated manner (Auf *et al.*, 1989), (Kyng *et al*., 2006), (Risse *et al.*, 2006), (Manoj *et al.*, 2007). The successful coordination requires current information in real time, so the deployment of an integrated information and communication system is vital for efficient, reliable and secure exchange of information (Meissner *et al*., 2002). A large scale emergency response operation involves multi-organizational teams including government authorities, public authorities, volunteer organizations and the media and work together to save lives, and other community resources (Mehrotra *et al*., 2008).

The telecommunication services are 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 (Lueck 2005), (Thompson 2005), the existing communication infrastructure was badly damaged and the remaining parts of the network were not able to provide adequate communication services to first responders (Portman *et al.*, 2008). The networks are preferred as they don't require any existing telecommunication infrastructure and are self-configured.

Reliable and robust communication is vital for successful emergency response operations (Portman *et al.*, 2008). During emergency situations, the deployed ad hoc communication network may experience failure or malicious threats (Mehrotra *et al*., 2008). A *faulty* node may experience some software or hardware problem and drop a fraction of received packets. A *malicious* node may attract all packets and drop them to create communication interruptions among emergency management teams. The flow of real-time voice and video data over emergency ad hoc network may create *congestion* and may result into delay and packet loss. The extensive loss of packets holding emergency related information may result into mismanagement of emergency response efforts. We propose a dynamic trust management scheme for emergency ad hoc networks, which identifies such type of misbehaving nodes and isolates them from the established routes.

The organization of the paper is as follows. Section II describes some related work. Section III presents an overview of the proposed dynamic trust management scheme. Section IV describes the system components. The simulation results are presented in section V and section VI concludes the paper.

MATERIAL AND METHODS

Related work

The Watchdog and Pathrater (Marti *et al*., 2000) scheme has been proposed to identify misbehaving nodes and select a path which delivers the packets with high probability. The path rating is

computed by averaging the rating of the nodes along the given path. The CONFIDANT (*et al.,* 2002) has been proposed to enforce cooperation among network nodes. It maintains a black-list of misbehaving nodes and uses alarms to warn other fair nodes. It performs route re-ranking, route deletion and route request rejection from a misbehaving node. It also alerts the source about the presence of misbehaving nodes in the route. The CORE (Michiardi *et al.,* 2002) has been proposed which provides more complex reputation mechanism as compared with CONFIDANT. It measures the overall reputation of a node by combining its subjective, indirect and functional reputation. The reputation information is stored in a reputation table at each node. It uses a request/response mechanism to identify the behavior of neighbor nodes. An agent-based trust evaluation framework (Pirzada *et al.,* 2004) has been proposed to categorize nodes based on the relevant information. The trust of a node is computed by performing trust derivation, quantification and computation. The aggregate trust of a node is computed by combining trust categories along with their weights. A cluster-based trust evaluation scheme (Jin, *et al*., 2005) has been proposed which evaluates the trust of a node based on own experience and recommendations by the cluster head. The cluster head authenticates a node through trust value certificate which is used by member nodes to show their trustworthiness to other network nodes.

Proposed dynamic trust management scheme

The proposed dynamic trust management scheme works on top of Ad Hoc On Demand Distance Vector (AODV) (Perkins C.E. *et al*., 2003) routing protocol. Traditionally, the AODV routing protocol uses hop-count as a route selection metric. The proposed scheme enables AODV to find the shortest possible route containing only trustworthy nodes. The proposed scheme comprises of two major components namely Trust Manager and Route Manager. The *Trust Manager* comprises of the Monitor and Trust Evaluator and is responsible for evaluating and managing trust of neighbor nodes. The *Route Manager* comprises of the Route Setup and Route Maintenance and is used for establishing and maintaining reliable routes based on the information maintained by the Trust Manager. **(Fig. 1)** describes the proposed dynamic trust management model.

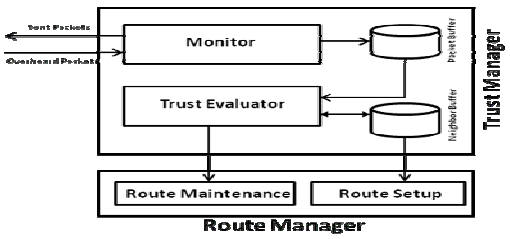


Fig. 1: Dynamic trust management model

The *Monitor* at a node observes the packet forwarding behavior of its neighbor nodes and the *Trust Evaluator* at a node uses this information to evaluate the trust of its neighbor nodes. The *Route Setup* establishes a route comprising of only trustworthy nodes. If some misbehaving node is detected in an established route, the *Route Maintenance* is used to inform the source node to establish a new reliable route. We use the term trust and reliability interchangeably. The proposed system works as follows. When a node sends or overhears a packet from its neighbor node, the Monitor stores and maintains the packet information. After certain number of sent packets (Packet interval), the Trust Evaluator evaluates the packet forwarding behavior of the neighbor node and ranks it accordingly. If some unreliable node is detected in an established route, the Trust Evaluator intimates the source to find a new reliable route through Route Maintenance. During Route Setup, the source node initiates route discovery by broadcasting Route Request (RREQ) messages. The intermediate nodes receive RREQ messages and broadcast the same to their neighbors. When the RREQ reaches at the destination, it generates a Route Reply (RREP) message. When a node receives RREP message from its neighbor, it checks for the reliability information of the neighbor. If the neighbor is reliable, the RREP message is forwarded towards the source node; otherwise the RRREP message is dropped. This process continues until the source node receives first RREP message from its trustworthy neighbor node. This indicates the establishment of a trustworthy route and the data packets are transferred along the established route.

Components of the proposed scheme

It has been mentioned in section III that the proposed dynamic trust management scheme comprises of various components. This section presents a brief description of those components.

A. MONITOR

The Monitor stores the packet forwarding behavior information of neighbor nodes in the packet buffer by observing their packet forwarding behavior. **(Fig. 2)** shows the structure of the packet buffer. The $P_{id_{i,j}}$ represents the packet ID which has been sent by node *i* to node *j*, $P_{src_{i,j}}$ represents the source address of the sent packet, $P_{dst_{i,j}}$ represents the destination address of the sent packet, ID_j represents the ID of node *j*, $T_{i,j}$ denotes the packet sending time from node *i* to node *j* and $T_{j,i}$ represents the packet overhearing time at node *i* from node *j*.

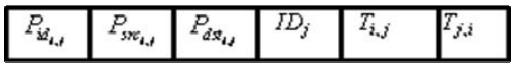


Fig. 2: Structure of packet buffer

When a packet *P* is sent by node *i* to node *j*, the Monitor at node *i* stores the packet ID into $P_{id_{i,j}}$, source address into $P_{src_{i,j}}$, destination address into $P_{dst_{i,j}}$, receiver ID into ID_j, and the packet sending time into $T_{i,j}$. When node *i* overhears a packet *P'* in promiscuous mode (Marti S. *et al.*, 2000) from its one-hop neighborhood *N*, where $j \in N$, it compares the ID, source address and destination address of the overheard packet *P'* with associated entries in packet buffer. If there is a match, the Monitor at node *i* stores the packet overhearing time into $T_{j,i}$ and ignores the overheard packet *P'*. If there is no match, the Monitor at node *i* simply ignores the overheard packet *P'*. The following algorithm describes the working principle of the Monitor at node *i*.

```
if (P → j) then
  store P_id_{i,j}, P_src_{i,j}, P_dst_{i,j}, ID_j, T_{i,j}
elseif (P' → i) then
  if (P'_id_{j,i} == P_id_{i,j}) then
    if (P'_src_{j,i} == P_src_{i,j}) then
      if (P'_dst_{j,i} == P_dst_{i,j}) then
        set T_{j,i} = current time
      end
    end
  end
  ignore overheard packet P'
end
```

B. TRUST EVALUATOR

The Trust Evaluator is responsible for evaluating the trust of neighbor nodes depending upon the information provided by the Monitor. The Trust Evaluator stores the trust information about neighbor nodes in a neighbor buffer as shown in **(Fig .3).**

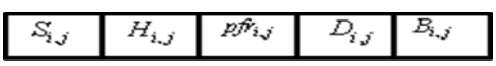


Fig. 3: Structure of neighbor buffer

The $S_{i,j}$ represents the number of packets sent by node *i* to node *j*, $H_{i,j}$ represents the number of packets overheard at node *i* from neighbor *j*, $pfr_{i,j}$ denotes the packet forwarding ratio of node *j* observed by node *i*, $D_{i,j}$ represents the average round-trip delay of packets sent from node *i* to neighbor node *j* and $B_{i,j}$ represents the behavior of node *j* observed at node *i*. When the number of packets sent by node *i* to neighbor node *j* reaches packet interval *n*, it computes the values of $S_{i,j}$, $H_{i,j}$, $pfr_{i,j}$, and $D_{i,j}$. The value of *n* should be neither small nor large, but it should be selected in such a way that it can help in identifying the true behavior of the neighbor node. The value of $pfr_{i,j}$ is computed as below:

$$pfr_{i,j} = H_{i,j} / S_{i,j} \qquad (1)$$

The value of $D_{i,j}$ is computed by taking the average of the round-trip delay of the overheard packets at node *i* from node *j* after sending *n* packets as follows.

$$D_{i,j} = \overline{(T_{j,i} - T_{i,j})} \qquad (2)$$

The Trust Evaluator at node *i* can determine the value of round-trip delay threshold Th_d after exchanging some packets with its one-hop neighborhood *N*, where $j \in N$, during initial communications similarly as shown in Eq. (2). Once these values are computed, the behavior of node *j* observed by node *i*, $B_{i,j}$ can be computed as follows. If the value of $pfr_{i,j}$ is zero, an alarm for node *j*, $M_{i,j}$ is incremented by one and the route maintenance is initiated. The values of $S_{i,j}$ and $H_{i,j}$ are reset to zero. If the value of $M_{i,j}$ reaches five, node *j* is assumed to be malicious. If the value of $pfr_{i,j}$ lies between zero and packet forwarding threshold, Th_{pfr}, and the average round-trip delay is less than or equal to the round-trip delay threshold, an alarm for node *j*, $F_{i,j}$ is incremented by one and the route maintenance is initiated. The values of $S_{i,j}$ and $H_{i,j}$ are reset to zero. If the value of $F_{i,j}$ reaches five, node *j* is assumed to be faulty. If the value of $pfr_{i,j}$ lies between zero and packet forwarding threshold, and the average round-trip delay is greater than the round-trip delay threshold, node *j* is assumed to be congested and the route

maintenance is initiated. The values of $S_{i,j}$ and $H_{i,j}$ are reset to zero. If the value of $pfr_{i,j}$ is greater than or equal to the packet forwarding threshold, and the average round-trip delay is less than or equal to the round-trip delay threshold, node *j* is assumed to be reliable. The values of $S_{i,j}$ and $H_{i,j}$ are reset to zero. The following algorithm describes the working principles of the Trust Evaluator.

C. ROUTE MAINTENANCE

When the Trust Evaluator identifies its neighbor as faulty, malicious or congested, it initiates Route Maintenance to inform the source node for the establishment of a new reliable route. The route maintenance is initiated by sending a Route Error (RERR) message to the source node as shown in **(Fig. 4)**. For example; when node *i* detects that node *j* is malicious, it sends RERR message to node *g* to establish a new reliable route. Node *h* deletes the route to node *l* from its routing table and node *g* starts a new route discovery.

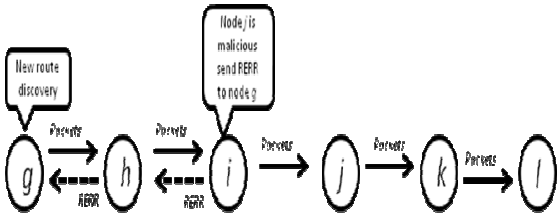


Fig. 4: Route maintenance

D. ROUTE SETUP

The source node initiates route setup by broadcasting Route Request (RREQ) message to its neighbors. The intermediate nodes forward the RREQ message to their neighbors and the RREQ message reaches at the destination. The destination unicasts the Route Reply (RREP) message to the source along the reverse route. An intermediate node receives RREP message from its downstream neighbor and checks for the trust information of the neighbor from its neighbor buffer. If the trust information of the neighbor is not found, it indicates that there has not been any previous interaction between the current node and its neighbor, and the RREP message is forwarded to the upstream neighbor of the current node. If the downstream neighbor is a faulty or malicious node, the RREP message is discarded by the current node. If the downstream neighbor is a reliable node, the RREP message is forwarded to the upstream neighbor of the current node.

If the downstream neighbor was detected congested during the last interaction, the RREP message may be forwarded to the upstream of the current node on the hope that the downstream node might have become uncontested. When the source node receives first RREP message from its downstream neighbor, it establishes a reliable route to the destination. Once the reliable route is

```
if (S_{i,j} == n) then
    compute H_{i,j}
    compute pfr_{i,j} = H_{i,j} / S_{i,j}
    compute D_{i,j} = (T_{j,i} − T_{i,j})
    if (pfr_{i,j} == 0) then
        set M_{i,j} = M_{i,j} + 1
        initiate routemaintenance
        set S_{i,j} = 0, H_{i,j} = 0
        if (M_{i,j} == 5) then
            set B_{i,j} = malicious
        end
    end
    if (pfr_{i,j} > 0) then
        if (pfr_{i,j} < Th_{pfr}) then
            if (D_{i,j} ≤ Th_d) then
                set F_{i,j} = F_{i,j} + 1
                initiate route maintenance
                set S_{i,j} = 0, H_{i,j} = 0
                if (F_{i,j} == 5) then
                    set B_{i,j} = faulty
                end
            end
        end
    end
    if (pfr_{i,j} > 0) then
        if (pfr_{i,j} < Th_{pfr}) then
            if (D_{i,j} > Th_d) then
                initiate route maintenance
                set S_{i,j} = 0, H_{i,j} = 0
                set B_{i,j} = congested
            end
        end
    end
    if (pfr_{i,j} ≥ Th_{pfr}) then
        if (D_{i,j} ≤ Th_d) then
            set B_{i,j} = reliable
            set S_{i,j} = 0, H_{i,j} = 0
        end
    end
end
```

established, data communications take place. The route setup process is represented in **(Fig. 5)** as follows.

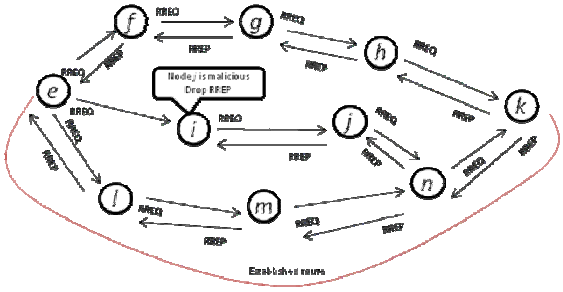


Fig. 5: Route setup process

The source node *e* broadcasts RREQ message for finding a route to destination node *k*. The intermediate nodes *f, i* and *l* receive the RREQ message and broadcast the same to their neighbors. When destination node *k* receives RREQ messages, it generates RREP message and unicasts it to the source node *e* along the reverse routes. Node *h, j* and *n* receive RREP message and forward to their upstream neighbors as node *k* is assumed to be reliable. It is assumed that during previous interactions, node *j* was detected as malicious at node *i*. When node *i* receives RREP message from node *j*, it finds that node *j* is malicious and drops the RREP message. If node *e* receives the first RREP message from node *l*, the route $e \to l \to m \to n \to k$ is established. The RREP message received from node *f* is simply ignored. The flowchart in **(Fig. 6)** describes the route setup process.

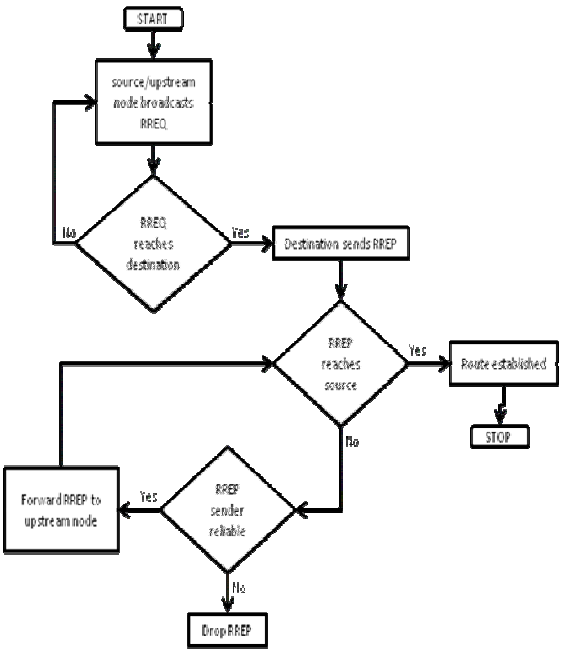


Fig. 6: Route setup flowchart

RESULTS AND DISCUSSION

Simulation Results

We simulate the proposed scheme and evaluate its performance in terms of average network throughput and average end-to-end delay. The simulations are carried out in the presence of faulty, congested and malicious nodes. For convenience, we label all fair nodes using AODV routing protocol as AODV, a mix of faulty and fair nodes using AODV as FAODV, a mix of malicious and fair nodes using AODV as MAODV and a mix of fair nodes and congested nodes using AODV as CAODV. We name our scheme as Trusted AODV (TrAODV) for all scenarios. The simulation parameters are summarized in **(Table I)** as follows.

Table 1. simulations parameters

Number of nodes	50
Coverage area	1000 x 1000 meters
Propagation model	Two ray ground
Mobility model	Random way point
MAC protocol	802.11
Routing protocol	AODV & TrAODV
Packet type	CBR
Packet size	512 Bytes
Interface queue size	100 packets
Packet interval *n*	100 packets
Packet forwarding threshold	0.7
No. of misbehaving nodes	5
Node movement speeds	1,2,3 meter / second
Simulations time	10000 seconds

(Fig. 7 and 8) show the performance of the proposed scheme in terms of throughput and delay in the presence of faulty nodes.

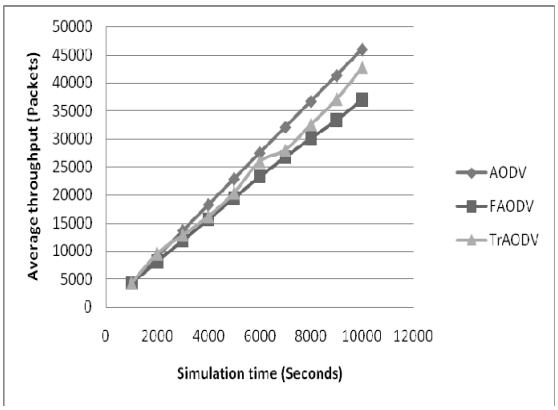


Fig. 7: Throughput performance against faulty nodes

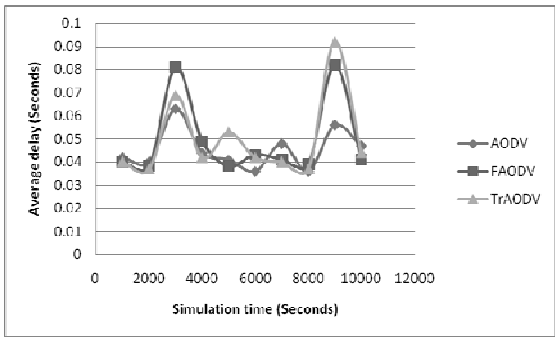


Fig. 8: Delay performance against faulty nodes

The performance of the proposed scheme in terms of throughput and delay against malicious nodes is shown in **(Fig. 9 and Fig. 10)** respectively.

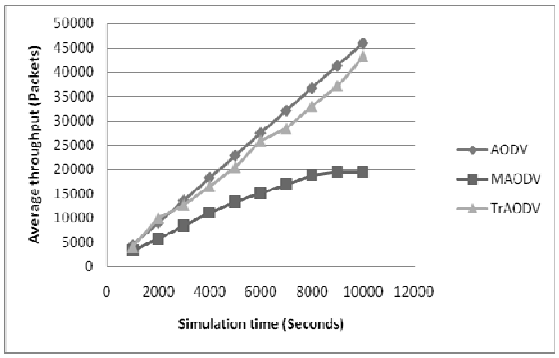


Fig. 9: Throughput performance against malicious nodes

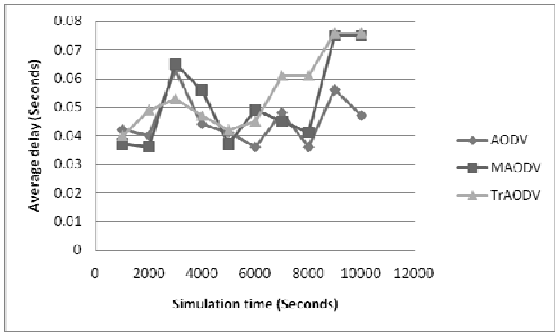


Fig. 10: Delay performance against malicious nodes

(Fig. 11 and 12) represents the performance evaluation of the proposed scheme in terms of throughput and delay in the presence of network congestion.

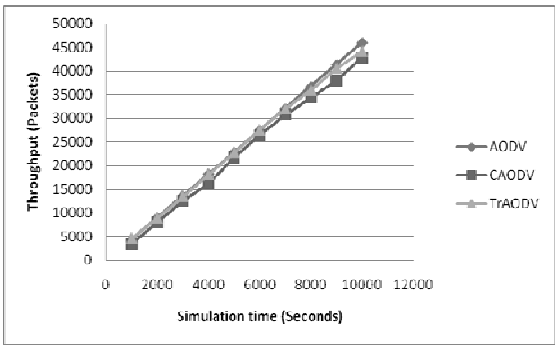


Fig. 11: Throughput performance against congestion

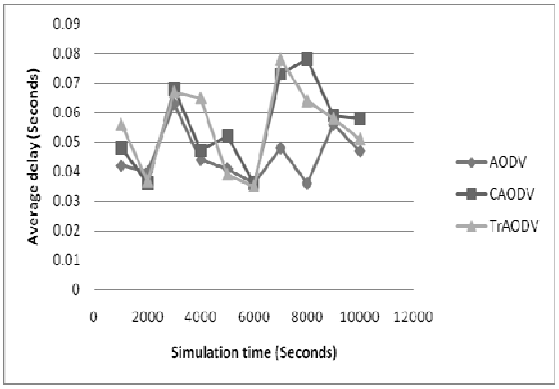


Fig. 12: Delay performance against congestion

CONCLUSION

We propose a dynamic trust management scheme for emergency ad hoc networks which keeps track of faulty, congested and malicious nodes and isolates these nodes from the established routes. The simulation results show that the throughput performance is improved in the presence of faulty, malicious and congested nodes against a little increase in delay. The proposed scheme only uses direct observations to identify misbehaving nodes. It is required to extend this scheme to obtain the trust information about a node through direct observations and recommendations from other trustworthy nodes.

ACKNOWLEDGEMENT

This work is a modified version of the paper presented at ICCET 2011 conference organized by Department of Computer Science, Shah Abdul Latif University, Khairpur, Sind, Pakistan.

REFERENCES

Auf der Heide E., (1989) Disaster Response: Principles of Preparation and Coordination, Online Book: http://coe-dmha.org/dr.

Buchegger S., and J. Boudec (2002) "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes-Fairness in Distributed Ad Hoc Networks", Proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing, 226-236.

Hubaux J., T. Gross J. Boudec and M. Vetterli (2001) "Towards Self Organized Mobile Ad Hoc Networks: the Terminodes Project", IEEE Communications Magazine 2001, Vol. (**39**): Issue 1: 118-124.

Jin S., C. Park D. Choi K. Chung and H. Yoon (2005) "Cluster-Based Trust Evaluation Scheme in Ad Hoc Networks", ETRI Journal, Vol. (**27**): No 4, 465-468.

Kyng M., E. Nielsen and M. Kristensen "Challenges (2005) in Designing Interactive Systems for Emergency Response", Proceedings of the 6th Conference on Designing Interactive Systems, 301-310.

Lueck T., (2007) "Grant to Help City Broaden Radio Network", New York Times, September 19, Manoj B., and Baker A., "Communication Challenges in Emergency Response", Communications of the ACM, Vol. (**50**): Iusse 3, 51-53.

Marti S., T. Giuli and M. Baker (2000) "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, 255-265.

Mehrotra S., T. Znati and C. Thompson (2008) "Crisis Management", IEEE Internet Computing Vol.(**12**): Issue 1: 14-17.

Meissner A., T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner, (2002) "Design Challenges of an Integrated Disaster Management Communication and Information System", The First IEEE Workshop on Disaster Recovery Networks (DIREN 2002).

Michiardi P. and R. Molva (2002) "CORE: A Collaborative Reputation Mechanism to Enfor Node Cooperation in Mobile Ad Hoc Networks", Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communication and Multimedia Security, 107-121.

Perkins C.E, E.M.Belding-Royer and I. Chakeres, (2003) "Ad Hoc On-Demand Distance Vector (AODV) Routing", IETF Internet Draft.

Pirzada A., and C. McDonald (2004) "Establishing Trust in Pure Ad Hoc Networks", Prceedings of the 27th ustralian Conference on Computer Science, 47-54.

Portman M. and A. Pirzada (2008) "Wireless Mesh Networks for Public Safety and Crisis Management Applications", IEEE Internet Computing Vol. (**12**): Issue 1: 18-25.

Risse T. and H. Kirchner, (2006) "Challenges in Information Systems for Disaster Recovery and Response", Proceedings of the 3rd GI/ITG KuVS Fachges Prah, Berlin 16-19.

Thompson C., (2005) "Talking in the Dark", New York Times Magazine.