HNEC: A Hybrid Network Emergency Communication Model

Abdussalam Nuri Baryun, University of Glamorgan, UK

Khalid Al Begain, University of Glamorgan, UK

David Villa, University of Castilla-La Mancha, Spain

ABSTRACT

To communicate within disaster scenarios, different devices/systems need to cooperate with specific protocols. The key communication protocol needs to provide interoperability among these systems and provide the solution for emergency services. The paper studies the hybrid network disaster recovery (HNDR) systems and classifies its communication scenarios and requirements. We propose a new networking protocol for the hybrid network, with ability to forward sessions and messages through different transport protocols, and copes with node mobility and node failure. The paper considers heterogeneous network disaster recovery scenario and proposes a cost effective and easy to deploy hybrid network emergency communication protocol (HNEC). This internetwork protocol is a specific model of the inter-domain messaging (IDM) protocol for emergency communications. The routing protocol procedure is similar to the reactive AODV procedure but is different in maintaining routes from unpredicted link breaks or node failure. A detailed simulation model with the designed network layer model is used to investigate network delivery rate and end-to-end delay performance. The performance results are analyzed using varying node load, mobility speed, and network size.

Keywords: *Network Disaster Recovery;Ad Hoc Network; Sensor Network; Routing Protocols.*

INTRODUCTION

When a large scale natural disaster occurs, the local communication infrastructures are typically damaged, and become unreliable or disabled. Rebuilding the communication infrastructure requires many days or weeks. Therefore, rescue teams will have to rely on their communication systems. Having a reliable wireless network would be very valuable for rescue teams in the first hours after the disaster, when the likelihood to find alive victims is much higher.

In disaster environment there will be a need for many heterogeneous network systems, technologies, and computing devices from different manufacturers. In this case the design of a common infrastructure is complicated due to the dynamic characteristic of user requirements and application scenarios. Both mobile ad hoc network (MANET) and wireless sensor network (WSN) are ad hoc networks, but WSN is with different system architecture. WSN devices provides additional/or specific service of sensing the environment. It contains a sensor unit with the communication unit. MANET nodes are usually larger communication devices such as personal digital assistants (PDAs), smart phones and laptops. These mobile devices support recovery operations and emergency communications. The main objectives of the paper is to design and implement a set of mechanisms, services, protocols and procedures to provide a fully functional heterogeneous network from scratch in only few hours.

The main contribution of this paper is implementing a new protocol as extension of a reactive ad hoc on demand routing, based on inter-domain messaging (IDM) instead of internet protocol (IP). The new protocol uses remote method invocation message in routing and forwarding instead of packets. Another contribution is developing a new addressing scheme specifically for disaster networks, and modifying IDM to specify to disaster networks purposes. The paper is organized in five sections. Firstly, we introduce and classify the hybrid network disaster recovery communication systems. Secondly, we survey related work of solutions to DNR situations. Thirdly, demonstrate the HNEC hybrid protocol for the disaster network. Fourthly, we describe the simulation model and analyze performance of the newly developed protocol. Finally, we summarize and conclude.

THE HYBRID NETWORK DISASTER RECOVERY (HNDR)

Communications

Potentially, in disaster situation a fast deployment network is recommended and the proposed solution can be categorized in three ad hoc networks: a) using MANET only with coverage depends on network size and antenna gain, b) using Wireless Sensor and Actuator Network (WSAN) with mobile sinks to the MANET. This combination adds to MANET sensing and reacting services capabilities. Sensors measure and monitor a physic magnitude (e.g. temperature, poison, smokes, nuclear damages, etc.), but actuators change a state of a process or object which may drive a physical magnitude. c) adding High Altitude Platform (HAP) and satellite systems, to improve coverage to larger areas and may be used to support emergency call systems (e.g. HAP system may be alternative to cellular emergency system). The additional ad hoc nodes (such as HAP or satellite systems) can be utilized for larger disaster impacts. HAP system provides coverage of about 300km in diameter. Satellite communication system requires more complexity and larger antenna for communication than in HAP, therefore, HAP systems are more flexible and advanced (range distance is less than 20 km) and that its transceivers can be smaller. In some situations dangerous areas cannot be accessed safely, it is recommended to examine the suspicious area. Small sensor devices may be distributed within those areas to gather information and send response when needed. Therefore the internetworking between MANET and WSAN is essential. This paper develops a hybrid protocol for emergency networks of sensors, actuators, smart phones and PDAs. The protocol involves routing and internetworking functions for MANET and WSAN within a disaster scenario. The network user communicates through the network nodes by sharing their resources. Most of the HNDR nodes are IDM routers and are able to interconnect different network technologies.

The network disaster recovery (NDR) was defined by Chen, Macwan, and Rupe (2011) as recovering communication after a disaster and supporting communications during that recovery until normal situations. Rapidly practical exercises for NDR were established in many cities to gain experience and get prepared for unpredicted situations (Morrison, 2011). The post-disaster planning and practices result in best practice procedures and coordination for communication teams and systems.

Utilized Technology at Disaster Situation

The disaster recovery network contains different nodes with different capabilities. Due to the different recovery needs in the disaster impact areas (DIAs), the communicating node may have different techniques. The communication technologies used in and out the DIAs are classified in Table 1. Each technology is used to solve the global efficient communication of the NDR and to solve the local need for communication. There are two important examples that may clarify the global benefits and the local needs.

Firstly, the rescuers should be able to communicate easily with others to be able to complete his mission, without using conventional communication infrastructure, and with fewer casualties.

Table 1. The HNDR Communications' Systems, distributions and Services

	Wireless Sensors and Actuators	**PDA**	**Portable Computers**	**Large Portables with large Antennas**	**Fixed Base Station (BS)**
Type of node Services	-Physical measure /event monitor. -compute and analyze. -communicate and route data.	-mobile comput and commun. -camera monitor	-portable compute and commun. - data, voice, and video storage. - WLAN management.	-long transmission range, and high speed communication. -large memory storage, and processing. -mobile and portable communication.	-Telecomm and internet services. -Heterogeneous network manag. -backup database and video storage.
Energy Storage	VL	LW	H	VH	VH
Mobility	Fixed	H	LW	H/LW	VLW
Communication links possibilities and standards	Bluetooth IEEE802.15.4 ZigBee 6LoWPAN	WiFi 3G Sensor links HAP	WiFi 3G WiMax HAP	WiFi 3G WiMax HAP UAV Satellite System	WiFi 3G WiMax HAP Satellite System Internet WAN
Data Transmission Rate (speed)	VLW	M	H	VH	VH
Number of node distributed in network	VLR	LR	M	LW	VLW
In/out disaster area	In (All)	In (LR) /Out (LW)	In (VLW) / Out (M)	In (VLW) / Out (LW)	Out
Used for	Alarm and event monitor.	-Data, voice, video comm. By rescuers (low quality). - may commun with rescues. -Gateway to WSN	-Data, video, voice comm. by doctors, recuers, with the BS.	-all comm. (high quality), - disaster field managers, and network managers -as gateway for the base stations	-as BS and for disaster managers.
GPS capability	Some	Maybe	Maybe	Maybe	Yes
IDM Platform	Some	All	All	All	All

VLR - very large LR- Large M- medium VLW- very low LW-Low
VH- very high H- high BS- base station WLAN- wireless local area network

The prediction of any further disaster occurrence may be indicated locally by using interaction between WSAN and MANET, or indicated globally by using interaction among: MANET, HAP system, and satellite system. All MANET nodes will be able to receive any call or message from the base station even if the DIA is large.

Secondly, the physicians outside the DIA will locally need full information of their patients' accident while examining (e.g. biology disaster, special distributed disease, etc.). But the information they need is inside the DIA and will require both the local and global information technology. The rescuers should be able to collect information to rescue and to save lives and their lives to continue the rescue mission. Furthermore, the physician should be informed of their patients' accident history to diagnose the problem to complete the NDR goal.

The other important issue is to maintain; a) the communications inside the DIAs, b) the communications outside the DIAs, and c) the communications between inside and outside the DIAs. From Table (1) it can be shown that the smart phones or PDAs will have high mobility to be used by rescuers and form their MANET, with the capability of communication with different gateways as: sensors, portable computers, large portables, and the base station.

Rescuer's Communication Devices

The key device for rescue in the scenario is a set of smart phones and PDAs carried by each rescue group members. The PDA creates one or more spontaneous ad-hoc networks using a WLAN technology (probably IEEE 802.11 Interface). In addition, the system needs to support several kinds of devices that may be integrated when they are present. The PDA is characterized by high mobility and medium autonomy. The following complemented devices that can be used in the scenarios to support rescue mission requirements:

Sensors: Depending on the kind of the disaster, it may be convenient to deploy an arbitrary set of sensors. Sensor nodes may integrate several kind of transducer sensor: temperature, light, motion, vibration, sound, position, etc. The sensor nodes form a WSN using a low power wireless technology. The sensor nodes typically have low data rate and very low autonomy (with small batteries). At difference with other WSN applications, this does not require especially small size or weight although they need to be robust enough to allow their deployment by means a low altitude plane. Last, they must be low cost since many may be required and in most cases they will be destroyed or used in just one emergency situation.

Portable wireless computers: These are devices that are convenient into the infrastructure by an easy way. They can form a better medium to pick a lot of information from sensors, PDAs and smart phones, and they also can present maps, graphical data, etc. These devices are carried by some rescue staff and they have good autonomy, medium mobility, and suitable medium radio range (e.g. may have smart antenna). Furthermore, they may have several network interfaces (WiFi, 3G, WSAN, etc.) to enhance the network resources.

Vehicles and base stations: The rescue vehicles (cars, helicopters, etc) may operate as base stations to communicate other isolated networks. Vehicles have very high autonomy and radio range. Base stations have direct data link to communicate easily remote areas in same zone.

Remote "clients": Base stations (BS) may provide remote access to "external" clients. Using available data technologies (e.g. satellite systems) base stations can give access to remote computers through internet. This allows headquarters to obtain direct information about rescue tasks and progress.

The HNDR Network Desired Services

The platform must support a very heterogeneous set of services to support all activities developed by the staff. We classify the services in three categories:

Core services: These are common services provided by the middleware platform:

- Event propagation.

- Event logging: For internal and external (Environmental) events.
- Network File System.
- Deployment.
- Service/Node discovery.
- Heterogeneous Network management.

Support services: These are specific services needed by rescue operations:

- General emergency telecommunication services (ETS) requirements considered in RFC3689 (Carlberg and Atkinson, 2004).
- Audio/Video transmission. Streaming and real time communication.
- Image sharing.
- Device position.
- Data aggregation/composition.

Optional services: Valuable services:

- Data analysis.
- Visual representation (GIS).
- Real-time topology analysis. To help routing algorithms and prevent network fragmentation.

HYBRID NETWORKS

The TCP/IP network, the WSN and MANET networks are different in their architecture, but their interconnection can provide interesting services. Networking different network architectures provides a hybrid network. The previous sections proposed a heterogeneous network solution for disaster recovery assumes that each node connecting to a network should have the right network interface technology. Still, an internetwork protocol is needed to communicate nodes in a hybrid network. Some researchers combined WSN with the internet by using IP to internetwork them. However, accordingly to Dunkels, Alonso, and Voigt (2004) the problem of heterogeneous networks with sensors based on TCP/IP is that it adds overheads to sensor applications that affect its performance. They proposed a modified IP protocol by reducing the IP address between 8 and 16 bit as a light address to be suitable for sensors and to implement interface converging at the gateways. In Han (2007), the authors are proposing a Tiny TCP/IP which still faces some challenges. This paper proposes IDM based protocol (Villa, et al. 2008) for internetworking and a hybrid reactive routing procedure which are described in titled section; the hybrid protocol.

Related Works

Many research works in hybrid network topic can be related to this paper's solution approach in four aspects: a) combining networks for disaster recovery, b) internetworking, c) addressing scheme for hybrid network, and d) using middleware approach to integrate networks. A disaster network scenario was introduced by Fujiwara, and Watanabe (2005) with a hybrid wireless network, combining ad hoc networks and a cellular network to maintain connectivity between a BS and node users in the DIA. Their approach considers disaster impact that does not damage the cellular infrastructure. On the other hand, Dilmaghani, and Rao (2006) consider the infrastructure damage possibility and they proposed in a Hybrid Wireless Mesh Network as a well-suited candidate capable of creating an easy deployed network replacing the damaged cellular network, however, it internetwork only with IP. This paper introduces hybrid of MANET and WSAN networks by networking them with a hybrid protocol.

Internetworking is the function of routers to connect networks of different network technologies (network interfaces), however, many approaches for internetworking have been surveyed by Baryun, and Al-Begain, (2011). According to Senner et al. (2008), a non-IP networking protocol is preferable to combining MANET and WSN for fire rescue operations. The protocol architecture was ID-based routing with MANET nodes having two medium access protocols (capable to be used as a gateway for sensors), the scenario application were fire-emergency indoor and outdoor. The PDAs use wireless LAN to communicate among each other and use Zigbee to communicate among sensors. According to Gadallah, and El-Kassabi (2008) using a light IP architecture for WSN, and IP based network for MANET. Furthermore, it assumes no internetworking problem when using both the IP and light-IP architectures. Their approach using a dual routing protocol for ID based and data content based. However, most integration solutions for WSN and MANET are by using gateways (Feeney et al. 2001; Horreet al, 2007; Ansari et al. 2008). That is because of their different address schemes and protocol architecture. However, having a combined routing protocol to integrate MANET and WSN are more complicated than using a gateway translating protocols for integration.

Some researchers unite the addressing scheme to suite network architectures differences (Gadallah, and El-Kassabi, 2008; Mayer, and Fritsche, 2006; Baryun, Al-Begain, and Villa, 2011). The address scheme depicted by Senner, Karnapke, Lagemann, and Nolte (2008) is 8 bit address which distinguishes WSN and MANET networks address by one bit, and another bit distinguishing between broadcasting and unicasting. The purpose of shortening the address in many researchers' works is to simplify the packet size and processing of tiny devices like motes or RFIDs. On the other hand they reduce the upper limit of network size. However, for a very large network the IPv6 provides 128 bit address for the internet of things (IoT), and includes compression techniques to reduce packet header size. In addition, the fixed addressing allocation of dynamic ad hoc networks requires node discovery and route maintenance for sensors, mobiles, and other node devices, therefore, the design of a routing protocol suitable for all devices is required.

Middleware communication platforms (i.e. DCOM, .NET, Jini, Java RMI, CORBA, and ZeroC Ice) are used with different features and purposes, however, the implementation of the complete heterogeneous networking middleware is still a challenge. Middleware applications were surveyed for MANET (Hamid, Al-jaroodi, and Mohamed, 2006) and WSN (Wang, Cao, Li, and Das, 2006). Both surveys argue that middleware add good advantages to these application specific networks. However, due to their unreliable connectivity the middleware approach still faces challenges. Dyo (2005) proposed a middleware integration approach between WSN and mobile devices. He argues that it eases the networking communication even though there are some middleware design differences for those devices. According to Horre, et al., (2007) describes advantages of using middleware in integration of sensors, PDA, and internet. However, they argue that there are challenges for E2E integration ability in the tradition middlewares. As using middleware for integration it is used for networking, in the model of Common Object Request Broker architecture (CORBA) to internetwork different networks' systems, by message source routing (OMG, 2002; OMG, 2008). However, its messaging technique makes it not suitable for heterogeneous networks because it gains overhead in the message. Another middleware communication platform is the Internet Communication Engine (Ice), its goal is to build a heterogeneous environment for a wide verity of internet domains (Henning, and Spruiell, 2003). Ice focused on Internet applications and it does not put attention on WSAN or ad hoc network heterogeneity. However, to give more flexibility to the network and the ability to change services, researcher investigated in virtual networks (Mosharaf, Chowdhury, and Boutaba, 2009).

Inter-Domain Messaging Protocol (IDMP)

The general purpose IDM model was first introduced in 2008 by Villa, et al. (2008). The IDM model uses the ZeroC Ice platform. The IDM model adds to the Ice platform (i.e. middleware for internet domains) internetworking with non-IP network domains. IDM is an object oriented generic communication model and aimed to provide heterogeneity, routing and security for different devices (i.e. sensors, actuators, etc). The IDM model is designed to be integrated with Ice platform, to use Ice services (i.e. IceBox services, IceStorm services, IceGrid services, etc) and to introduce the IDM protocol which acts as a transparent transport mechanism to communicate conventional Ice clients and objects. IDM protocol is a seamless routable protocol that reduces overhead by means of a cross-layer transport mechanism. The authors recommend IDM model framework for network communication applications which involve WSAN or limited resource devices.

The implementation of IDM in disaster situations was first introduced by Baryun, Al-Begain, Villa (2011). They investigated the reliability of IDM on top of IEEE802.15.4. The protocol is based on a distributed object model, where the IDM objects are the nodes of the IDM network. The network services are available through IDM objects. In fact, IDM addresses services instead of hosts. However, its addressing is a universal hierarchical object oriented addressing scheme, which means its logical address includes: services, events, interfaces, hosts, routers, etc. Each object has a unique address which preferably includes in it the domain, network, host and application identities, to distinguish objects in different subnets, hosts, or applications. The IDM router can route messages between different applications, hosts, subnets, or domains. Furthermore, addressing for objects can be classified in different addressing schemes depending on the underlying networks' requirements or applications' purpose.

Mobile Sink and Multi-Sink

There are some drawbacks of using gateways for integrating hybrid networks, due to the dynamic topology and unexpected link breaks and/or node-faults in WSAN and MANET networks. Using the gateway as integrating such dynamic networks requires its handover to another gateway if it moves away from the networks' wireless coverage. However, in WSN it is not possible to have gateways (called sinks) without some practical problems (Akkay, and Younis, 2004). There is a need of many sinks to communicate to WSAN because of its energy constraints. Furthermore, while networking MANET and WSAN, the multi-sinks are mostly mobile sinks. This mobility and energy constraints complicates the network gateways design.

To gain a longer life time, all WSANs in the heterogeneous network will require multiple sinks to reduce the disseminated load among edge nodes or sink-neighbors. In addition a routing technique is required to use alternative routes and to balance-consumption of paths to sinks. The heterogeneous network may require multiple mobile gateways for MANETs if they use different routing protocols (proactive or reactive protocol). Each routing protocol in the gateway will need a different IP address. However, the gateway will be running two different routing processes after each update period or at each topology change. Therefore, for WSAN and MANET, the key solution is providing seamless communication among networks and all nodes through a hybrid network protocol.

In the proposed solution, the gateways of each network should have the hybrid protocol (all of them in the more flexible case). It behaves with these networks as if they are like a single one network, performing one routing protocol for all devices and assuming that any device can be used to route data to other devices or to other networks. However, to route among networks with different technology (i.e. different network interfaces); there is a need for that the gateway to have those network technologies to access and internetwork such networks. For example, to integrate between WSN/IEEE802.15.4 and MANET/IEEE802.11, the sink or gateway will need both technologies and if the gateway has more network technologies it will be able to access more networks. In the disaster situation, the rescuer communication devices (i.e. PDA, smart phones, etc.) are capable to access and internetwork many networks and to become the multi-sink. Another important issue is the gateway technique used between IP networks and non-IP networks. In addition to their technology differences they have different network architectures. The gateway's hybrid protocol is responsible to internetwork such architectures.

The IDM routable protocol uses a universal object address scheme to integrate all different networks into one hybrid network. Unifying the address to become unique in the entire network is essential, however, to insure uniqueness it adds overhead to the IDM message header. To combine different network architectures the IDM provides endpoints to access each architecture to encapsulate and decapsulate messages, and to provide a mechanism to transport data through different network architectures. The multi-layer routing facility of IDM makes it possible to use the protocol in network-layer, transport-layer or middleware-layer. Furthermore, to solve the dynamic topology of these networks, the IDM platform is associated with a hybrid routing protocol and a Quality of Service (QoS) forwarding management technique, to implement the mobile sink internetwork services. This protocol is described in the next section. Therefore, the hybrid network will have mobile gateways that are capable of being multi-sink and capable to coordinate access, routing, and service management to improve the heterogeneous network performance.

In the disaster network solution the sinks and gateways are the smart phones, PDA and vehicles. While the network nodes are: objects, sensors, actuators, smart phones, PDAs, vehicles, HAP, and satellite).

THE HNEC PROTOCOL

The HNDR networking protocols are to be implemented in the IDM layer with specification language of Ice (Slice) and by using a specific modified IDMP for emergency. The hybrid network emergency communication protocol solution (HNEC) for the disaster network is the integration of IDM heterogeneous protocol and a hybrid routing protocol called Hybrid Network Disaster Recovery protocol (HNDR). The IDM router module implements the hybrid routing protocols interfaces and functions. The hybrid protocol is a multilayer router by using endpoints plug-ins between IDM layer and IDM under-layers.

The HNEC Protocol

This protocol is the internetworking protocol for the HNDR network. The HNEC implements a special routing protocol for network disaster protocol and a specific QoS forwarding management technique. HNEC like the IDMP unifies all of networks providing a single routing mechanism built on top of the existing networks' protocols. HNEC uses a specific object address scheme and its messages structure are created by modifying IDM message structure. The reason behind using a specific name for this protocol rather than naming it the IDM, is to differentiate between routing protocols using IDM. In the disaster situations the IDMP modified version for these applications is the HNEC protocol and is specifically for HNDR network or emergency communications.

The IDM objects implement interfaces, that the designer needs to specify using the interface definition language Slice (Henning, and Spruiell, 2003). The object services are available through object's interface(s). The object interface is called a facet. Each remote object has at least one facet. The Adaptive Location Protocol (ALP) module is responsible of mapping logical object addresses to physical transport endpoints. IDM supports all protocols so that each domain has their own rules and each network/subnetwork may have their own protocols.

HNEC Address and Message Structure

A unique address scheme is required for internetworking general purpose networks. However, their configuration and lookup techniques may be challenging in MANET and sensor networks. Address auto configuration issues and consideration are used. In (Feeney, Ahlgren, and Westerlund, 2001) uses the zeroconfig to address hosts in spontaneous networks. This technique is easier in configuring networks as a self configure technique, and is used for some hosts of our addressing scheme. In the HNEC the unique address has four fields: Object, Host, Network, and mission, as shown in Fig.1. For the objects identification in each host, two bytes are enough to distinguish applications and their objects. The host-ID is autoconfigured by the zeroconfig to generate IP addresses only for IP capable devices. The address fields are configured by the ALP module. The ALP in each node is also responsible to register and locate the remote object by getting its proxy reference through its Lookup method. Any node registers its local objects and remote objects it serves at the Locator of the ALP module. The registration adds the object address, and its associated adapter endpoints in the location map table. For IP capable devices the host ID includes the host and network ID. For non-IP systems (i.e. WSAN, satellite system, etc.) MAC addresses are included in its host ID. Six bytes are allocated to this field to enable the identification of the host. Usually many tiny sensors have a 16 bit MAC address and most communication systems have 48 bits MAC address size. This different in address size can be used to distinguish sensor devices from the mobile devices.

Object ID 2 Byte, identifies services,
resources or events.
Host ID 6 Bytes, MAC addresses
for non-IP devices, and IPv4 address
for IP devices
and Laptops.
Network ID 8 Bytes, GPS position coordination
for all nodes.
Mission ID 2 Byte, identifies different
APPs-purpose, rescue-groups,
subnet regions and systemType.
Address size:18 Bytes

Figure 1. The HNEC unique address

The HNEC field for network id is the network position using GPS services. The network identification is based on location. The 2 last bytes are for domain and rescue-groups. For the host identification the systems enabled with IP can generate a unique IP address by using zeroconfig protocol. For the network identification the use of GPS position for all nodes, will require about 8 bytes for accuracy of 3 meters. The host ID and network ID do not ensure the uniqueness of the addresses generated, because they are self configured. There is possibility of repeated MAC address by different manufactures or a repeat of IP address by the zeroconfig protocol in different networks. Therefore, a fourth field to distinguish these possibilities is required which is established by the mission field. Its configuration can be organized by the network management team.

The mission ID is categorized in Fig.2. The first two bits in the mission ID are to identify the address transmission (TR): unicast, multicast, anycast, and broadcast. The next 6 bits are for autonomous system ID. The communication system types like mobile-satellite system (SS), mobile-HAP system (HS), PDA ad hoc system (MN1), smart-phone ad hoc system (MN2), wireless sensor system (WS), and wireless actuator system (WA), are identified by 4 bits and rescue groups with the last 4 bits. The system types identify the combination of communication system and computer system. Therefore, there may be two types of PDA or smart-phone systems used in the disaster situation. These mobile devices are the most suitable devices becoming gateways or sinks for HNDR. These systems may be used by different groups of rescuers. The last 4 bits is for identifying recue-groups (16 options).

TR	Domains	Systems	Groups

Systems		Groups	
0000	general	0000	general
0001	MN1	0001	Rescue 1
0010	MN2	0010	Rescue 2
0011	MN3	0011	Police
0100	WS	0100	Firefighter
0101	WA	0101	Ambulance
0110	HS	0110	Management
0111	SS		

TR: 00 - Broadcast, 01 - Unicast, 10 - Multicast, 11 - Anycast.

Figure 2. The mission ID of HNEC address

The Domain field can be configured by the administrator depending on the disaster recovery plan requirements. Others systems or group identifiers options are reserved for future use.

The HNEC data-message structure is a modified IDM message which has two header sizes, one short and other normal. For the stream-message it is the same as IDMP which uses IDM-socket. The modified message structure is shown in List.1 in Slice language. Usually for sensor communications the HNEC message size should not be longer than 102 bytes which is the limit for the frame payload of IEEE802.15.4 standard, because it's MTU is 127 bytes.

```
Module IDMP{
  struct HeaderData {
          byte magic_I, magic_D, magic_M; \\ 3B
          byte MessageType;     \\ 1 Byte (B)
          short MessageSize;    \\ 2 Bytes
          int requestId;        \\ 4 Bytes
          byte routerId;        \\ 1 Byte
          HNEC:: Identity Dst;  \\ 18 Bytes
          HNEC::Identity Src;   \\ 18 Bytes
          byte hoplimit;        \\ 1 Byte
          ToS tos;              \\ 1Byte
          int flow;             \\ 4 Bytes
          byte mode;            \\ 1 Byte
          };
 struct ShortHeaderData {
          byte magic_I, magic_D, magic_M; \\ 3B
          byte MessageType;     \\ 1 Byte (B)
          short MessageSize;    \\ 1 Bytes
          short requestId;      \\ 2 Bytes
          byte routerId;        \\ 1 Byte
          HNEC:: Identity Dst;  \\ 18 Bytes
          HNEC:: Identity Src;  \\ 18 Bytes
          byte hoplimit;        \\ 1 Byte
          ToS tos;         \\1Byte (has 3 bit flow)
           byte mode;           \\ 1 Byte
          };
 struct ForwardData {
          string operation;       \\ variable size
          Encapsulation param;  \\ method dependent
          };
 struct ForwardShortMsg {
          ShortHeaderData header;  \\ 47 bytes
          ForwardData payload;       \\ max: 55 bytes
          };  \\  forward through sensors
 struct ForwardUserMsg {
          HeaderData header;           \\ 54 bytes
          ForwardData payload;
          };   \\  forward not through sensors
 struct ForwardRawMsg {
          HeaderData header;
          Ice:: ByteSeq   payload;
           };   \\  forward not through sensors
    };
```

List 1. The HNEC message structure.

The HNEC short message header for sensor data communication is 47 bytes, which gives room for the encapsulated data to be from 8 bit to 55 bytes. However, for the devices with IP capable the payload is not restricted to a limited payload size because IP has a fragmentation mechanism.

The HNEC forwarding mechanism is network specific forwarding using destination address as index in the forwarding table. Forwarding request messages and reply messages. However, because it forwards messages that invocate methods, there may be a return result (if available) to the request, therefore, the reply message is forwarded to the request source. In this case the message type is reply and the requestId is the same as the requestId of the request message. The router ID is to identify the HNEC router, because there may be other routers in the network for other purposes. The HNEC forwarding algorithm priorities messages depending on three items: message type, Type of Service (ToS) and flow. The ToS and flow distinguish the importance level among messages. In most protocols first in first out (FIFO) is used in forwarding data which is not preferred in emergency communication. Forwarding for special messages or emergency neighbor nodes should have higher priority. For subnetworks the router indexes the network address which is identified in the address prefix. Router may priorities messages while checking the destination address's application identity, or group identity within the mission field, however, mainly it checks the flow field in IDM message format.

In HNDR disaster scenario, all computing devices (sensors, actuators, smart-phones, PDAs, laptops) are HNEC nodes (providing IDM services) and probably many are HNEC gateway routers. For these routers they implement the Hybrid Network Emergency Reactive routing protocol (HNER). The HNER is an AODV-like routing protocol (Perkins et al., 2003). As the AODV is implemented on top of IP layer, the HNER is implemented into the IDM layer, on top of the IDM endpoints. The IDM endpoints and HNER protocol are described in the following sections.

IDM Endpoints and Endpoint-References

The endpoints (EPs) plug-in entities are the abstraction that provide IDM layer a crosslayering to underlying protocols and technologies. This endpoint Plug-in may be called the Endpoint-Plug (EPP). They encapsulate all details regarding network data transport. The EPPs are used by the middleware kernel to encapsulate and send messages to remote objects in a transparent way. Ice platform has three of-the-shelf endpoints: TCP, UDP and SSL. That is all Ice need to perform end-to-end transport on Internet. We are adding other Ice-compliant endpoints:

- xbow: XBow protocol transport for IDM invocations in a WSN using Crossbow motes. The low-level addressing scheme use MAC numbers.

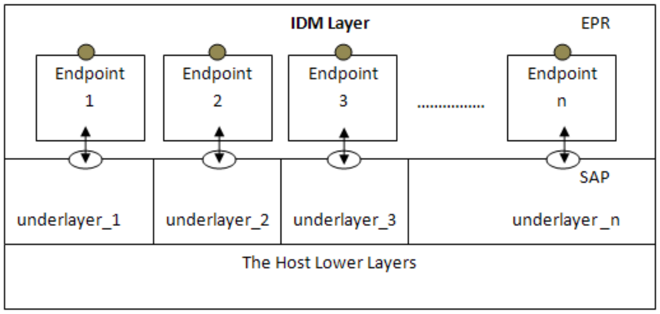

Figure 3. IDM layer and its Endpoints

- erh: To encapsulate Ice directly on Ethernet frames. Only can be used in the LAN neighbourhood and it uses a specific "protocol" field value to refer the adaptor listening in the node. Usually the node has a single eth endpoint.
- ip: Very similar to eth. It uses the IP address and a "protocol" field number to contact the adaptor.
- zigbee: zigbee protocol transport for IDM invocations in WSN, using a 'protocol' field number to refer the adaptor listening.
- unix socket: For high performance communication systems.

Endpoint-Reference (EPR) is the endpoint physical identification which includes four items: protocol name (i.e. UDP, TCP, IP), host ID, port number, and timeout. Each EPR is allocated to the service access point (SAP) of the IDM underlayer-protocol. The SAP is the port number. The EPR is created by the object adapter. IDM endpoints are designed to not replace the typical protocols of each network systems of HNDR. However, it uses their underlayer protocols to forward messages among IDM capable nodes.

HNER Routing Protocol

The HNER protocol is a facet of the HNEC router as shown in List. 2 in Slice language.

```
Module HNEC{
   enum status{ active, repair, invalid};
   dictionary<string, string> Context;
   struct RoutingEntry{
      HNEC::Identity Dst;
      HNEC::Identity Mask;
      HNEC::Identity NextHop;
      int DstSeq;
      string facet;
      IDMP::EndpointSeq  epr;
      byte RouteCost;
      float entryLifeTime;
      status  routeStat;
      Context cntx;
      };
   interface HNER{
     void RREQ(byte reqFlags, byte minEng,
                    byte hopCount, byte dataSz,
                    HNEC::Identity Src, int  SrcSeq,
                    HNEC::Identity Dst, int DstSeq);
     void RREP(byte minEng, byte hopCount,
                     HNEC::Identity Dst, int DstSeq,
                     HNEC::Identity Src, float LT,
                     byte prefixSz);
     void NHEL(HNEC::Identity Dst, int DstSeq,
                     byte minEng, byte speed);
     void RERN(bool N, byte reason,
                     HNEC::Identity UnDst);
     void RERL(bool N, byte reason,
                     HNEC::Identity UnDst);
      };
};
```

List 2. The HNER interface as a facet of HNEC.

The HNER routing algorithm is similar to AODV, just for some additional modification to routing parameters in messages and routing table.

The HNER is a remote object interface of the HNEC router. Therefore, this protocol can reach any HNEC node/device through HNEC gateway routers in the HNDR. The HNEC router considers the network context, DA context, device context, and user context. This awareness of these parameters allows the router to select routes including route context.

The destination decides the route selection if it receives RREQ while the message mode is one-way and if the mode is two-way the destination leaves the source to decide the selection of route. However, the source decides the selection of the endpoint used to traverse the network. Service discovery protocol (SDP) maybe used in the case of finding the service required, because of mobility and possible node failures or node battery depletion it can induce changes in the availability of services and topology. Gateways use NHEL messages for multi-sink and mobile sink announcements. When a sensor node receives the announcement it includes the gateway in the network gateway list.

The HNER has four method operations which are the route request method (RREQ), the route reply method (RREP), route error node method (RERN), and the route error link method (RERL). Each method contains arguments that may involve in the update of the routing table. These method operations are implemented in the HNEC module. The routing table entry structure is shown in the HNEC module, and the entry items include EPR to refer to the transport path, and the context indicates the context parameters. RREQ method is invoked for route discovery, or for route repair in the same algorithm as AODV algorithm. However, the HNER-RREQ involves two additional parameters; the route minimum energy (minEng), and message data size (dataSz). The minEng is the lowest energy of a node in a route. Each node compares its remaining energy and if it is lower than the energy in the RREQ it will amend the route minEng to its remaining energy. For the route to the source each intermediate node updates its routing table by gathering information from RREQ parameters. The dataSz will help the router to be aware of the data size context provided by the application layer, therefore, it may select the route that has a suitable expected lifetime. The route lifetime in AODV is depending on the number of nodes. The HNER involves the network context. The expected route lifetime can be estimated through the use of routes through such area or such destination.

HNER protocol has four method-messages in comparing with the AODV three messages. Two messages are for link or node error detections. The AODV only detects the link break either by using the underlayer feedback or by the hello messages. The HNER detects errors through hello and acknowledge message invocations. HNER depends on the neighbor nodes to detect both errors and they inform interested nodes. If a node notices it's failing to perform, then it informs neighbors nodes by broadcasting RERN, otherwise neighbors can expect node failure by its information about the nodes speed and remain energy included in the last NHEL method-message received. The RREQ flags and source sequence number and destination sequence number are treated as in the AODV algorithm procedure. The difference is that AODV algorithm and messages are using IP addresses but HNER uses HNEC addresses. Furthermore, AODV message is encapsulated in IP packet, but HNER method is invoked using IDM remote message invocation, and the HNER methods parameters are encapsulated in the IDM message.

The routing cost of the HNER is the combination of route hop count and route minEng. However, the route selection includes the route cost and the route context. These parameters are included in each route entry for every route paths created. Depending on the route context the HNER will consider either a multipath or single path routing. Interior and exterior gateway routers are important in the HNDR network to reduce overhead and to make efficient routings. The

HNEC protocol contains HNER for interior routing (IR). In future work a proactive protocol as the exterior routing (ER) will be recommended. Only gateways with large energy supplies have ER. However, to simplify the routing discovery a geographical mechanism can be used by both IR and ER, because addressing includes object location information. In this paper we implement only the HNEC and HNER routing.

Quality of Service Forwarding Management

Two types of forwarding used in the HNEC protocol are; a store-and-forward and a store-carry-and-forward techniques. There are some situations where it is important to deliver a message even if a route cannot be established. These important messages can be carried by intermediate nodes and delivered when it finds a route to destination. This is true for delay tolerant applications. Also in these cases the intermediate node devices should be resource-capable to store and carry information (i.e. the device mobility is used to get the stored message delivered or forwarded through an established route) until forwarded or delivered. These are managed by the QoS forwarding management (QSFM) module. In many QoS architectures, forwarding traffic priorities are dependent only on traffic characteristics (DiffServ, and IntServ). The work of Villanueva et al. (2006) highlights network administrative and management tasks to improve context-aware QoS of MANET for home applications. Their approach of QoS architecture is used in the QSFM framework. However, in the HNDR applications, it is essential to manage forwarding traffic flows taking into account the actual status of the disaster recovery environment, the network context, user context, and device context.

The QSFM architecture provides per-class service differentiation taking into account context information which is gathered through Ice middleware services and IDM platform (e.g. event gathering services). Shared information between applications within HNDR allows implementing mechanism to provide QoS features by both DiffServ (based on class) and IntServ (based on flow). On the other hand, the service forwarded is context aware in respect to the routing environment. Furthermore, reliable and/or secure forwarding are crucial for some messages. The reliability and security are decided by the QoS profile at the source initiating the request. QoS management is adaptable to applications requirements.

```
Module HNEC{
  Module QSFM{
    enum serviceFeature {bestOffer, maxLatency,
                          minBandwidth,
                          reliability, maxJitter
                          authorize, authenticate
                         };
    enum flowFeature  {guarantee, controlLoad,
                       maxBurstSize, peakRate,
                       secure, emergency};
    enum contxtFeature  {domain, location,
                          network, user, device};
    dictionary<serviceFeature, string> servProfile;
    dictionary<flowFeature, string>  flowProfile;
    dictionary<contxtFeature, string> cntxtProfile;
    interface Admin  {
      void setQsfmServ(servProfile qos, ToS tos);
      servProfile getQsfmServ(ToS tos);
      void setQsfmFlow(flowProfile qos, int flow);
      flowProfile getQsfmFlow(int flow);
      };
   };
};
```

List 3. The QSFM module in Slice language.

Two types of QoS profiles one for service type and other for flow. The QoS class profile updates the diffServ, and the QoS flow profile update the IntServ. Both profiles are updated depending on the service request agreements between end-to-end nodes for the communication. An additional context profile is provided to ensure context aware communication. The previous two profiles are concern of the received message content and received message source's context. In the third profile, the context of the node receiving messages is concerned. For example, in an emergency evacuation incident, nodes evacuating the dangerous area need cooperation and find the way-out alternatives. As it is not possible to save lives while the own node's life is in danger. Therefore, it is important that the information collected, forwarded, and delivered is priorities on the third profile that includes the node's environment context situation. This profile may be updated periodically or on an event bases. Depending on these three QSFM profiles that are created for the applications' messages, the HNEC router forwards and delivers messages to destinations. To increase the processing speed QSFM lists for each flow the forwarding and delivery items; the next hop, interface, and EPR.

The QSFM is responsible to select the suitable EPP for the client depending on the client's QoS requirements. The parameters that are considered while selecting the underlying protocol in the client or server:

- Invocation is one way or two ways.
- Service is connectionless or connection oriented.
- Confirmation/ proof of delivery.
- Service features
- Flow features
- Context features
- Ordering of messages.
- Authentication.
- Authorization.
- Source routing or table based routing.

On the other hand, each EPP entity lists and checks the QoS offered by its underlying protocol or network technology and sends the availability to QSFM. The parameters of the network offered QoS available are:

- Maximum BW.
- Maximum Latency.
- Maximum jitter.
- Reliability.
- Security.

The HNEC protocol routes and delivers the message depending on the service required and the availability of the QoS in the underline protocols. Some of the requirements such as encryption may be provided at the end-to-end services, but others requirements such as the required BW must be guaranteed along the whole route nodes. This is arranged through the QSFM which is out of scope of this paper.

SIMULATION AND ANALYSIS

The HNEC is connection and connection-less oriented protocol. Therefore, it uses acknowledgements or receives confirmations to improve the delivery reliability. The carry and deliver technique used is investigated in this paper also. Baryun, Al-Begain and Villa (2011), investigated the forwarding with and without acknowledgement while no link-break-feedback detection is served by below underlying protocol. They investigated AODV/IDM routing instead of AODV/IP. They recommended modification to AODV in their non-IP network model. Our

Table 2. The Simulation and Model Parameters

Simulation	**Parameters**
OPNET	version 14.5
Duration	900 sec
Updated interval	500,000 events
Values per statistics	100
Network Model	
Network Size	10, 20 Nodes
Simulated Disaster Area	500 X 500 m
Mobility	RWP
Mobility Speed (Uniform distribution)	0–10, 0–20, 0–30 m/s
Medium Access Protocol	IEEE802.15.4
Transmission power	0.1 W
Modulation	BPSK
Operating frequesncy	2 GHz
Bit Rate	250 kbps
Mean inter arrival rate (Exponential distribution)	2, 4, 8, 16, 24 msg/s
message size (constant)	1024 bits

simulation model implementation modifies the AODV/IDM into the HNER/HNEC to improve the delivery rate.

The simulation parameters as shown in Table-I are the input parameters to the simulation environment. The OPNET 14.5 (OPNET Technologies, 2008) is the simulation tool package used in this paper. Each node is modeled with four layer modules; application, network, medium access, and physical layer. The network layer implemented is the IDM layer which contains the HNEC/HNER routing. Using the default process model of the IEEE802.15.4 of OPNET in the simulation required some modification. This OPNET default process model contains interfaces to Zigbee process model. The modification abstracts the data link layer. However, the main implementation is modeling the forwarding and routing procedures. The HNEC model encapsulates/decapsulates IDM messages, updates forwarding table, and invokes HNER routing model to discover and maintain routes. Both models are included in the node model and they are related as parent and child. All routing messages enter the HNER process has to pass through HNEC model. In the simulation scenarios two network size (N) of 10 or 20 nodes were investigated, where all nodes are mobiles and are data sources. A default Random Waypoint (RWP) mobility model of OPNET is used. Nodes Mobility maximum speed (S) are stated at an integer uniform distributed, the simulation scenario include three speeds; between 0- 10 m/s, 0-20 m/s, or 0-30 m/s. Therefore, the scenarios are implemented for S= 10m/s, 20m/s, and 30m/s. All scenarios were simulated for 900 seconds with a zero pause time. The zero pause time is the worst case scenario which is more suitable for our investigation. Higher pause time will provide better performance than the finding.

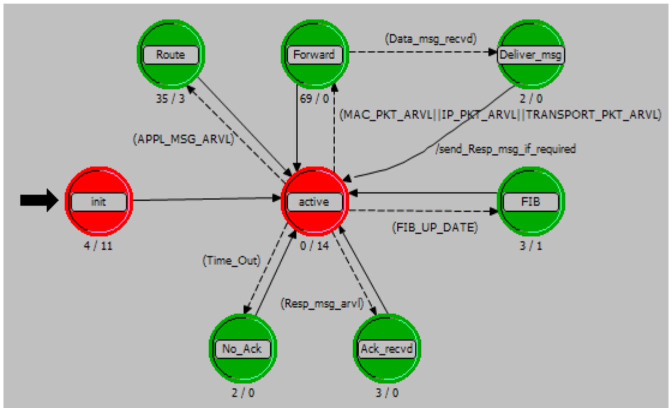

Figure 4. The HNEC Process Model

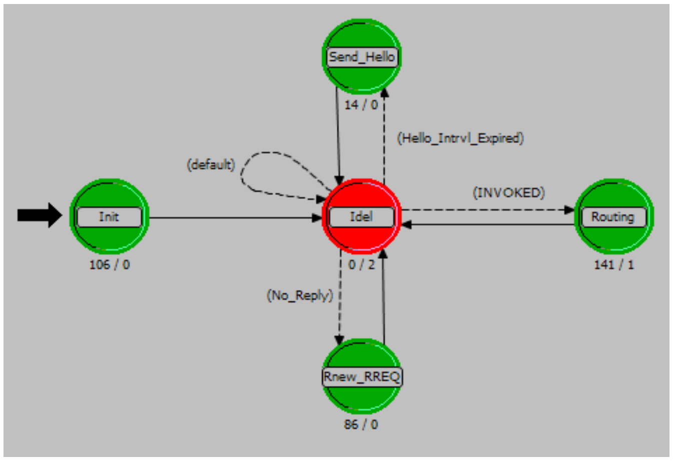

Figure 5. The HNER Routing Process Model

A simple finite state machine process model implemented for HNEC as shown in Fig. 4 and for the HNER as in Fig.5. The HNEC has eight process states as; initial-state, active-state, forward-state, route-state, forward information base table (FIB) state, ACK received state, and no-ACK received state. The HNEC is the parent process model which invokes the HNER process at the route state. For the HNER process model has five state, and two tables one is the Routing Information Base Table (RIB), and the other is the request message table. The RIB is the table to be used for the route selection and route updates.

For this simulation the HNEC buffers until a maximum of 100 messages for each destination. Each message has a constant size of 1 KByte and session duration of 100 seconds. Each node changes its route destination after 100 seconds in a uniform distribution selection. Each node selects its speed and trajectory direction randomly. The HNEC route table updates each 25 seconds.

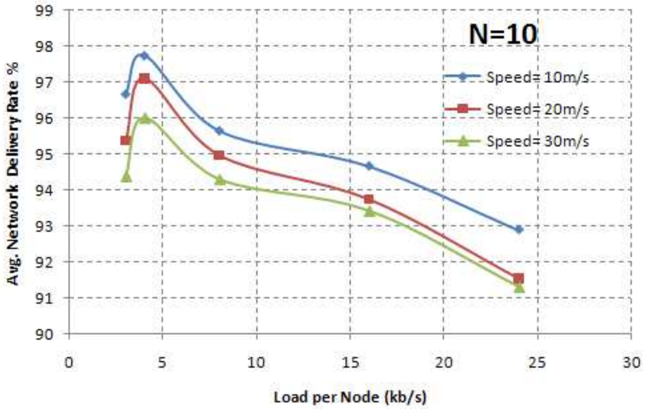

Figure 6a. The average delivery rate vs load per node with network size N=10

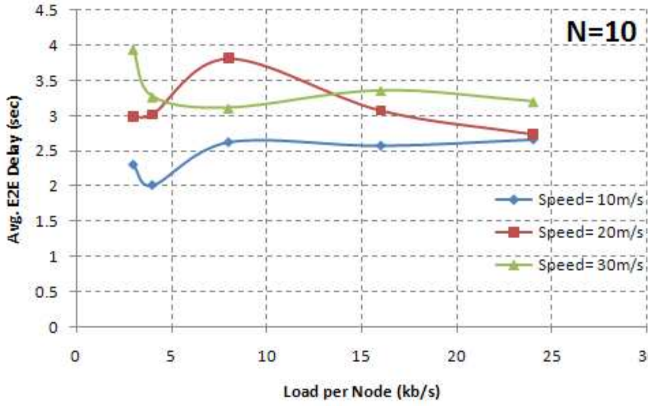

Figure 6b. The average E2E delay vs Load per node for N=10

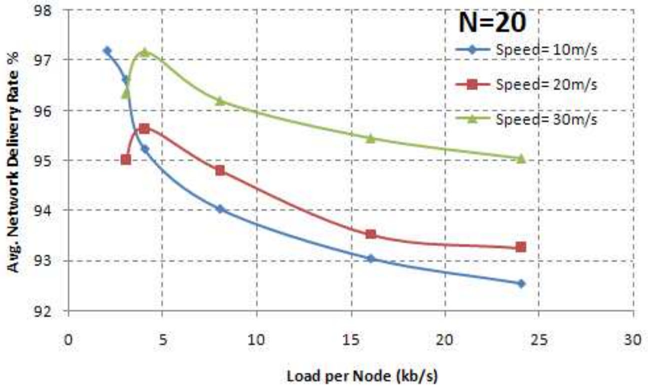

Figure 7a. The average delivery rate vs load per node with N=20

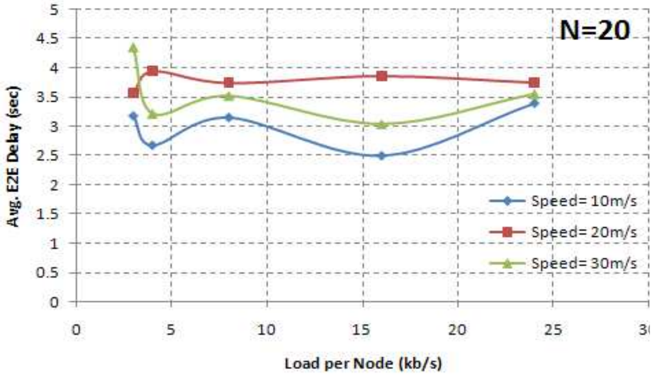

Figure 7b. The average E2E delay vs Load per node with N=20

Therefore, for each route discovery the entry lifetime is 25 seconds. The periodic neighbor hello messages are 3 seconds and the delivery acknowledge time-out is 3 seconds. The maximum period to store and carry messages by intermediate nodes is 30 seconds.

The performance metrics are deliver rate and end-to-end (E2E) delay while varying the maximum mobility speed and varying the load per node. The results obtained from the simulation scenarios are shown in Fig. 6 and 7. Each point in the figures is the average of 100 values taken from a two simulation runs with different seeds (50, 129). The investigation focus is on services with high delivery reliability and tolerant to delays below 30 seconds. However, for all simulation scenarios the delay standard deviation (SD) was below 4 seconds. The E2E delay SD increases by node speed and is higher by 0.4 seconds for N=20 than N=10. This deviation indicates jitter effects on message delivery which may not be suitable for some services. Therefore, higher speed always causes higher jitters. However, the average link break rates are; 1.08, 1.22, and 1.36 break per second (break/s), for S= 10, 20, 30 m/s respectively when N=10. The average link break rates are; 1.55, 2.1, and 2.23 break/s, for S=10m/s, 20m/s, and 30m/s respectively when N=20.

Fig.6a shows that the best performance of delivery rate is at S=10 m/s and load of 4 messages per second. Furthermore its E2E delay is the lowest for all different speed scenarios. The reason behind this is that it faces less link breaks and less message loss possibilities. Furthermore, the possibility of full buffers is less than other scenarios. The E2E delays as shown in Fig.6b are high delays compared with finding of Parkins et al. (2001), however, these delays (i.e. above 1 second) are reasonable to improve reliability of forwarding and delivering through discovered routes (i.e. improved about 20% of delivery rate comparing our N=20 model with 20 sources with Perkins's scenario model of 40 sources with N=50).

The Fig.7a results have different delivery performance than Fig.6a where the network delivery of a 20 mobile network with maximum speed of 30m/s is better than the delivery rate of 20 mobile with maximum speed of 20m/s or 10m/s, at node's load rates above 4 messages per second (msg/s). The reason is that their route discovery times are same, link breaking rates are approximately same, but their networks benefits from mobility speed in delivering messages. On the other hand there are some occasions while the majority of nodes may concentrate in some area leaving other empty because of the random distribution. This situation increase the possibility of delivery losses and only higher mobility decreases its duration. Furthermore, the increase of node density in the same simulation area (e.g. the DIA) makes it more possible to deliver messages with higher delivery at an optimum mobility speed range. Therefore, the network delivery for N=10 has optimum mobility speed range between 0-10m/s and for the N=20 the optimum speed range is between 0-30m/s. However, the network with 10m/s still overcomes other scenarios in E2E delay as shown in Fig.7b, and has a better delivery rate only for load rates below 4 msg/s.

Another point of view regarding comparing delivery rate results in different network size or different node densities is to consider the possibility of increasing number of sources, or decreasing node densities in the consideration of the three mobile speeds. From the results shown it is recommended to increase number of nodes from 10 to 20 mobiles when the mobility maximum speed is 30m/s. Another recommendation reduces the node's load to 8 msg/s or below, this will result with an average delivery rate larger than 94%. The decrease of number of mobile nodes in the area decreases node density and from the results it is recommended to reduce the speed to maximum of 10m/s.

CONCLUSION

The IDM platform and protocol is a general purpose model for heterogeneous networks and it is valuable in many different applications or purposes. For disaster situation we develop a specific protocol based on the IDM model for HNDR network communications. We call this protocol the hybrid network emergency communication protocol.

The HNEC protocol has three essential modules to perform the protocol features; 1) The heterogeneous function and internetworking different domain and networks are performed by IDM module, 2) the hybrid routing and gateway mobility functions performed by HNER interface, 3) the transportation selection and context aware functions are performed by the QSFM module. The HNEC is able choose the route path transportation depending on context aware and QoS features. Routing with IP applications do not have this feature because it only chooses among the network technologies. The IDM model's EPPs are designed for both underlying protocols (IP, UDP, SSL, etc.) and/or underlying network technologies (xbow, WiFi, 3G, etc.). This enables the HNEC to communicate among different devices' protocols and technologies.

The simulation results of the HNEC routing were improved compared with AODV performance of delivery rate. The forwarding technique of store-carry-forward was used. The routing protocol uses acknowledgement in addition to hello messages for link-break detection. However, by investigating the mobile routing of different mobility speeds, it has been concluded that increasing the speed may improve the delivery rate results depending on the node density in the disaster impact area. The message E2E delay performance is sensitive to mobility speed changes. Higher mobility speed always results in a higher E2E delay.

REFERENCES

Akkay, K., & Younis, M. (2004). Energy-Aware Routing to a Mobile Gateway in Wireless Sensor Network. Global Telecommun. Conf. Workshop. (pp16-21). Dallas, Texas, USA.

Ansari N., Zhang, C., Rojas-Cessa, R., Sakarindr, P., Hou, E., & De, S. (2008). Networking for Critical Condition. *IEEE Commun. Mag.*, *Vol.*15, *I*(2), 73-81.

Aoyama, T. (2009). A new Generation Network: Beyound the Internet and NGN. *IEEE Commun. Mag.*, *Vol.*47, *I*(5), 82-87.

Baryun, A., Al Begain, K. (2011). Survey on Sensor and Moble ad hoc Internetworking. Proc. of the 6th Advanced Technology Workshop (March, pp49-54). University of Glamorgan, Pontypridd, UK. ISBN: 978-184054-241-7.

Baryun, A., Al Begain, K., & Villa, D. (2011). A Hybrid Network for Disaster Scenarios. NGMAST Conf. Proceedings, (Sept., pp 129-136). Cardiff, UK.

Carlberg, K., & Atkinson, R. (2004). General Requirements for Emergency Telecommunic-ation Service. RFC3689. Informational, IETF. Retrieved May, 1, 2011, from www.ietf.org.

Chen, C-M, Macwan, A., & Rupe, J. (2011). Network Disaster Recovery. *IEEE Communication Mag.*, *Vol.*49, *I*(1), 26-27.

Dilmaghani, R., & Rao, R. (2006). Hybrid Wireless Mesh Network Deployment: A Communication test bed for Disaster Scenarios. *ACM, WiNTECH'06,* Sept., Los Angeles, California, USA.

Dunkels, A., Alonso, J., & Voigt, T. (2004). Making TCP/IP Viable for Wireless Sensor Networks. Proceedings of the first European workshop on wireless sensor networks. Berlin, Germany.

Dyo V. (2005). Middleware Design for Integration of Sensor Network and Mobile Devices. ACM International Conf. Proceedings. NY, USA.

Feeney, L., Ahlgren, B., & Westerlund, A. (2001). Spontaneous Networking: An Application-Oriented Approach to Ad Hoc Networking. *IEEE Commun. Mag.*, *Vol.*39, *I*(6). 176-181.

Fujiwara, T., & Watanabe, T. (2005). An ad hoc networking scheme in hybrid networks for emergency communications. *Ad Hoc Networks. Vol.*3, I(5), 607–620.

Hamid, S., Al-jaroodi, J., & Mohamed, N. (2006). Trends in Middleware for Mobile Ad Hoc Networks. *Journal of Communication, Vol.*1, *I*(4), 11-21.

Henning, & Spruiell. (2010). Distributed Programming with Ice. Revision 3.4.0. ZeroC. Retrieved January 1st, 2011, from http://www.zeroc.com.

Horre W., Michiels, S., Matthys, N., Joosen, W., & Verbaeten, P. (2007). On the Integration of Sensor Networks and General Purpose IT Infrastructure. MidSens'07, Proc. of the 2nd Int. Workshop on Middleware for sensor networks. Nov., ACM Press. NY, USA.

Morrison, K., T. (2011). Rapidly Recovering from the Catastrophic Loss of a Major Telecommunications Office. *IEEE Commun. Mag.*, *Vol.*49, *I*(1), 28-35.

Mosharaf, N., Chowdhury, K., & Boutaba, R. (2009). Network Virtualization: State of the Art and research Challenges. *IEEE Comm. Mag*, *Vol.*47, *I*(7), 20-26.

OMG, Object Management Group, (2002). The Common Object Request Broker architecture and specification. Framingham, Massachusetts, USA.

OMG, (2008), Object Management Group, CORBA Messaging. V3.1. Retrieved October 1st, 2010, from http://www.omg.org/spec/CORBA/3.1/.

OPNET Technologies, (2008). OPNET Modeler documentation set. Version 14.5. Retrieved January 1st, 2009, from http://www.opnet.com.

Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc On-Demand Distance Vector (AODV) Routing. RFC3561. Experimental, IETF.

Perkins, C., Royer, E., Das, S., & Marina, M. (2001). Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks. *IEEE Personal Communications*, *Vol.*8, *I*(1), 16-28.

Senner, T., Karnapke, R., Lagemann, A., & Nolte, J. (2008). A combined routing layer for Wireless Sensor Networks and Mobile Ad-Hoc Networks. The second International Conference on Sensor Technologies and Applications. Cap Esterel, France.

Villa, D., Villanueva, F., Moya, F., Urzaiz, G., Rincon, F., & Lopez, J. (2008). Object Oriented Multi-Layer Router with Application on Wireless Sensor-Actuator Networks. IEEE International Conference on Networks. New Delhi, India.

Villanueva, F., Villa, D., Moya, F., Barba, J., Rincón, F., & López, J. (2006). Context-Aware QoS Provision for Mobile Ad-hoc Network based Ambient Intelligent Environments. *Journal of Universal Computer Science, Vol.*12, *I*(3), 315-327.

Wang, M., Cao J., Li, J., & Das, S., (2006), Middleware for Wireless Sensor Networks: A Survey. *Journal of computer science and technology*, *Vol.*23 *I*(3), 305-326.